

FEDERAL TRADE COMMISSION

I N D E X

	PAGE:
1	
2	
3	
4	
5	
6	3
7	
8	4
9	
10	14
11	
12	
13	79
14	
15	150
16	
17	211
18	
19	
20	
21	
22	
23	
24	
25	

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

FTC SPAM SUMMIT:

THE NEXT GENERATION OF THREATS AND SOLUTIONS

FEDERAL TRADE COMMISSION
601 NEW JERSEY AVENUE, N.W.
WASHINGTON, D.C.

DAY 1

WEDNESDAY, JULY 11, 2007

P R O C E E D I N G S

- - - - -

WELCOME

1
2
3
4 MS. CHRISS: Good morning, everyone. Hi there.
5 Please take your seats, we are about to begin. This is
6 it. Spam Summit, the Next Generation of Threats and
7 Solutions. I am so pleased and delighted to see all of
8 you here. This is wonderful. I see that we are going
9 to have some very good debate, just by the faces in the
10 audience. I recognize a lot of you from our past
11 events. So, thank you for being here.

12 Before we get started, I do have a few
13 housekeeping announcements. So, let's just get through
14 them. If you have a cell phone, or any other noise
15 maker, just turn it off. Just turn it off now. It is a
16 good time to turn it off. Otherwise, there's a risk,
17 you could receive spam from us if you don't, so turn it
18 off. Turn it off.

19 The other thing is, we are a Federal Government
20 agency and we do practice certain safety measures. If
21 there is an emergency, and that is very unlikely, you
22 have two exits, the way you came in, and then out
23 through the hallway and straight back. We also practice
24 something called shelter in place. If that happens, you
25 will go into the hallway and wait for further

1 instructions.

2 This is the meat of the matter: You, the
3 audience, are so integral to this, so I want to tell you
4 the three ways you have to participate. We will have a
5 roaming microphone at the end of each panel, so wait for
6 the mic, state your name and your affiliation and go for
7 it. The other way, if you're out there in webcast land,
8 you can email us at spamsummit@ftc.gov, and you can also
9 use your question note cards if you are in the room and
10 they will be provided to the moderators. So, we want to
11 hear from you.

12 Now, without further delay, I would like to
13 introduce our chairman. She is a leader in this
14 technology arena, and she has been so incredibly
15 supportive of all of our consumer protection efforts in
16 this area, and I'm so pleased to introduce, without
17 further ado, Chairman Deborah Platt Majoras.

18 (Applause.)

19 OPENING REMARKS BY CHAIRMAN MAJORAS

20 CHAIRMAN MAJORAS: Well, thank you. Wow, we
21 don't usually have a stage. Thank you so very much,
22 Sana, and thanks to you and your team for all the great
23 work putting this together. Welcome to everyone here.
24 I'm particularly grateful to all of our very
25 distinguished panelists for joining us for the next two

1 days.

2 In 1971, C. P. Snow, noted British author and
3 commentator on science and technology issues, said of
4 technology, "It brings you great gifts with one hand,
5 and it stabs you in the back with the other." Although
6 spam was known only as lunch meat, mystery meat, I don't
7 know, back in 1971 when he said this, his quote is
8 really spot-on with respect to email and spam.

9 Email technology has brought us great gifts in
10 the form of quick, efficient, ubiquitous communication,
11 but it's also brought us spam, which has the potential
12 to metaphorically stab us in the back by inundating
13 consumers' inboxes with unwanted email, facilitating
14 fraud and malware and frankly betraying consumers' trust
15 and confidence in the Internet and the electronic world.

16 In 2003, the FTC convened a spam forum to
17 discuss the technical, legal and financial issues
18 associated with spam. Now, today and tomorrow, in a
19 continuing effort to stay apprised of developments, we
20 want to explore the next generation of spam threats and
21 solutions.

22 The volume of unsolicited emails being reported
23 by email filtering companies is rising, creating
24 significant costs for businesses and consumers alike.
25 Botnets, the networks of hijacked personal computers

1 that spammers are using to conceal their identities, has
2 become the preferred method for sending spam. Even more
3 troubling, spam reaching consumers' inboxes is more
4 often being used to launch phishing attacks and to
5 deliver malicious code or malware to consumers'
6 computers.

7 This new generation of malicious spam goes
8 beyond mere annoyance. It can result in significant
9 harm to consumers and undermine the stability of the
10 Internet and of email in particular.

11 If you click on a link in an email message, you
12 may be lured to a website that will either trick you
13 into you divulging your personally identifying
14 information, or infect your computer with spyware or
15 other types of malware. Even merely opening a malicious
16 email can subject you to harm. The surreptitious
17 development of such malware can result in slow computer
18 performance at a minimum. Installation of key logger
19 software that can record and then report on your every
20 key stroke. The spread of computer viruses, and the
21 hijacking of your computer for use as a botnet.

22 In addition, new threats to communication media
23 other than email are knocking on the door. Spam's
24 cousins, spim, which is spam over instant messaging,
25 spit, spam over Internet telephony -- spam to mobile

1 devices threaten to undermine the benefits of mogul
2 services and Internet telephony in the same way as spam.

3 Social networking websites have become yet
4 another frontier for spam messages. The lessons we've
5 learned and continue to learn from spam, thus, are going
6 to be valuable as we address, or even better, try to
7 avoid similar problems in these other communications
8 technologies.

9 Now, we have to work to combat malicious spam in
10 several ways, and the first is through law enforcement.
11 We cannot permit the electronic frontier to become a
12 lawless world. The FTC has engaged in aggressive law
13 enforcement to combat spam, and since 1997, we have
14 aggressively pursued deceptive and unfair practices
15 perpetrated through spam in 89 law enforcement actions
16 against 142 individuals and 99 companies, with 26 of the
17 cases filed after Congress enacted the CAN-SPAM Act in
18 late 2003.

19 For example, in one recent case, FTC versus
20 Dugger, the FTC sought to stop the underlying use of
21 botnets to send spam. We allege that the defendants
22 relayed sexually explicit commercial emails through
23 other people's home computers without their knowledge or
24 consent, in violation of the CAN-SPAM Act, and under the
25 final order obtained in the case, these defendants are

1 banned from continuing to violate the Act and they are
2 to turn over all of their ill-gotten gains.

3 Of course, malicious spam can also be used as a
4 means to disseminate spyware or other malware that
5 causes the same problems and the FTC has been actively
6 pursuing spyware companies using our authority under
7 Section 5 of the FTC Act, and we have brought about a
8 dozen law enforcement actions in the past two years.

9 In most instances, though, the acts of malicious
10 spammers are criminal. Criminal law enforcement
11 agencies are best suited to expertly shut down those
12 operations. So, for example, in June, the FBI and the
13 Department of Justice announced a crackdown on botnets
14 and those who control them. As part of this operation,
15 the FBI and DOJ identified more than one million
16 personal computers infected with malware that attack
17 them to be hijacked and used as a part an army of bots
18 to allow other computers to send malware and send spam.

19 Today the crackdown has noted three arrests:
20 Robert Soloway who allegedly sold spam kits and botnets
21 for spamming; James Brewer who allegedly compromised
22 more than 10,000 PCs around the world; and Jason Downey,
23 who allegedly ran a botnet used to conduct distributed
24 denial of service, DDoS attacks.

25 So, while there's no single solution to halting

1 the use of botnets malware completely, these law
2 enforcement actions are significant in this effort.

3 Now, a second way to defend ourselves against
4 malicious spam is knowledge. That is knowing with whom
5 we're interacting. Just as we can ask visitors to swipe
6 identification badges used by metric identifiers to
7 verify who's entering our physical space, we can use
8 authentication technology to verify who's entering our
9 electronic space.

10 At the Commission's November 2004 Email
11 Authentication Summit, which we co-sponsored with the
12 Department of Commerce's NIST, the commission gathered a
13 wide spectrum of interested parties to try to find a
14 solution to the problem of email anonymity. We had the
15 goal then of invigorating the search for and getting
16 some agreement on viable email authentication tools.

17 Since that time, domain level email
18 authentication and the email reputation services have
19 been adopted, at higher levels. Over 70 percent of the
20 Fortune 100 now authenticate their outbound email, while
21 over 25 percent of the Fortune 500 authenticate their
22 outbound.

23 Trade associations like The Directing Marketing
24 Association and the Email Sender & Provider Coalition
25 require their members to authenticate their email. So,

1 we are making progress, still not enough. The
2 Commission urges improvement in anti-spam technology and
3 in particular continuing in domain level authentication.

4 This technology, we still believe, paired with
5 reputation and accreditation systems holds great promise
6 for preventing spammers from operating anonymously,
7 which is something they obviously count on. So, we
8 intend to continue working with industry to spur these
9 efforts.

10 Third, to protect ourselves, we have to practice
11 self defense. We're all consumers. Every consumer
12 needs to learn how to spot, avoid, and defend themselves
13 against malicious spam. We've taken many steps to
14 educate consumers about how to avoid problems with
15 phishing, malware and spam bots in consumer alerts, such
16 as, should I sing this, botnets and hackers and spam, oh
17 my, and on our comprehensive educational website,
18 OnGuard Online. These educational materials encourage
19 consumers to use anti-virus and anti-spyware software to
20 keep their computers up to date, among other tips.

21 During this summit, we are going to explore
22 other measures that both consumers and businesses can
23 take to further empower themselves, and on this in
24 particular, we absolutely need your help. The biggest
25 problem we have in consumer education is not with

1 pulling together the right materials, and we do get help
2 from industry in doing that, it's distribution. Every
3 one of us can help with that issue.

4 Fourth, just as we sometimes need help to
5 protect ourselves in the physical world, collaboration
6 among all the stakeholders in the electronic world is
7 invaluable. Absolutely critical in this fight. Given
8 the technical aspects of the spam problem, continued
9 collaboration with experts from the technical community,
10 including ISPs and email filtering companies, will
11 strengthen these efforts against malicious spam. In
12 addition, because of the global nature of the spam,
13 international cooperation is essential.

14 Most of our enforcements actions involving spam
15 have had international components and we've been
16 cooperating with our law enforcement counterparts around
17 the world in battling spam. We're cooperating not only
18 on individual cases, but we're very active in the London
19 Action Plan Initiative, which we helped start, an
20 informal network of spam enforcers and industry
21 representatives from over 20 countries that allow us to
22 discuss cases, techniques, investigations, educational
23 initiatives and the like.

24 Of course, the recently enacted U.S. Safe Web
25 Act, which gives us authority to cooperate even more

1 closely with our overseas counterparts, gives us the
2 tools we need to strengthen that program and we are
3 using those to cooperate today.

4 Now, my hope is at this two-day summit, you all
5 will work with us to further explore this problem and
6 the approaches I have just outlined and new approaches.
7 By the end of the summit, we would like to have a record
8 that defines the malicious spam problem, identifies
9 methods used for sending this spam, uncover the malware
10 economy, how they're making money, identifies threats
11 that malicious spam poses to emerging platforms like
12 mobile devices and social networking websites, examine
13 the methods that law enforcement can deploy to deter
14 these malicious spammers and cybercriminals, develop new
15 education for putting consumers back in control, explore
16 technological tools for keeping malicious spam out of
17 the inboxes, identify best practices for legitimate
18 email marketers, and finally, establish a plan that we
19 can quickly implement as the stakeholders here to reduce
20 the deleterious effects of spam bots and malicious spam.

21 The risk that malicious spam will erode
22 confidence in the Internet's benefits to consumers is
23 too great to ignore, and we have to continue to act
24 quickly to try to address it. As my former colleague,
25 Commissioner Orson Swindle said at our last spam forum

1 in 2003, we all have to work together to address this
2 problem, and that's why we're here today.

3 So, I look forward to the continued development
4 and collaborative initiatives between law enforcement,
5 international bodies, private industry, all interested
6 groups, to combat the proliferation of spam bots and the
7 spread of malware via spam.

8 So, with that, let's get down to it. I thank
9 you all again very much for being here and we look
10 forward to hearing from you. Thanks so much.

11 (Applause.)

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

DEFINING THE PROBLEM

MR. HUSEMAN: I would like to welcome everyone here today and it's good to see so many familiar faces from the 2003 FTC Spam Forum. As Chairman Majoras mentioned, much has changed in the world of spam in the last four years and one thing we definitely want to change in this Spam Summit from the 2003 spam forum is that we are not going to have any fights this year.

This opening panel is going to explore some of the big picture issues that we are going to discuss in more depth over the next two days, and in this panel in particular we're going to focus on defining the problem and trying to address a few key questions.

Now, the first question is that the earlier findings indicated that most spam was fraudulent, deceptive and offensive, so how has the nature of spam shifted now? The second question is, is spam now being used for malicious and criminal purposes?

Finally, we're going to try to address, is this spam reaching consumers' inboxes or is it being filtered by some of the Internet service providers filtering software and other mechanisms?

So, let me first introduce the panelists, then the panelists are going to give some brief presentations, and then I will follow that up with

1 questions and we will open it up to questions from the
2 audience.

3 So, just starting to my left, first is Susannah
4 Fox, she's the associate director for the Pew Internet
5 and American Life Project, and that is a research
6 organization that's funded by the Pew Charitable Trust
7 to examine the social impact of the Internet.

8 Next is Thomas Grasso who is a supervisory
9 special agent at the Federal Bureau of Investigation,
10 the FBI, and Tom is continuing the work that he started
11 in 2003 to develop the National Cyber Forensics and
12 Training Alliance, which is a joint partnership between
13 law enforcement, academia and industry.

14 Next is Trevor Hughes, who is the executive
15 director of the Email Sender & Provider Coalition, which
16 is a group that's trying to create solutions to the
17 continued proliferation of spam, and ESPC's membership
18 provides volume mail delivery services to an estimated
19 250,000 clients.

20 We start off, when I introduce my next panelist
21 with the first audience quiz, what do Ben Affleck,
22 rapper Eminem and Scott Richter have in common? And the
23 answer is that in 2003, they all made Details Magazine's
24 top ten list of the most influential and powerful men
25 under 38. So, we won't ask Scott whether he's under 38

1 in 2007, but he is chief executive officer of Media
2 Breakaway, and he founded his first online marketing
3 company in 2001.

4 Finally we have Charles Stiles, who is the
5 chairman of the Messaging Anti-Abuse Working Group, and
6 he served on the organization's board of directors for
7 the last three years.

8 So, that ends the introductions, I will start
9 off with Susannah.

10 MS. FOX: Good morning. Thank you very much for
11 having me this morning. My name again is Susannah Fox,
12 and I work for the Pew Internet and American Life
13 Project. We study the social impact of the Internet,
14 which means we study who's online and what they do, but
15 also who's not online, and why. Most of our research is
16 based on telephone surveys, which we feel provide a
17 pretty accurate picture of the changing population. All
18 of our reports and our data sets are available for free
19 on our website at PewInternet.org.

20 Our most recent survey report about spam found
21 that email use has not decreased over the years, but
22 people trust it less. Fifty-five percent of email users
23 say that spam has made them less trusting of email, in
24 general, which is about the same percentage as what we
25 found in previous years. When asked if the volume of

1 spam in their inboxes had changed, most users say they
2 don't perceive a change, but 37 percent of email users
3 say that their personal email inboxes have received more
4 spam. That's up 13 points since 2004.

5 Thirty-six percent of email users say they have
6 received unsolicited email requesting personal financial
7 information, such as a bank account number or Social
8 Security number. That's essentially the same percentage
9 as we found in January 2005. However, most email users
10 describe spam as an annoyance. Only one in five email
11 users say that spam is a big problem for them. That's a
12 drop from our surveys three years ago.

13 This drop might be due to a perceived decrease
14 in the volume of the most offensive kind of spam
15 containing explicit adult content. Fifty-two percent of
16 email users report having received a pornographic spam
17 in our most recent survey, which was fielded in February
18 2007, down from 63 percent two years ago and 71 percent
19 three years ago.

20 People are also becoming more knowledgeable
21 about spam. They know better how to recognize it and
22 handle it, and that seems to give them a sense of
23 control. Sixty-eight percent of email users say they
24 almost never unintentionally open an email message
25 without realizing it was spam. Seventy-one percent of

1 email users say the use filters provided by their email
2 provider or employers, up from 65 percent two years ago,
3 and we also see that reflected in the data, where work
4 email is being protected much better than personal
5 email.

6 It might also be that for many people, spam has
7 become like traffic, or even air pollution. You can
8 complain about it, you can plan for it, you can try to
9 avoid it, but it might just be a fact of modern life
10 that we have to live with. Those of us who are online
11 every day are often surprised when our survey data comes
12 back that most people don't spend all day online. Most
13 people don't know a lot about the technology they use,
14 but they do rely on email and the Internet to stay in
15 touch with family and friends and to get work done.

16 A majority of Internet users are not
17 sophisticated about technology. They don't know they
18 should upgrade to a better email provider. They don't
19 know they should read the fine print when they sign up
20 for a newsletter or buy a product from a new site. They
21 do know that spam is cluttering their inboxes. The
22 consequence of all this is a loss of trust in email.

23 MR. HUSEMAN: Thank you very much, and we will
24 ask you some questions about your findings in a little
25 bit. Over to Tom, please.

1 MR. GRASSO: Thank you, it's good to see
2 everyone. My name is Tom Grasso, I am a special agent
3 with the FBI. I work at a nonprofit entity in
4 Pittsburgh called the National Cyber Forensic Training
5 Alliance, which is a very unique operation, I think it's
6 the only one of its kind right now. I am one of ten FBI
7 staff that's assigned there, seven of us are agents, and
8 I go to work every day where I work with people that
9 aren't FBI, I work with people from industry, from other
10 government agencies, from academia, and what we try to
11 do is get the information that we need from people that
12 are out there basically running the Internet, the ISPs,
13 the software companies, have them share the information
14 with us about who's attacking them, who's causing them
15 problems, and where the crimes are occurring on the
16 Internet. Certainly, spam is one of those major
17 problems.

18 In 2003, we started up a project at the NCFTA
19 called Slam Spam, and it was our intent, our goal to
20 coalesce and bring together information from our various
21 industry partners and get that into the hands of
22 government and law enforcement so that we could go out
23 and do something about the spam problem from an
24 enforcement perspective.

25 I'm very happy to be here at the FTC. The FTC

1 has been the leader in this front as far as I'm
2 concerned with their aggressive actions that they've
3 taken against the various spammers and stuff like that.
4 So, it's an honor for me to be here and also to have
5 worked with the various investigators and attorneys for
6 the FTC.

7 So, when we started this project in 2003, it was
8 really us going out to the people in industry, many of
9 the people that are in this room, and saying to you,
10 what is the spam problem? What is the nature of it, and
11 what can we do about it? And what we found out is that
12 spam is really more than just these annoying messages
13 that you get in your inbox. Yeah, certainly that is a
14 big part of it, and it's something that we find most
15 offensive about it, but really with spam, it involves
16 all sorts of other criminal activity.

17 Bot networks, which are networks of thousands of
18 and these days hundreds of thousands of compromised
19 computers that are being used to disseminate the spam.
20 Denial of service attacks that are occurring on a
21 regular basis against sites that help us filter spam.
22 The products that are often being spammertized, if you
23 will, are fraudulent in nature, or have some type of
24 criminal aspect to them.

25 So, there is a lot of bad stuff that goes on

1 with spam, and I think it's a worthy target of anybody
2 in law enforcement, when you're on the Federal level or
3 not, I think it's something that is causing a big
4 problem on the Internet, and I think we need to do
5 something about it, and the way that's going to happen
6 is with collaboration, government, industry, all of us
7 working together on this problem, and I think that this
8 meeting that I'm here at today is a great example of
9 that. I think we are going to help with that a lot.
10 Thank you.

11 MR. HUSEMAN: Thank you very much. Now I would
12 like Trevor Hughes to come up, please.

13 MR. HUGHES: Good morning. I do have some
14 slides. Do you know how to get my slides up? There it
15 is. Excellent.

16 Good morning, it's delightful to be here, my
17 name is Trevor Hughes, I'm the executive director of the
18 Email Sender & Provider Coalition. We are a trade
19 association made up of companies that are trying to do
20 the right thing in the email space. They are trying to
21 use email legitimately in the marketplace, for good
22 purposes, for marketplace purposes, and for a long time
23 now we have been trying to stabilize and make more
24 predictable the environment in which they operate.

25 We came into the debate, the discussion of spam

1 with a very clear agenda, very clear purpose, and that
2 was that in our energy, in our enthusiasm to fight spam,
3 we were missing one part, and that was that we needed to
4 defend the legitimate use of this channel, which is the
5 killer ap that we're all trying to protect in the end.

6 And so the ESPC has now for five years been
7 working very aggressively to try and protect this killer
8 ap, email, this thing that we all know and love so much.
9 I would like to suggest that email has perhaps become
10 one of the most fundamental tools for us in
11 communicating in both our work and personal lives.
12 Certainly we've seen surveys that suggest it's more
13 important than phones and mail and other things, and I
14 know from my personal experience and I'm sure many of
15 you do, that you're already getting itchy to get on the
16 hallway and get in your BlackBerry and see what's in
17 your inbox.

18 Email is one of our fundamental means of
19 communication, and we need to make sure that as we fight
20 spam, which is a threat to the eco system of email, we
21 also work to protect this very thing that we know and
22 love so much.

23 So, what I want to talk to you about today is a
24 little bit about what we have seen over the past four
25 years since the last time we gathered for an event

1 looking at spam itself. Obviously we met in the interim
2 to talk about email authentication. I want to talk to
3 you about the CAN-SPAM Act and the effect that that's
4 had on the legitimate marketplace. I want to talk to
5 you about technology and consumer choice and consumer
6 research that our organization conducted.

7 You'll hear more about that later through this
8 event from Dave Lewis, chairman of one of our
9 committees, and I want to talk to you about the
10 evolution of industry practices and the differentiation
11 between the legitimate use of email today and spam. I
12 think we are much better today at distinguishing between
13 those things.

14 I, too, like Brian, though, have to reflect,
15 before I dive into my few slides here, on what a
16 difference four years makes. Four years ago, the
17 tension in this room was palpable. There was, almost, a
18 fist fight four years ago. There were rumors that there
19 may be people taken out in handcuffs. It didn't happen.
20 But we were all sort of on the edge of our seats in this
21 moment of fighting spam. I think we are all more
22 mature, and have been around a lot longer in the debate.
23 It's more sanguine, more professional.

24 I see a lot of familiar faces now, people who
25 have been fighting this good fight for a long time. I

1 think that reflects upon perhaps what Susannah has said,
2 that the problem has matured in the marketplace. Not
3 only consumers, but the people fighting the problem have
4 been finding things that work and working those
5 solutions, working on new challenges, and we have just a
6 different perception and a different focus today.

7 I would like to suggest that our organization
8 really is interested in trust, and if you look at some
9 of the business school research on what is trust in the
10 business marketplace, it's made up of a few things, but
11 two of the four components are competence and
12 consistency. Certainly when I look at the ESPC, I think
13 that we have focused aggressively on making sure that
14 our members are competent in complying with the law, in
15 complying with our best practices, in complying with
16 technological solutions in the marketplace, and they are
17 consistent in doing those things.

18 That's going to be my big close at the end, that
19 I think those are two of the functions that are most
20 different between the legitimate marketplace today and
21 spammers, that we are competent and consistent today.

22 Let me speak quickly about CAN-SPAM. I know
23 that we can probably spend two days talking about
24 whether CAN-SPAM is a success or a failure, whether it's
25 done anything or not done anything. I would like to

1 suggest to you that I think CAN-SPAM has done as much as
2 it could, and that it is being used for the tool that it
3 is. None of us ever should have, and if any of you ever
4 did look at it as being a silver bullet to stop spam,
5 you were misguided at the outset.

6 The CAN-SPAM Act provides a stable platform of
7 predictable and consistent platform for legitimate
8 businesses to engage in commerce through the channel of
9 email. For that purpose, and for that purpose alone, I
10 would say it has been a great success. But it also
11 gives the FTC, and you've heard the chairman speak
12 before, the ability to go after spammers. It gives AGs
13 the ability to go after spammers.

14 I think that we have not seen the deterrent
15 effect that we had hoped to see with the CAN-SPAM Act,
16 that there are still fraudsters and crooks out there,
17 many of them have moved to off-shore, phishing is still
18 a problem, but at the end of the day, the effect on the
19 legitimate marketplace has been great. In fact, the
20 FTC's report to Congress suggested that something like
21 90-plus percent of the mainstream marketplace was
22 complying with the CAN-SPAM Act. So, it has had an
23 effect, and that effect has been sizeable and
24 substantial, particularly in the legitimate marketplace.

25 I also want to talk about technology, and

1 consumer choice. We did consumer research earlier this
2 year, and our survey showed while consumers may not be
3 reading terms and conditions when they sign up, while
4 they may not understand that there are better
5 alternatives out there in terms of filtering email or
6 moving to other email clients that may be doing a better
7 job, they are tyrannical editors of their inbox. They
8 know how to manage their inbox.

9 We all know this, in an incredibly sophisticated
10 way. They spend a split second analyzing every single
11 message in their inbox to determine whether they will
12 keep it or not, and in fact, our surveys showed that
13 they look at only two things, they don't open most
14 messages, they look at the from line and the subject
15 line, and if your message looks spammy or phishy or just
16 bad from the from line or the subject line, if they
17 don't know and trust you, if you haven't been competent
18 and consistent in sending your message, they will delete
19 you immediately. You never even get opened or seen.

20 That suggests to me that we need to perhaps move
21 away from a paternalistic view of consumers and
22 recognize that consumers can be an ally. They can be
23 mobilized to help us in this fight. Certainly there are
24 some solutions in the marketplace that are trying to do
25 that, I think we can certainly do more.

1 One of the things that we certainly saw in our
2 survey was that consumers want more buttons, not less.
3 Many of the major email clients, web mail providers,
4 ISPs, offer a report-a-spam button and that's it.
5 Unfortunately, that turns out to be a fairly clumsy tool
6 for a lot of consumers, because they know that there are
7 some messages that they just want a safe and verified
8 unsubscribe from. They have asked for it once, and it's
9 not really spam, but the only tool that they have to say
10 get me out of this email chain is to report it as spam.

11 Well, that has effects for legitimate businesses
12 in their reputations in email channel, and it creates
13 consequences in the email channel that are not good in
14 our broader fight against spam.

15 So, one of the messages that we would like to
16 convey today for sure is that I think we need to
17 mobilize consumers and give them more tools in the
18 inbox, allow them to report something as spam, to report
19 something as fraud, to unsubscribe from a message, or
20 just to send feedback to the sender. Those types of
21 tools would be embraced, based on the research that we
22 have.

23 I would also like to talk about the effective
24 industry practices. The chairman mentioned before that
25 we were the first organization to require our members to

1 authenticate email. In fact, we were one of the
2 organizations that was at the center of developing some
3 of the very earliest email authentication standards.
4 We've gone beyond the CAN-SPAM Act, we've gone way, way
5 beyond the CAN-SPAM Act. Before the CAN-SPAM Act was
6 passed, we were requiring our members to only engage in
7 permission-based, consent-based marketing practices, and
8 we stand strongly by that. We think that that mix of
9 the CAN-SPAM Act with best practices for industry that
10 extend further is a good mix for legitimate businesses.

11 We've also issued standards and recommendations
12 on deliverability, and we have conversations every week
13 with our members. In fact, we have at least a couple of
14 calls every week, talking about the latest technological
15 developments and the latest deliverability challenges
16 that exist for legitimate businesses in the marketplace.

17 I think that one of the things that we've seen
18 in authentication, though, is that more senders do need
19 to be authenticating. Our organization is significant
20 and influential I think in this regard, but there are so
21 many more senders. In fact, one of the problems that we
22 have, it's sort of a chicken and an egg problem, is that
23 senders don't want to authenticate until there's
24 consequences on deliverability on the receiving side of
25 the equation. So, you don't want to authenticate if

1 it's not going to have any effect on your mail
2 whatsoever.

3 So, we need more ISPs to more consistently adopt
4 and engage in authentication. There's some good news
5 there, but I think there's better news that we could
6 hope for and expect some time down the road.

7 I think at the end of the day, we need to
8 realize, and this first panel is about redefining the
9 problem, we are at a new environment, we are in a new
10 form of communication about these issues, and the
11 problem is not the problem that it was four years ago.
12 The problem of spam today, the differentiation between
13 spam and legitimate mail is pretty clear. Legitimate
14 senders are competent and consistent. They comply with
15 CAN-SPAM. They follow industry best practices. They
16 authenticate their mail.

17 Spammers still do the kind of herbal Viagra
18 stuff that we all know and love from four years ago, but
19 it's become a bit more insidious today with phishing and
20 other attacks. They are not consistent, and they're not
21 competent, either. Sometimes they don't even spell
22 well.

23 We need to recognize those inconsistencies,
24 those incompetencies, and to differentiate between spam
25 and legitimate mail so that we can really attack the bad

1 stuff and protect the good stuff.

2 So, in closing, I think that we can now better
3 identify what is bad, and perhaps consumers are doing it
4 as well as we are, and Susannah's data suggesting that
5 consumers have a more sanguine attitude towards spam is
6 indicative of this. We can recognize spam much better
7 today than we ever could before. The legitimate
8 marketplace is competent and consistent and spammers are
9 not. I think we need to keep focusing on that
10 differentiation, so that we can build higher walls and
11 greater protections against these problems.

12 That's all I had. This is how you can get in
13 touch with us. Thank you very much.

14 MR. HUSEMAN: Thank you, Trevor.

15 (Applause.)

16 MR. HUSEMAN: Now, Scott Richter, can you please
17 come up.

18 MR. RICHTER: Good morning. My name is Scott
19 Richter and I'm the CEO of mediabreakaway.com, and today
20 I want to talk about the challenges facing legit email
21 marketers.

22 What I want to discuss is unsolicited email
23 messages, or excuse me, email versus legitimate
24 marketing messages. There's three big challenges facing
25 email marketers today. The first is deliverability, the

1 second is suppression lists and the third is consumer
2 education.

3 First I would like to address deliverability.
4 The email marketers can follow all the rules and still
5 be blocked. There are several reasons for this. One is
6 a lot of filtering systems are automated. This causes
7 millions of legit messages from mom-and-pops to
8 high-volume email marketers to be blocked.

9 Next, the next issue has been suppression lists,
10 which came from the CAN-SPAM Act. At the time it was a
11 great idea, but now many of these lists have grown to
12 over ten million plus names on them. A lot of smaller
13 senders who have small lists from their newsletters who
14 put advertisements into them to earn a living do not
15 have any way to run a list of this size against their
16 list of maybe 100 to 500 to 1,000 users.

17 Lastly, I would like to talk about consumer
18 education. A lot of times, consumers identify messages
19 as spam that they do not, in fact, opt into and confirm
20 their email address lists. A lot of times, the longer
21 someone has had the same email address, the harder it is
22 for them to remember what they have signed up for over
23 the years.

24 Another issue with the consumer education is
25 that many times they do not read the privacy policies of

1 the sites they are joining. A lot of times they may not
2 be aware of what they are signing up for on the sites.

3 In summary, filtering often blocks legit email.
4 Whether it's non-permission or especially on permission
5 given email just because people don't recognize it.
6 Ever-growing suppression lists are becoming very
7 difficult to manage, and consumers need to be educated
8 to not identify permission email that they have signed
9 up for in the past as spam, as a lot of ISPs have made
10 it more easy to identify any messages in their spam
11 filter as spam.

12 That's it. Thank you.

13 (Applause.)

14 MR. HUSEMAN: Thank you, Scott. Okay, Charles
15 Stiles now.

16 MR. STILES: Good morning. I recognize so many
17 of you here this morning. You may know me as Postmaster
18 at AOL, but I am speaking today on behalf of MAAWG as
19 chairman of the board. If you're not familiar with
20 MAAWG, it's an organization of just over 100 companies
21 that are working together to collaboratively fight
22 messaging abuse in all of its various forms, through
23 best practices and white papers, reports, and serving on
24 forums like this, providing information to those that
25 are helping to develop solutions.

1 MAAWG was formed in 2004, and we have a close
2 affiliation with a number of organizations, including
3 the JEAG, the ESPC, which is represented here on the
4 panel today, the Anti-Phishing Working Group, the London
5 Action Plan, and we continue to work collaboratively,
6 and also to develop and work on technologies, and to
7 work with public policy, not as a lobbying organization,
8 but as a resource to those that are helping to make
9 decisions and helping us to combat this problem.

10 Where are we today that we weren't in 2004?
11 Well, I think our mailboxes are probably a lot better
12 off. Our metrics report shows that more consumers are
13 using email, and that we're actually delivering the mail
14 that we should be delivering, while we still block 75 to
15 80 percent of the mail every day that's coming in.

16 What's needed right now is a little bit of time,
17 a little more collaboration, and we will continue to
18 work collaboratively to come up with these solutions and
19 will implement them as industry leaders to fight the
20 problem. That is all.

21 MR. HUSEMAN: Thank you. Let's start off
22 talking about the volume issue of spam, and what's
23 actually reaching consumers' inboxes. Susannah, Pew had
24 some statistics that said that consumers believe that
25 they're actually receiving more spam in their inboxes,

1 but yet at the same time, it's become less of a problem
2 and less of a nuisance. At the 2003 Spam Forum, a big
3 point of discussion was that email was at the tipping
4 point, where we were on the verge of consumers not being
5 able to use email as a tool of communication in
6 commerce, that doesn't seem to be the case now. I would
7 like to ask the panelists what's changed and what are
8 consumers actually experiencing today?

9 MS. FOX: Well, I'll start. The fears were
10 misplaced, luckily. Everyone loves email, it's
11 something that we see popular at every age level. We do
12 surveys down to age 12, and up to our oldest citizens.
13 We love our oldest citizens, because they're often home
14 answering the phone for our telephone surveys, and it's
15 one of the first activities that someone does online,
16 and they continue it. Even teenagers who say that email
17 is mostly for communicating with old people, they still
18 use it.

19 MR. HUSEMAN: What do the panelists think? What
20 is actually the consumers' inbox experience today?

21 MR. STILES: I think the consumers' inboxes
22 today are already benefitting through some of the work
23 that has been done through the government organizations,
24 through the collaboration in the industry, through some
25 of the technology that's been created, developed and

1 deployed. Consumers today are getting spam, but I think
2 had we not put forth the effort that we've done, it
3 would be unbearable, and right now we would be dealing
4 with catastrophe.

5 MR. HUGHES: Our survey earlier this year
6 suggested that consumers are seeing an amount, whether
7 it's more or less, I certainly do believe that there's
8 more spam being sent. I think organizations like AOL
9 and Charles' good work are helping to block a lot of
10 that before it gets to the inbox.

11 I think consumers, though, are also becoming
12 more sophisticated with how they deal with their inbox.
13 Our research showed that they look at the from line and
14 the subject line, and they do that very quickly. This
15 is not sort of a long ponderous analysis, this is a
16 split second analysis, and if there's any indication of
17 spamminess, it just gets deleted.

18 So, I think a big part of the management of this
19 problem, the attitude that Susannah found in her survey,
20 is that consumers have better skills within themselves
21 to cope with the problem, and their service providers
22 and senders are doing better things to help them manage
23 the problem.

24 MR. STILES: Keep in mind that the metrics
25 around this problem haven't existed for very long.

1 MAAWG's metric report has been around now for a year and
2 a half, and up until that time, there wasn't such a
3 report that was that extensive that looked across the
4 entire industry at everybody' mailboxes, currently
5 representing 510 million mailboxes on this report.

6 So, we're just now really starting to put our
7 hands around this problem and understand what the scope
8 is. I think that's difficult for us to look back four
9 years and put numbers and quantify it to four years ago.

10 MR. GRASSO: One of the changes from a law
11 enforcement perspective, something that I am keyed into
12 that I have noticed over the last year or so and I would
13 be interested to hear any of the people that are
14 involved in messaging to comment on this, but I'm seeing
15 less spam that is actually spammertizing something, and
16 more spam that is either phishing or some type of other
17 malicious attack, malicious software, trying to drive
18 somebody to a malicious website that's going to install
19 a virus or a Trojan on their computer.

20 I'm starting to see more of that, and I would be
21 interested over the next two days to hear from different
22 people in the messaging community, your thoughts on
23 that. That's just something I'm biased to, because
24 we're concerned about that stuff and that's stuff that's
25 actually happening right now.

1 MR. HUSEMAN: So, turning to the nature of spam,
2 Tom, as you mentioned, Susannah, what did your study
3 indicate about the types of spam that consumers are
4 receiving now as opposed to four years ago?

5 MS. FOX: Well, I'm also going to be really
6 interested to hear the data from the industry, because
7 what we do is talk to people about their perceptions.
8 So, when they're talking to us on the phone, it's what
9 they remember about their experience, and so what they
10 remember is that for them, phishing has been pretty much
11 at the same level since 2005, but porn spam, the
12 language really changes when you ask people to talk
13 about the spamvertising versus the porn spam, the
14 language gets much stronger and people say things like,
15 it's hideous, women especially really don't like it.

16 Luckily that has gone down. The levels of adult
17 content spam has gone down. Really, most people are
18 seeing it blocked, and what I should have also mentioned
19 is that only about less than half of email users
20 actually check their filters to see if there's any false
21 positives.

22 MR. HUSEMAN: Scott, from the marketing
23 perspective, what do you see now about the nature of
24 spam?

25 MR. RICHTER: We've definitely seen more of a

1 shift in messages as more Fortune 1,000 and larger
2 retailer companies realize that online marketing is a
3 big presence and a big part of their future. We've
4 definitely seen that. As her results show, the
5 marketing messages that are being sent are more consumer
6 oriented, consumer friendly, to the users that the
7 people do have an interest in. It's not just all herbal
8 pills and adult content.

9 MR. HUSEMAN: Charles, what about from your
10 group's perspective, about the types of email, the types
11 of spam that consumers are receiving? How has that
12 changed?

13 MR. STILES: I think that we see that it has
14 become more criminal, but at the same time, our groups
15 have started to realize that you've got to be careful in
16 the aggression that you use in stopping spam, and in
17 fact, the number of tagged or blocked connections per
18 mailbox has dropped over the past few quarters across
19 our metrics report, showing that we're actually looking
20 at the types of messages that our consumers are
21 receiving, and ensuring that the legitimate messages are
22 coming through, because that's just as important, if not
23 more important, than stopping some of the spam.

24 MR. HUSEMAN: Trevor, do you have anything to
25 add?

1 MR. HUGHES: Well, I'm struck by what Charles
2 said, because that is such a change from four years ago.
3 Four years ago, we were rallying arms to fight spam and
4 fight spam only. I think it is an indication that an
5 organization that represents the receivers of the world,
6 MAAWG, and our organization, the ESPC, do work
7 collaboratively now. We recognize that we are joined in
8 this fight, and that the delivery of legitimate mail is
9 as important as the fight against spam, because if we
10 don't protect the good stuff, we are not protecting the
11 very thing that we're fighting for.

12 So, I'm encouraged by the nature of the debate
13 and the discussion there.

14 MR. HUSEMAN: Susannah, did your group or did
15 any of the panelists have information about consumers
16 not receiving messages they want to receive because of
17 aggressive filtering or blocking?

18 MS. FOX: We just had the question about whether
19 you check your spam filter, and it was interesting to
20 see that about more than half of people said no, I
21 rarely check that filter.

22 MR. HUSEMAN: Something that's definitely
23 changed in the past four years is the enforcement focus,
24 the CAN-SPAM Act obviously passed, at the end of 2003,
25 effective the beginning of 2004, and we've also seen our

1 first criminal prosecutions against spammers.

2 Tom, would you talk generally about how law
3 enforcement strategies have developed over the past few
4 years?

5 MR. GRASSO: Sure. So, when we first started
6 looking at the spam problem back in 2003, it was
7 pre-CAN-SPAM, so we didn't have a law on the books that
8 was going to specifically make sending spam illegal, if
9 you were. So, we were looking at it from a different
10 angle. We were trying to look at, well, is there a
11 botnet involved, are there computer intrusions involved,
12 things like that.

13 CAN-SPAM came around, and I have to say, from
14 the criminal side, people weren't really ready to rush
15 into CAN-SPAM, as using it as a tool to prosecute. I
16 think that is not because it's a bad law or anything
17 like that, I think it's because when you have a new law
18 come on the books, prosecutors are reluctant to use it
19 as opposed to something else that they know is tried and
20 true. Okay?

21 I think that's been that way for a long time,
22 it's just common sense. But what we're starting to see
23 now are more CAN-SPAM prosecutions, every day. I'm
24 starting to get more reports from our field offices that
25 they're charging people with title 18-1037, which is the

1 CAN-SPAM Act, so I think it's starting to snowball now,
2 where we're starting to see people get charged with
3 this, we're starting to see successful cases based on
4 title 18-1037, and more and more prosecutors are willing
5 to employ that and use that as a tool.

6 Another thing that I will say is that going back
7 three or four years, we started off with looking at
8 these, the people that we thought were the worst out
9 there, and it took a while to build these cases, and we
10 didn't have some successes right away. We're starting
11 to see those successes now, particularly over the last
12 year or so. We've had a number of arrests, indictments,
13 prosecutions, involving some of the worst spammers. So,
14 I think the law enforcement community and the justice
15 community is starting to accept this, that you can go
16 out and that this is a problem. You can get these
17 people, and you can prosecute them for doing this, and
18 good things will come out of it.

19 MR. HUSEMAN: Charles?

20 MR. STILES: Being a mailbox provider, it's also
21 interesting to note that we don't often times know
22 exactly what it is that's needed by prosecutors to get
23 this information, so MAAWG has been working with law
24 enforcement officials around the globe, not just here in
25 the U.S., to determine what it is that's needed to go

1 after spammers and what information needs to be gathered
2 for what term and how to go about doing that. That's
3 something that continues to go on.

4 We'll be meeting again in October here in D.C.,
5 and look forward to another joint meeting with the law
6 enforcement officials to help other ISPs that are our
7 member companies understand what it is that they need to
8 gather.

9 MR. HUSEMAN: Charles, you mentioned
10 collaboration between partners. What more can we do,
11 what has changed in the past four years and what should
12 we be doing going forward as far as collaborating
13 domestically and internationally?

14 MR. STILES: I think that we really look at this
15 as a problem here in the U.S. I think a lot of times we
16 try to blame those internationally for creating the
17 problem, but we now are looking at this as a global
18 problem, and believing that the solution will come
19 globally as well.

20 We are working with organizations across Europe,
21 and also the Asia Pacific region, to help understand
22 what they're dealing with, share what we've learned,
23 learn what they've solved already, and working with
24 their law enforcement agencies so that we understand how
25 we can cooperate with them in tracking down the

1 spammers.

2 MR. HUSEMAN: Tom, what's your insight on our
3 collaboration with international partners or
4 international enforcement efforts?

5 MR. GRASSO: Well, not everywhere has a CAN-SPAM
6 Act. So, when we're dealing with foreign governments,
7 we'll often times have to take a different angle to it,
8 does it involve a botnet, can you go from the content of
9 the spam, does it involve child pornography or something
10 like that that you can get them interested in.

11 But, yeah, I would say that our international
12 law enforcement cousins out there are the keys to making
13 this happen. The criminal spam is, as someone said
14 earlier, is moving overseas, is coming from overseas.
15 They're using bot networks that are owned by subjects
16 that are overseas.

17 So, it's these relationships that we're going to
18 build with the international law enforcement community
19 that I think is going to be key to the continued success
20 of this. We're working on that every day. My group
21 does a lot of international travel, as much as we can,
22 getting to meet the other law enforcement agencies out
23 there across the globe.

24 There's diplomatic channels that can be gone
25 through, but I think the best thing for us, for me as

1 law enforcement, anyone else in this room that is
2 involved in enforcement, I would say the best thing you
3 can do is develop a relationship with somebody overseas,
4 a law enforcement officer overseas. You are going to
5 get stuff done a lot faster and it's going to be more
6 reasonable the way you're going to get things done as
7 opposed to if you just rely on international treaties
8 and stuff like that.

9 So, it's very important to develop these
10 relationships and know the people you can count on
11 overseas.

12 MR. HUSEMAN: Trevor, we've had two and a half
13 years under CAN-SPAM, what is your view as to whether
14 any additional remedies are needed?

15 MR. HUGHES: Well, gosh, we would like to see
16 regs, that's for sure, the final regs. We're waiting
17 for those on tenterhooks. We certainly have worked very
18 hard on all of the components that have emerged so far.

19 In terms of additional legal remedies, I'm not
20 sure if applying additional legal standards on the
21 legitimate use of commercial email in the marketplace is
22 where the problem is today. It seems to me that the
23 types of problems that we're facing, the crooks, the
24 fraudsters, phishing, we've got lots of law to cover
25 those things. Whether it's FTC Act, whether it's

1 criminal, whether it's at a state or federal level,
2 there is lots of laws to cover that stuff, because it's
3 theft, it's ID theft, it's all sorts of things, it's
4 fraud.

5 So, I'm not sure if additional laws or standards
6 changing or adding to CAN-SPAM is the right way, and in
7 fact I would say that would distract us, perhaps, from
8 some of the more important work. I would much prefer to
9 see more energy, more resources, going into enforcement,
10 so that we can get that deterrent effect. The 6:00 news
11 visual of a phisher with a raincoat over his head coming
12 out of a federal court is a very powerful image.

13 MR. HUSEMAN: Scott, from your perspective, how
14 has the new CAN-SPAM statute affected the marketplace?

15 MR. RICHTER: I think overall, it's definitely
16 helped the marketplace, because it's given us a set of
17 guidelines to follow that we know if we follow we're not
18 breaking the laws. The biggest challenge, like I said,
19 that's been growing, and from our standpoint, since we
20 operate a marketing program on the Internet, is that the
21 suppression list issue, as these suppression lists keep
22 growing, I think it was a great idea at the time, but
23 there needs to be some kind of time limit put on
24 suppressions lists, or a better system figured out.

25 In ten, 20 years, some of these suppression

1 lists will be hundreds of millions of addresses on them
2 that probably 50 percent of them will already be
3 inactive addresses as users change addresses or don't
4 keep the same address for many years or move on from
5 jobs and different stuff. But that's been the biggest
6 challenge with CAN-SPAM that we've seen.

7 MR. HUSEMAN: So, I'll leave time for questions,
8 but let me ask one final topic of the panel. Let's talk
9 about consumer education. Susannah, from your surveys
10 and your statistics, what more should we be doing about
11 consumer education or consumers' awareness. Could you
12 expand on that?

13 MS. FOX: Well, experience is the best teacher,
14 and what we have noticed in the seven years of polling
15 is that the Internet population has matured. Basically
16 we're at a point now where if you're on, you're on, and
17 if you're off, you're off. There's about 15 percent of
18 American adults who are completely disconnected from the
19 network, but most of the rest of us have been online,
20 have been online for a long time and have been dealing
21 with spam and have been learning about how to deal with
22 spam.

23 I actually am not sure how to reach consumers.
24 You know, I don't have expertise in that area, except to
25 say that we do notice that as people do gain experience,

1 they gain a little bit in savvy. What we also worry
2 about and notice is that the spread of broadband, we're
3 now reaching about 50 percent of American households
4 with broadband. With broadband comes overconfidence.
5 Everything moves so quickly with broadband, you think
6 that you're kind of a rock star superhero online, and so
7 you take more chances sometimes. So, that's something
8 to watch.

9 MR. HUSEMAN: Charles, since the nature of spam
10 has changed over the past few years, have we done a good
11 job as a community of keeping up as far as educating
12 consumers about this change? What's your view on
13 consumer education today?

14 MR. STILES: Well, as far as keeping up with
15 spam filtering, I would say absolutely, it's constantly
16 changing and evolving, but as far as educating the
17 consumers, I think it's difficult for us to expect the
18 consumers to understand all the aspects of spam in this
19 type of an environment when we in the industry are
20 trying to put our hands around it as well.

21 MR. HUGHES: I would add to this that I don't
22 think it's necessarily sort of direct education, you
23 don't have to send them a brochure or textbook or make
24 them sit through a panel on spam issues, but I think
25 offering consumers more tools will allow them to engage

1 in and experience that over time they will develop more
2 sophisticated responses to what's happening in their
3 inbox.

4 Again, our surveys suggested to us that
5 consumers would love to have more than just a
6 report-a-spam button in their inbox. They would love to
7 have a report a spam, an unsubscribe, that was safe and
8 trusted, and maybe even a feedback mode that once a week
9 is okay for this type of message, but don't send it
10 twice or three times a week.

11 So, giving consumers those types of tools, I
12 think, leads to that experiential type education that
13 Susannah suggested.

14 MR. HUSEMAN: So, I would like to open up for
15 questions. We have about ten minutes left, and please
16 wait for the microphone so that way the webcast and the
17 court reporter can make sure to hear you. If you can
18 state your name for us.

19 MR. LEIBA: Hi, I'm Barry Leiba, and I have two
20 questions. I'll try speaking up. I'm Barry Leiba, I
21 have two questions, one is about surveys and one is
22 about consumer education.

23 The consumer education one is I find it a little
24 bit odd to consider it a consumer education issue that
25 consumers don't know that they signed up for marketing

1 mail when they bought a product at your website, and I
2 rather look at it as a marketing issue that maybe it
3 should be clearer to consumers that there's an option to
4 get the marketing material and an option not to. So, I
5 would like a comment on that from Scott.

6 And for Susannah, how do you deal with surveying
7 people on cell phones, which is an increasing issue of
8 people who no longer have land lines?

9 MS. FOX: I'll take the survey question quick.
10 It's a big problem for us going forward, but the good
11 news is that we are developing ways to survey people on
12 cell phones. We have done some experimenting with that.
13 It turns out to be very important. In the last election
14 cycle, we did some political polling, the Pew Research
15 Center, with a cell phone only population and actually
16 found that although it skews very young, we are now
17 approaching I think one in four people 18 to 25 who are
18 cell phone only.

19 We didn't notice a change in terms of political
20 affiliations, so that the Pew Research Center was still
21 able to call correctly the last election with a land
22 line survey. That's very different with health surveys,
23 public health surveys find that people who are cell
24 phone only engage in much riskier practices, which I can
25 email you some papers on it.

1 So, we are noticing that there's a big shift, of
2 course, toward cell phone only, but there is success in
3 terms of getting people to answer short surveys. We
4 have to limit it to ten minutes, whereas a land line, we
5 can keep the person on the phone for about 20 minutes.

6 MR. LEIBA: Thanks.

7 MR. RICHTER: In recognition to your consumer
8 education question, I think what the concern is is that
9 a lot of filtering technology is automatically putting
10 mail that people did sign up for and people are aware of
11 it into the bulk folders, and what my concern is is that
12 a lot of these companies have made it very easy, when
13 you do look at your bulk folder, with where you can
14 check all, if it's 50 or 100 or however it's set up, and
15 you just hit submit spam, and a lot of times people
16 aren't reading those messages.

17 Then at the ISP level, they're just
18 automatically saying, well, if you just sent a thousand
19 emails to us and five users reported spam on the
20 automated report button, then you just must be spamming.
21 I think a lot of times what's happening is that the
22 filtering technologies don't really -- you know,
23 obviously it's all computerized and there's a lot of
24 times there's not a human in there looking at them, so a
25 lot of times anything with an HTML link in it, has an

1 image, has a postal address or certain words in the
2 subject line, or the body of the email, are just being
3 put into the spam folder.

4 The biggest thing is then consumers see, oh, you
5 have 100 messages in your spam folder, just click submit
6 all and with the feedback loops that ISPs are offering
7 now, they're just looking at those metrics and a lot of
8 times their metrics aren't changing at the pace that the
9 complaints come in.

10 I just think it's the ISPs, some of them have
11 done a much better job than others, but a lot of them
12 don't do a good job of saying to the user, are you sure
13 this is spam, did you look at the email, are you sure
14 you didn't sign up, it's just check all and submit.

15 MR. LEIBA: Thank you.

16 MR. HUSEMAN: Well, one thing that has changed
17 in the past three years is that my vision has decrease
18 and have more than ten minutes for questions. Trying to
19 see the clock at the back of the room -- so, we have a
20 lot of times for questions and I will intersperse some
21 as well. So, the next question from the audience? Yes?

22 MR. SCHWARTZMAN: My name is Neil Schwartzman,
23 I'm the compliance officer for Sender Score certified by
24 at ReturnPath. I just want to offer some context about
25 the number of complaints from consumers that do block

1 our mail, anyways, the mail that we certify, is
2 certainly not on the order of five complaints. We
3 offer, depending on the volume of the sender, anywhere
4 between 0.4 percent and up to 2.9 percent of the overall
5 email stream before somebody gets blocked, or off our
6 whitelist and consequently possibly blocked at the
7 receiving end.

8 As you know, our whitelist is used by places
9 like Hotmail, many other -- Roadrunner, a lot of other
10 large receiving sites, and I've got to say that it
11 mistypifies the reality of the situation by saying five
12 complaints are going to get you banned. It simply is
13 not true.

14 MR. HUSEMAN: So, one question that I would like
15 to ask is about the technological tools. Specifically
16 about authentication. What steps have been taken since
17 our 2004 summit for email authentication from both the
18 sender's perspective and the ISP's perspective and what
19 else can we do? Trevor?

20 MR. HUGHES: I think there's very good news on
21 the sender side. We require it of our members, the DMA
22 requires it of their members, and we have processes in
23 place to make sure that people are authenticating before
24 we accept their membership application now.

25 We have seen, I would say, qualified success on

1 the receiving side of the equation. One of the things
2 that's been true about the problem that we have here,
3 since the very beginning, is that we have a number of
4 very large ISPs that represent about a half, perhaps
5 even more, of inboxes in the United States, and then
6 beyond that, it is tens of thousands of receiving
7 domains. Think of every company, every university,
8 every small regional ISP.

9 So, we have this sort of split world, where it's
10 very easy for us to talk to the major ISPs,
11 organizations like Microsoft and AOL and Yahoo and are
12 all very much engaged and very much a part of an ongoing
13 dialogue, and are looking at, if not having already
14 engaged in some form of authentication.

15 But that second half of the equation, the tens
16 of thousands of sites out there, or tens of thousands of
17 receiving domains, that's a real challenge for
18 authentication. Authentication really is only a
19 functional tool if it's used on both sides of the chain.
20 If the sender is authenticating your messages properly,
21 then the sever is using that authentication for
22 something, they are using it to determine what goes into
23 an inbox or goes into a bulk mailbox, they're throwing
24 it into a formula with a bunch of other things to
25 determine whether something gets delivered or not.

1 They're doing something with it.

2 And, so, while I think we've seen fairly good
3 traction on the largest ISPs, we're still struggling
4 with a lot of ISPs and we're still struggling with
5 consistency across the ISPs.

6 MR. HUSEMAN: Charles, what's your response to
7 that issue?

8 MR. STILES: I think the good news is that email
9 technology has solidified a great deal over the past
10 three or four years and they have become much more
11 static and constant and people understand them much
12 better than they did. They now know that these are not
13 silver bullet solutions to fighting spam but rather they
14 are components to a larger set of tools that will help
15 us to combat spam.

16 From the ISP's perspective, your biggest win is
17 of course getting the large ISPs to implement
18 authentication technologies. The bad news is that when
19 you deal with the largest mail systems, you're also
20 talking about the most complex implementations. Over
21 the last quarter, you're looking at 510 billion messages
22 that need to be evaluated for this type of
23 authentication. So, that's a lot of work that needs to
24 go into our infrastructure.

25 Now, the good news from that is that most ISPs

1 are looking at authentication or actively working at
2 implementing and I suspect you will hear more about
3 different ISPs putting those systems into production.

4 MR. HUSEMAN: Scott, what's your view on email
5 authentication, and in the marketplace, what is
6 occurring?

7 MR. RICHTER: We've done tests, most of our mail
8 we do use it on, and some of our mail we don't use it on
9 all the time. You know, one thing we've noticed is that
10 with email authentication sometimes is that if somebody
11 has written rules against it, it obviously blocks all
12 the mail you send immediately, and we believe that
13 sometimes they're not blocking the mail because there's
14 anything wrong with it, maybe a filtering company has
15 wrote a rule against our postal address, wrote a rule
16 against something in the email.

17 So, I believe that it has some benefits if ISPs
18 are honoring it like they say they want to, I think it's
19 very beneficial. If ISPs are just using it to pinpoint
20 certain organizations not to accept their mail faster,
21 then it's a negative impact.

22 MR. HUSEMAN: Tom, can you talk about the
23 interplay between enforcement and technology, what
24 technological developments have occurred that maybe have
25 helped our enforcement strategies or helped our

1 investigations or what more could we do?

2 MR. GRASSO: Well, I think first and foremost,
3 it is the authentication services that are out there,
4 the people that are filtering the spam, and providing
5 that service to their customers, also have some great
6 data available to us in law enforcement as to the amount
7 of spam and where it's coming from.

8 So, if we get to the point where we're targeting
9 a specific spammer and we want to know, we need to reach
10 those levels that are defined in CAN-SPAM, it's the
11 different authentication services that can provide us
12 with that data. You know, we can show them a piece of
13 spam and they can say, yeah, this was a thousand copies
14 of this tried to hit our customers' mailboxes over a
15 couple of minutes the other day.

16 So, that's really valuable information that they
17 can provide to us.

18 MR. HUSEMAN: An issue that Susannah addressed
19 was about the sexually explicit spam messages. What
20 changes have we seen in the past four years with that,
21 and, Tom, if you can start out with the law enforcement
22 perspective.

23 MR. GRASSO: So, I can say that there was a
24 recent case out of Phoenix, which I think a lot of
25 people are familiar with, FTC was involved in the case,

1 and resulted in some successful prosecutions of some
2 individuals that were charged with not only CAN-SPAM
3 violations, but also charged with obscenity violations,
4 just because of the nature of their spam was clearly
5 obscene and bestiality, things like that, it wasn't your
6 typical type of adult spam.

7 So, yeah, it's still a problem, it's out there.
8 I think from the government's side, we're willing to
9 look at it from whatever angle we can, whether it be a
10 CAN-SPAM violation or an obscenity violation. I think
11 this is the type of spam that bothers consumers the
12 most. You know, especially if it's obscene, if it
13 involves one of your kids is opening it in their
14 inboxes, this is the stuff that really bothers people,
15 and in fact, what is CAN-SPAM? It's controlling the
16 assault of nonsolicited pornography, yeah, so I mean,
17 CAN-SPAM was geared at this problem and I think this is
18 what bothers people the most.

19 MR. HUSEMAN: Tom, we have a question from the
20 audience for you as well, what is the NCFTA and how do
21 we get involved and are they focused on issues other
22 than spam?

23 MR. GRASSO: Absolutely. The National Cyber
24 Forensics and Training Alliance is a 501(c)(3) nonprofit
25 entity, it's based out of Pittsburgh, and the best way

1 to summarize it is that it's a neutral ground where law
2 enforcement and industry can come together and work on
3 cybercrime problems. We do not only work on spam.

4 Spam was the first initiative started at this
5 project when it was brand new back in 2003, but since
6 then, we have got into all sorts of other things,
7 phishing, stock fraud, which ties into spam, of course,
8 as you all know, pharmaceutical, online pharmaceutical
9 fraud, basically anything, any type of cybercrime that
10 is a big problem for the Internet community and for
11 industry, that's what they work on at this facility.

12 And what's nice about it is that I get to come
13 to work every day and sit down and work side by side
14 with analysts from industry. There is no walls up, no
15 barriers, we work together. We collaborate on these
16 cases together, roll up our sleeves and work on them,
17 and it's extremely refreshing for me, coming from a
18 government background, to be in that type of
19 environment, and it's also extremely beneficial for us
20 to be able to be working with these great people from
21 industry that have all sorts of fantastic data that they
22 want to share with us on the problem.

23 As far as if you want to become involved in the
24 project, you can talk to me about it, our CEO, Ron
25 Plesko, happens to be here, he was here, is Ron still

1 here? Nope, okay. Our CEO of the NCFTA is here, but we
2 do have a website, www.ncfta.net, and you can get more
3 information about the project there.

4 MR. HUSEMAN: So, one of the questions from the
5 audience, go ahead.

6 MR. ZWILLINGER: Mark Zwillinger, I'm from
7 Sonnenschein, Nath & Rosenthal. Just a quick question,
8 defining the problem area, we know the FTC is very
9 concerned that one of the problems is inadequate
10 supervision of affiliates, and to what extent an
11 advertiser is responsible for the activities of the
12 affiliates who send the emails on their behalf, and so
13 the question I guess is geared to Scott as someone who
14 runs an affiliate network, I'm interested in your
15 position and to what extent an advertiser should control
16 the action of the affiliates and I also wanted to hear
17 from Trevor whether that view is consistent with how the
18 ESPC looks at sort of affiliate control and supervision.

19 MR. RICHTER: As far as our affiliates go, when
20 they join our program, obviously they agree to the terms
21 and conditions, part of the terms and conditions is that
22 they don't break any laws and that they'll follow
23 CAN-SPAM. Some of our individual advertisers have
24 different rules on top of our terms and conditions.

25 Obviously they have to follow suppression lists

1 and different programs, stuff like that, but it's
2 definitely tough. At any given time if an affiliate of
3 any network or for any advertiser does something
4 unauthorized, we usually, we're very good about taking
5 immediate action, and usually what we will do is we will
6 immediately disconnect the links and have the links go
7 to a page saying this affiliate has been terminated, if
8 they've done something wrong, so at least that way
9 nobody is taken advantage of and they know that action
10 has been taken.

11 MR. HUGHES: I think the affiliate issue is a
12 very big issue, and I think we probably should spend
13 time talking and thinking about it. Former FTC
14 commissioners describe this as the problem of cascading
15 trust, that an advertisers gives a message to an
16 affiliate network, to an agency, to a partner, and then
17 they pass it and then they pass it and then they pass
18 it, and if it's a cost per conversion type campaign, if
19 they're getting paid, if there's a sale, everyone takes
20 a piece of that commission all the way back up.

21 The problem is as that connection between the
22 advertiser and the delivery of the ad to the consumer
23 becomes more attenuated across that network, that
24 affiliate chain, the ability of the advertiser to know
25 how it's actually being presented and how it's being

1 sent to the consumer is essentially gone. While
2 contractual provisions are the predominant mechanism for
3 an advertiser to try and gain some control, I don't
4 think we have seen a lot of auditing and accountability
5 from advertisers in terms of really getting out there
6 and managing how their messages are being perceived in
7 affiliate networks.

8 And I worry, I worry that advertisers not only
9 may be exposing themselves to legal risks because under
10 the CAN-SPAM Act, one of the more inspired policy
11 choices was that the sender of the messages, the
12 advertiser, within the message, not the company that hit
13 send, but the advertiser, within the message, the
14 advertiser can be on the hook for those practices of
15 that terminal end of the affiliate chain actor, and
16 those practices may be pretty nefarious.

17 So, I think that there certainly is room for us
18 to be looking at those practices. We don't have best
19 practices in that space, but it's certainly something
20 that we talk about quite a bit with our members.

21 MR. HUSEMAN: Charles, another question about
22 what's on the horizon? We've talked a little bit about
23 what's changed? Now we're hearing about image spam, PDF
24 spam, and technologically, what are we doing to look
25 ahead and prepare for the next evolution?

1 MR. STILES: Really we've just got to keep our
2 eyes open, and it's something that evolves and changes,
3 not only a day-by-day, but on an hour-by-hour basis, and
4 as we continue to see these changes come up, we find
5 different ways of combatting them.

6 What's the future hold? I don't know. I don't
7 think any of us can know for sure. I suspect that
8 botnets are going to continue to be a problem for quite
9 some time, because spammers have moved from the basement
10 into our own living rooms and taken over our own PCs. I
11 think that that's going to pose a problem for us for
12 quite some time.

13 Now the method they use for delivering their
14 message, whether it's image, whether it's an
15 application, whether it's PDF files, that remains to be
16 seen.

17 MR. HUSEMAN: Does anyone else have any thoughts
18 on that?

19 (No response.)

20 MR. HUSEMAN: Tom, if you can speak
21 specifically, have you contacted, when you've contacted
22 consumers whose computers have been compromised, I mean
23 I assume they're often unaware of that. What's been the
24 reaction?

25 MR. GRASSO: They're usually unaware. They say,

1 oh, boy, I noticed it's been running slow lately, so
2 that's the complaint that you get. But they're often
3 unaware of what exactly is going on. The computers that
4 are being co-opped to do this stuff, the malware is
5 really good at hiding itself. Easily from your average
6 user, but even sometimes from people that are computer
7 experts.

8 So, these people don't know it's on their
9 computer, they just know it seems to be operating
10 slowly, and that's mostly because their Internet
11 connection is the bandwidth has been soaked up with all
12 the spam that it's blasting out.

13 So, what we try to do is with the help of our
14 industry partners, obtain permission, authorization,
15 from the user to monitor that computer, to get them to
16 run some forensic tool that some of our industry
17 partners have developed that they can easily put on
18 their computer, create a report, give that information
19 back to us to show, yeah, okay, this computer is
20 infected with something, but who is it talking to, where
21 is it getting its commands from. That's what we're
22 interested in.

23 But to answer your question, yeah, they often
24 don't know until they get a call from us or from the
25 ISP.

1 MR. HUSEMAN: Do we have some questions from the
2 audience? Please wait for the microphones.

3 UNIDENTIFIED SPEAKER: This is a question
4 strictly as a computer user, my computer may be
5 compromised, can I contact you, is there something that
6 I can send to you or something that you send to me to
7 help me know whether I can find out?

8 MR. GRASSO: Okay. Well, there's a number of
9 websites out there that can help with this, and the
10 first one that comes to mind is a really great industry
11 partner of ours, Lawrence Baldwin, he has a website
12 called myNetWatchman.com, and if you go onto that
13 website, you'll see they have a tool on there called
14 SecCheck, and that's something you can download and run
15 on your PC and it will look for malicious software, for
16 signs of infection on your PC, and then it sends that
17 information back to Lawrence and he keeps all that in a
18 database that he can share with law enforcement if we
19 need it and things like that. That's one thing to do.

20 Joe, can you think of anything, any other sites
21 that are good at that?

22 MR. ST. SAUVER: Lawrence's site is certainly
23 one of the best.

24 MR. HUSEMAN: Can we have the microphone?

25 MR. GRASSO: This is Joe St. Sauver from

1 university of Oregon.

2 MR. ST. SAUVER: Lawrence's site is certainly
3 one that I would recommend, but I will say that there
4 are also many other industry partners out there who have
5 good tools, many of the anti-virus companies offer free
6 anti-virus fix that will take care of some of the
7 malware that may be on your computer, and there are
8 increasingly anti-root kit tools that are also
9 available. Google has many of those tools and will make
10 them available to you.

11 MR. GRASSO: Here's the problem, and in fact,
12 that the work that we're doing on law enforcement end,
13 we're undercover and we're in these different forums
14 where the virus writers are hanging out, they're writing
15 malicious software and they're marketing it on the fact
16 that it's not detected by any of the virus definitions
17 yet, okay, so they're writing this stuff, and they test
18 it against all the popular AV software, and then they
19 advertise, hey, I just wrote this new virus, it's not
20 detected by anything, who wants to buy it from me, okay?

21 So, this is part of the problem. So, it's kind
22 of like, I guess to answer your question, it's like a
23 catch-up game. You have to keep checking your machine
24 and if something is on there it's probably going to get
25 detected, maybe not right away, and I think that's

1 probably the best thing that you can do.

2 MR. HUSEMAN: Some more questions from the
3 audience? Yes?

4 MR. RAMASUBRAMANIAN: My name is Suresh
5 Ramasubramanian and I manage the spam operations for
6 Outblaze, we are a Internet provider.

7 MR. HUSEMAN: Can you speak up just a bit, sir,
8 please.

9 MR. RAMASUBRAMANIAN: My name is Suresh
10 Ramasubramanian and I manage the Antispam Operations for
11 an outfit called Outblaze and I would like to point out
12 one fundamental thing that a lot of the panel has been
13 discussing, but with authentication is pretty good in
14 its own right, but while we are looking for a cure for
15 all spam, or we are recommending that, for example,
16 email marketers use authentication to declare that the
17 mail is coming from a particular IP space, it's usually
18 kind of limited in this area, because while it creates
19 much more standardized way for us to know where a
20 marketer's email is coming from, quite often, if a
21 marketer gets blocked, he's getting blocked because of
22 complaints from his own actions, shall we say, from
23 email that he sends out.

24 It's not like where it's a bank or a financial
25 institution or something that is getting impersonated by

1 people sending from botnets and, for example, ebay and
2 PayPal and I'll safely say that we sign all of our email
3 with domain keys, and if you see email that claims to be
4 from us and it's not signed by us, feel free to trash
5 the email.

6 So, I'm looking at how useful authentication is
7 for a marketer beyond just declaring to an ISP that we
8 are going to be sending from this range? They are
9 normally sending from that range and they are reasonably
10 static sources, it's not like they skip around from
11 China to Brazil or to India to somewhere else and it's
12 just like a botnet. So, how useful is authentication
13 beyond that?

14 MR. HUGHES: So, I can respond to that. Hi,
15 Suresh. We never saw authentication, the ESPC has never
16 seen authentication as a silver bullet, we have seen it
17 as a dispositive mechanism for deliverability into the
18 inbox, and certainly it has not become that in the
19 marketplace today. But we do see it as one factor that
20 can be used by ISPs in their broader mix of factors to
21 determine what should go to the inbox or the junk box or
22 be blocked outright.

23 It's one more indicator that the legitimate
24 marketplace is acting competently and consistently, and
25 that is what helps to engender trust. I think over the

1 past four years, we have seen particularly on the issue
2 of email authentication, that the sending community and
3 the receiving community have found common ground to talk
4 about many of these things and that's led to greater
5 trust and greater discussions on all sorts of stuff.

6 So, we've never seen it as a silver bullet, your
7 points are very well taken, that for marketers it's not
8 dispositive of inbox delivery and should not be seen
9 that way. I still say, though, and we still require
10 that our members and that any marketer that's trying to
11 do things the right way should be authenticating their
12 messages.

13 MR. STILES: I think you need to make sure that
14 you look at authentication as a key component to a
15 reputation system. Authentication by itself doesn't
16 mean that you get a pass or a fail, it's really about
17 attributing a reputation and we need to remember that
18 reputation can be both good and bad.

19 So, the benefit to a marketer is to be able to
20 rely on their good reputation and bring up new IP
21 addresses which he may not have mail for or be mailing
22 under perhaps a different name than what they've mailed
23 from before and benefit from that positive reputation
24 and the good practices that they've upheld to that
25 point.

1 MR. SPIEZLE: Craig Spiezle from Microsoft. I
2 want to follow up on that comment, and again,
3 authentication is the first part. It's a driver's
4 license, and reputation, as Charles mentioned, is very
5 important, and that's the driving record. Sorry, I'll
6 speak a little louder.

7 So, but specific to the point there, so what
8 we're finding today, with marketers who authenticate and
9 have good reputation, actually their false positives
10 have decreased 85 percent, and the reason is, it gets
11 into the mix that Trevor mentions, is we're able to take
12 the result of a good reputation and apply that to the
13 mix, and so an example of a bank or a financial
14 institution, their mail may get junked because the
15 content with the financial data, their positive
16 reputation could override that and make sure it's
17 delivered. But we have a key success there.

18 The other part I think I want to challenge is
19 that while it's great that marketers are doing this, we
20 need to go a step further and get the brand owners and
21 the domain at the higher level. It's not just about the
22 email marketing domains, it's about authentication and
23 reputation, it's protection from the deceptive and the
24 forged mail which is coming from other sources.

25 MR. HUSEMAN: I have a question from the

1 audience. Botnets are recognized as a tremendous
2 problem, are ISPs quantifying the number of botnets on
3 their network or the percentage of users, and are they
4 taking steps to remedy the problem?

5 MR. STILES: Just speaking on behalf of MAAWG,
6 we do recognize it as a problem, we do have a botnet
7 subcommittee that's evaluating the situation. We have
8 not released any metrics on botnets specifically, and
9 the extent to which we resolve a botnet problem really
10 varies from ISP to ISP, because there are a significant
11 number of resources that are required for resolving
12 that. Everything from walled gardens, actually making
13 consumer calls out to the customer, even home visits,
14 and it really varies from ISP to ISP.

15 But yes, it's recognized, it is being dealt
16 with, and is being evaluated even further to see how we
17 can combat it more effectively.

18 MR. HUSEMAN: Tom, in the law enforcement
19 experience generally, what has been the prevalence of
20 botnets in your investigations?

21 MR. GRASSO: They play into just about all of
22 our cybercrime investigations in one way or the other.
23 I mean, this is what the criminal spammers are using to
24 send their spam out, they're not sending it from some
25 mail server that they own somewhere, they're sending it

1 through a botnet to hide where they're coming from. The
2 prevalence of botnets is increasing, their
3 sophistication is increasing and the size of them is
4 also increasing.

5 Microsoft has a project that they call the
6 Botnet Task Force, which I know all the Microsoft folks
7 here are familiar with, which they've put together
8 that's enabled us in law enforcement to team up with the
9 different industry folks and attack this problem. Now,
10 I think the official Botnet Task Force meeting is going
11 on right now down in Australia, so I don't think there's
12 anyone here from the Botnet Task Force, but does anyone
13 from Microsoft want to comment on that, what you have
14 seen through that initiative? Or I have the wrong
15 people here, okay, I'm sorry.

16 No, it's on the rise. But we're getting better
17 at identifying these and detecting these and sharing the
18 information as to where they are and some of the ISPs
19 are really good at getting them shut down, too, when a
20 command and control mechanism is identified, they are
21 getting really good at pulling the plug on that and
22 getting it shut down.

23 But there's guys out there, and just so you
24 know, these botnets are not deployed by the spammers
25 themselves, there's guys out there that this is what

1 they do for a living is they build these botnets and
2 they build them by sending you an email message that's
3 got a link to a malicious site, you go there and your
4 computer gets infected and now you're a bot, okay, and
5 you're reporting back to this guy's command and control
6 server.

7 Now, what he does then is he sells time on that
8 bot, okay, kind of like how in the old days you had to
9 pay for time to use the computers and stuff like that.
10 Okay, he will sell you like a week on his botnet, he
11 will sell you two weeks, whatever you want to use and
12 you've got his botnet to send out whatever you want.
13 You can spend out spam with it, you can D-DOS someone
14 with it, whatever you want to use it for, it's there for
15 you to use. But these guys build these and then they
16 sell time on them. It's a business for them.

17 MR. HUSEMAN: Other questions from the audience?
18 Yes?

19 MR. FENTON: Hi, I'm Jim Fenton. Scott Richter
20 mentioned in his remarks that one of the issues that
21 he's seeing in terms of deliverability is consumers who
22 have, in fact, opted into receive some messages, having
23 forgotten about that and hitting the spam button when
24 they receive these messages. Do you see a need to
25 increase the stringency of opt in, perhaps to double opt

1 in or something like that, either as a best practice or
2 as a requirement in order to avoid that problem?

3 MR. HUGHES: I'm happy to answer that based on
4 some research that we did earlier this year and I
5 actually want to mention a tool that Microsoft has
6 created as well. What our survey found earlier this
7 year was that consumers use the report-a-spam or
8 complaint button as a single button, as the only tool
9 available to them to respond to something that maybe
10 they asked before, but they don't want anymore, and
11 they're not as frequently using the unsubscribe function
12 found in the email itself. In fact, we may have created
13 that reality, because for many years, the marketplace
14 was telling consumers, don't unsubscribe from emails,
15 you're just verifying your email address for the
16 spammers so you will get more.

17 So, consumers at least have that legacy of
18 knowledge that okay, I'm not supposed to unsubscribe
19 from the email itself, but my provider, my email client
20 has given me a button here that says report a spam and
21 I'm smart enough, knowing my email client, that when I
22 hit that button, I know that that means that I don't get
23 stuff from that sender anymore. I don't know if that's
24 blocked, I don't know if people go out and arrest that
25 person, but I know it doesn't get into my inbox anymore

1 and that's okay.

2 So, frequently they're not reporting it as spam,
3 they're just using it for the de facto result of what
4 happens when they hit that button. We think that
5 consumers need more tools.

6 So, I wouldn't put the solution on the consent
7 part of the process, because the consent process seems
8 to be working well. The consumer knows that they asked
9 for it, they just need a better way to say they don't
10 want it anymore. So, we applaud Microsoft as being one
11 of the few ISPs that's actually implemented an
12 unsubscribe button.

13 So, it is helpful for consumers to be able to
14 distinguish between reporting something as spam and just
15 saying I don't want this stuff that I asked for before,
16 I just don't want it anymore.

17 So, I would encourage more ISPs to move in that
18 direction as opposed to us looking at the consent side
19 of the equation.

20 MR. HUSEMAN: So, I would like to go down the
21 list of panelists and ask you all the same question. If
22 you could briefly define, summarize, what is the problem
23 today, and how has it changed in the past four years?

24 MS. FOX: I would say the problem is the loss of
25 trust in email that we consistently find that people say

1 that spam is making them trust email less, and so I
2 would say that's the major problem from our perspective.

3 MR. GRASSO: What Susan said, yes. No,
4 absolutely. I think it's diminishing the trust of
5 email, its usefulness as a business tool, these are all
6 being affected by the spam problem. How it's changed
7 over the four years just to reiterate some of the stuff
8 I said earlier, at least from what I can tell, it seems
9 to be more about malicious software, phishing scams,
10 other types of things other than just, oh, hey, we've
11 got a product that we want to sell you. There's like a
12 lot of other stuff going on behind it, manipulating the
13 stock market, things like that.

14 So, we've got a whole host of other bad things
15 that spam is being used for where I think at one time it
16 was just about marketing stuff and I don't think that's
17 the way it is anymore.

18 MR. HUGHES: So, I am going to agree with
19 Susannah and Tom. I think four years ago we had this
20 big, ugly bucket of all sorts of things that were going
21 on, malicious activity, things that were sort of early
22 forms of phishing, but also the mainstream marketplace
23 didn't have standards, didn't have a lot to look to
24 really, we had all sorts of state things that were being
25 applied to us.

1 What I think we have changed in the past four
2 years is the legitimate email community has recognized
3 the need for it to protect email as a whole, and the use
4 of legitimate email as a subset of that whole, and they
5 have pulled themselves out of that ugly bucket of mess
6 and have developed standards, the best practices that we
7 have, we've developed technological tools, like
8 authentication and replication systems and there is
9 broad compliance with the CAN-SPAM Act.

10 That leaves, I think those things that Tom has
11 described, the more malicious, fraudulent criminal
12 activity as being major problems for us. That's not to
13 say that there's still not work to be done, and in fact,
14 I think one of the interesting things that's changed
15 over the past four years is that as we have brought sort
16 of mainstream email into the bright light of day and
17 given them standards and they are adhering to those
18 standards, we found that, and there's probably 20 or 30
19 of them in this room, that we need deliverability
20 experts to actually manage email for big companies now,
21 and many of our members provide those services to their
22 companies, the folks who participate on our calls are
23 the VPs of deliverability, directors of deliverability,
24 who have within their realm of responsibility compliance
25 with the law, technological updating and compliance with

1 technological standards, and actual relationships with
2 some of the bigger ISPs, talking to people like Charles
3 on a regular basis.

4 So, it is a much more professional, much more
5 sophisticated business environment today with still some
6 of these criminal and malicious threats on the fringes
7 that cause us all great concern.

8 MR. HUSEMAN: We just have a couple of minutes,
9 so Scott just briefly.

10 MR. RICHTER: I agree with what Trevor said, and
11 as the landscape changes more and more and what's
12 happened over the last couple of years going forward, it
13 definitely makes it much easier having guidelines and
14 rules to follow, the only downfall is that legitimate
15 email marketers still do get mixed up with people who do
16 phishing or malicious stuff, and until a lot of
17 filtering companies can understand the difference, it's
18 quite challenging because unfortunately, legit marketers
19 pay the price for it because it's easy to identify now
20 that it is identifiable, versus mail that does come off
21 of the bot networks.

22 MR. STILES: Bulk is still a four-letter word,
23 but it's not a bad word, so that's probably the biggest
24 change that's happened over the last couple of years.
25 Legitimate marketers don't have to be skeptical about

1 disclosing where they're mailing from and what they're
2 mailing and there's a collaborative effort between them,
3 and the spamming activity has moved literally from
4 teenagers trying to make a quick buck in the basement to
5 actual criminals who have lots of resources globally and
6 will stop at nothing to deliver their messages.

7 MR. HUSEMAN: I would like to thank all of the
8 panelists and we will reconvene again at 11:00 a.m.

9 (Applause.)

10 (Whereupon, there was a recess in the
11 proceedings.)

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1 EVOLVING METHODS FOR SENDING SPAM AND MALWARE

2 MR. HODAPP: If everyone would take their seats,
3 we would like to get started. If people could please
4 take their seats so we could begin with the panel. The
5 longer this takes, the later lunch will be. Or maybe no
6 lunch.

7 Okay, just less than a minute.

8 Okay, I would like those of you who perhaps have
9 unmuted your cell phones or wireless devices to mute
10 them again, please. This is the second panel of the
11 morning on the evolving methods for sending spam and
12 malware. My name is Lawrence Hodapp, I'm an attorney at
13 the Federal Trade Commission. The case I've done that's
14 the most pertinent here is the case against William
15 Dugger who the chairman mentioned in her remarks.
16 Dugger was using a botnet to send sexually explicit
17 spam.

18 The goal of this panel on evolving methods for
19 sending spam and malware is to highlight this
20 interrelationship between malware and spam. So, we'll
21 be talking about the more criminal variety of spam that
22 was discussed in the first panel. Not only do we want
23 to try to discuss the status of the methods being used
24 today, we also want to try to give you some of the
25 factors that we think may govern the evolution that's

1 occurring. What are the pressures?

2 We have an extremely well qualified panel to
3 discuss these issues. I will mention some of their
4 affiliations, but you understand that the views
5 expressed are their own and not necessarily those of
6 their organizations.

7 First here is Patrick Peterson, Patrick is vice
8 president for technology, IronPort Systems of San Bruno,
9 California. IronPort provides security products and
10 services for web and email. Patrick works in the
11 development of these solutions and is a frequent speaker
12 at industry events and a writer on security issues.

13 Next to him is Joe St. Sauver, Joe is the
14 manager of security programs at Internet2 on contract
15 from the University of Oregon. He is also a senior
16 technical advisor to the Messaging Anti-Abuse Working
17 Group.

18 Next to him is Jon Praed. Jon Praed is an
19 attorney and a founding partner of the Internet Law
20 Group of Arlington, Virginia. Jon has represented AOL
21 and Verizon in some precedent-setting litigation that
22 has held both spammers and the websites that employ them
23 liable, including monetary liability, which is of course
24 the best way to make them aware of the need to comply
25 with the law.

1 Next to Jon is Ben Butler. Ben is the director
2 of network abuse for GoDaddy.com of Scottsdale, Arizona.
3 GoDaddy is the world's largest domain name registrar and
4 also a major provider of web hosting. Ben has a
5 background in network and email administration and he
6 directs GoDaddy's zero spam policy.

7 Next to Ben is Suresh Ramasubramanian. Suresh
8 is the manager of anti-spam solutions for Outblaze
9 Limited in India.

10 MR. RAMASUBRAMANIAN: Hong Kong.

11 MR. HODAPP: I'm sorry, Outblaze is based out of
12 Hong Kong?

13 MR. RAMASUBRAMANIAN: For now, I am working at
14 home, I have a small kid to take care of.

15 MR. HODAPP: You don't have to work where the
16 company is these days. Outblaze is the largest provider
17 of email in the world. Suresh is responsible for the
18 spam filtering and blocking decisions that affect their
19 40 million email accounts. He was highlighted in
20 Business Week in 2002 as one of the 25 top e-business
21 professionals where they dubbed him the chief junkmail
22 zapper.

23 The panel has decided to proceed with three
24 presentations, after which we will have a substantial
25 amount of time to discuss the topics raised in those

1 presentations. Starting with Patrick Peterson, then Joe
2 St. Sauver and then Jon Praed. There's cards in your
3 packet that you can fill out and will be sent forward,
4 in addition to having questions and answers from the
5 floor at the end of the presentations. Likewise, people
6 on the webcast can submit their questions as described
7 earlier.

8 Now, Patrick, if you want to go ahead, we'll
9 proceed.

10 MR. PETERSON: Thank you, Lawrence. I'm very
11 excited to be here with what is certainly going to be
12 the best panel of the FTC Spam Summit, I'll just lay it
13 down right now. I should also make one other mention,
14 my owners are here, that is to say Cisco Systems, and
15 the transaction to acquire IronPort closed between when
16 I was invited and now, so I want to make sure that my
17 new owners get the credit for now owning IronPort
18 Systems, but as Lawrence mentioned, we had a bit of a
19 struggle with this panel. He got together with us, he
20 explained what he was looking for and he explained very
21 much that he wanted people who didn't have Ph.D.s in
22 spam to get a lot out of it, but he didn't want the
23 people with Ph.D.s in spam to be bored.

24 And so we went off, talked about a lot of things
25 and came up with a lot of great ideas and came up with a

1 really good solution for him. We said, our panel right
2 now is at one and a half hours, if we could have one and
3 a half days, we could really do justice to these topics.
4 So we came up with a compromise, I think he cut out like
5 30 seconds of his intro and we came up with this
6 alternative method. What the alternative method is is
7 that I am going to spend about 12 minutes and I am going
8 to do the training wheels version.

9 This is going to be the framework for
10 understanding maybe not simple but more basic things,
11 and the idea is that that will become the framework on
12 which a lot of the panelists will riff and go into a lot
13 of the more complicated, interesting things.

14 So, let me begin with this slide. I believe
15 that if we look at all of these complicated issues to
16 the right lens, it gives us a tremendous advantage in
17 really understanding the issues. This is the lens that
18 I use.

19 First of all, capitalism. Spammers today are
20 capitalists and they are very talented and genius, they
21 may be evil criminal, but they are talented and genius
22 capitalists, and what they are doing is designed to
23 maximize their profits. In particular, we are going to
24 use some examples throughout my training wheels
25 presentation from a group that I call My Canadian

1 Pharmacy, also known as the Yambo gang.

2 We estimate that they are doing over \$100
3 million in profit today from illegal pharmaceutical
4 products. Clearly you don't get to that scale of
5 business and stay out of the arms of law enforcement
6 unless you're pretty darn good at knowing how to make
7 money.

8 The second thing, of course, then, is if you
9 want to make money in spam, you've got to get it in the
10 inbox. The third thing is that once I, if I were
11 spammer, get it to the inbox, the next thing I have to
12 do is to actually have you take action, to get your
13 money, to infect your PC, what have you.

14 Again, so far, so good, it sounds simple. The
15 problem is, it gets very complicated, for the reason
16 listed on the slide. Spammers are actually operating in
17 an incredibly hostile environment. We're trying to
18 block their mail, we're trying to shut down their
19 servers, we're taking down their websites, trying to put
20 the handcuffs on them, trying to shut down their
21 affiliates.

22 And unfortunately, they haven't said, boy, this
23 is a pretty tough gig, we're going to give up and go get
24 a day job at Starbuck's or McDonald's or wherever it may
25 be, they have responded by adapting, and they have

1 adapted incredibly richly and quickly, which means that
2 a lot of these things which look straightforward can be
3 very complicated because of the way that they are
4 innovating.

5 So, this is our training wheels version of the
6 framework for understanding the spammers on which we
7 will kind of base the more advanced conversations. The
8 first three items are how they deliver the mail. They
9 need your email address, if they want to get it in your
10 inbox, they need the content and they need some way of
11 firing lots and lots and lots of these messages out, and
12 of course today they're using bots.

13 Items four through six are the actual action.
14 They need you to respond to that spam, it may be to buy
15 a stock, it may be to go to a website, it may be to call
16 a phone number for a diploma, but they need you to take
17 action. So, they need some kind of infrastructure for
18 that, and in some cases spam actually has a payment
19 directly to the spammer or the affiliate, and in other
20 cases they actually deliver product, and so in some
21 cases they need those as well.

22 Now, again, I'm going to try to keep it very
23 simple and basic. I know a lot of the people with
24 Ph.D.s are going to be raising their hands and saying
25 that's oversimplifified, but I think Joe is going to have

1 a pretty amazing presentation where he is going to put
2 together the way the eco system really works that they
3 have adapted to add a lot more color to this.

4 So, start with the top three methods of which I
5 have listed four here, for those of you who are
6 proofreaders in the audience. The first thing you can
7 do is you can go online and you can Google or Yahoo or
8 Microsoft search for email addresses and you can find
9 people will sell 40 million email addresses for \$40.

10 The second thing you can do is if you're a bad
11 guy and you've compromised someone's PC and are running
12 software, you can just grab the address book of all the
13 people that they email to and that's a nice list of
14 email addresses that allows you then to send email and
15 make sure it gets put in someone's address box.

16 Directory harvest attack is another technique
17 and I am going to talk about that in more detail, and
18 last but not least, you can go to a website and if
19 someone has an email address on that website, you can
20 actually purchase a tool, again online, very easy to
21 find, through search. A tool that will go out, spider
22 the web and come back with all of the email addresses on
23 the Internet or perhaps just targeted ones for the
24 people who are most likely to buy your product.

25 Since often times I think the directory harvest

1 is discussed and then maybe not well understood, I would
2 simply give a very simple example of how the directory
3 harvest works. The way I thought would be best to
4 explain it was actually to give a postal mail example of
5 how this would work if spammers wanted to get postal
6 mail addresses.

7 So, in this case I have hypothesized that a
8 spammer really wants to know who is actually working at
9 the Federal Trade Commission, so that they can send them
10 lots of bulk postal email. So, in this case, they may
11 put together a bunch of names and addresses like these,
12 pop them in the mailbox and go on vacation for a week.

13 When they come back, they may find that their
14 mailbox at P.O. Box 666123 Spammer Court in the Ukraine
15 has a bunch of mail that was sent back to them because
16 it was undeliverable. It turns out there's no Deborah
17 Jones, Jim Smith, James Jones or Lawrence Smith,
18 hypothetically speaking, working at the FTC, so the FTC
19 sent those letters back to the spammer.

20 What the spammer then does is he puts the two
21 together, knows what he sent, knows what came back, and
22 the difference is real people who work at the Federal
23 Trade Commission and the next time you mail to those six
24 people, you know that it's going to be delivered.

25 This is exactly the same thing that they do in

1 the email world. They actually have a server, it's a
2 bot, and it may be my uncle or aunt if they're not
3 careful with what they do with their email on a new PC,
4 and they program these things without my uncle or aunt's
5 knowledge to go and connect to the Federal Trade
6 Commission or Cisco or Comcast or wherever it may be and
7 say, jsmith@comcast, jsmith@cisco, j.smith, d.majoras,
8 Deborah Majoras, Deborah_Majoras, whatever it is, and
9 they'll basically go through the alphabet, they will go
10 through first name, last name, and they will figure out,
11 based on the response, yes, send me the email, no, this
12 person doesn't work here, what the actual addresses are.

13 Now, of course, in this online version, though,
14 they have some advantages, they don't have to wait a
15 week, it's realtime, they don't have to spend \$3.69 on
16 stamps for every nine ones they want to check, and of
17 course it's all done without them needing to control the
18 server which is doing it.

19 So, that's again our very quick overview on how
20 these email addresses are obtained, and I'm sure the
21 panel will have a lot more color on that.

22 They've got the email addresses, now they have
23 to get the content in the inbox, they have to get it
24 past the spam filters and they've got to get you to take
25 action. Today, as Special Agent Grasso mentioned,

1 they're trying to sell and get you to do lots of
2 different things. In the case of 419, it's the niece of
3 the former emperor of Nigeria who has \$30 million in a
4 bank account and just needs your help, perhaps someone
5 over in Italy has won the lottery and needs your help,
6 and there's lots of other kinds, selling you pills,
7 selling you diplomas, what have you.

8 In addition to the types of spam, there's
9 different techniques that they use to ask you to take
10 action. The reason that we emphasize these is the
11 technique they use to ask you to take action is often
12 the one which we on the security side use to identify
13 the fact that it's spam. Those are examples like a URL
14 spam where you click on the link to a website, an image
15 which doesn't actually have any text or links, or maybe
16 it's just text.

17 So, what I was going to do now is give quick
18 examples of pharmaceutical spam and stock market spam
19 and some of the ways that they commonly use these
20 techniques to be successful in that business.

21 So, I mentioned earlier, My Canadian Pharmacy,
22 very large, successful, \$100 million, \$150 million
23 business a year, this is an example of one of their
24 spams. It tells you the products that they are
25 advertising, it asks you to take action by clicking on

1 the link and it throws in some excerpts from The Hobbit.
2 They've got the software that they use to send this
3 program to take different pieces out of the text of The
4 Hobbit so that spam filters may be confused by this
5 legitimate-looking text in the message.

6 Again, the idea behind this is if you click on
7 the link, you go to the website. This is the content
8 that they are trying to get you to take action to visit
9 the site. Since we're doing the training wheels, I
10 won't dwell on the sophistication, but we've seen
11 tremendous innovation from this organization in getting
12 their spam delivered. We've seen them changing the
13 domains that they use in spam every 15 minutes. We've
14 seen them changing the content in the spam every 12
15 minutes, phenomenal innovation in the spam content in
16 order to get it delivered, because if it's not
17 delivered, they're not going to make any money.

18 There's a second technique as well which they
19 commonly use. Now, this is still asking you to go visit
20 a URL, but a lot of really smart people on the anti-spam
21 community have figured out how to look at an email
22 message and say, this is asking someone to visit a URL,
23 let's take a look at that domain and let's figure out is
24 it good or bad, was it registered recently, is it safe
25 or not.

1 And so what they have said is, well, we're going
2 to get rid of the text version of that domain in the
3 email. So this is an example of a spam which is an
4 image, it's a. Gif with no text whatsoever that can be
5 read by a machine, short of the rather complicated and
6 problematic optimal character recognition technique
7 where you actually render the image and try to interpret
8 it.

9 In this case, they're actually giving the end
10 users explicit instructions. You can't click on this
11 link, you can't copy and paste the link, you have to
12 actually read it here, open your browser and type it in
13 to visit it.

14 Again, the action that they want you to take is
15 the same, go visit this website, we've got a great deal
16 on herbal Viagra, or some other kind of Viagra, but
17 they've eliminated the presence of the link in the
18 email, by putting it inside an image, to try to increase
19 their deliverability and get past the spam filters.

20 Now, I'm going to talk briefly about another
21 kind of spam which we've seen a lot of and that is the
22 stock market spam. In this case, they're running the
23 pump and dump spam, they've acquired some shares at a
24 low price, they figure if they send out enough of these
25 messages, there's a sucker born every minute and someone

1 is going to decide to put their retirement savings into
2 one of these stocks, the more people who buy, the more
3 the price goes up, and they sell it at a profit. Old
4 technique, it's been around for a long time.

5 This was an epidemic in 2006 and I will give
6 some stats in a minute. The reason that it was an
7 epidemic is they found methods to use images to increase
8 their deliverability to very high rates. I also think
9 that they found perhaps some weaknesses in the way that
10 our brokerage systems and whatnot are used.

11 Now, three or four years ago, if I had been here
12 giving this presentation, again, lots of hands would
13 have shot up and said, we know how to stop images, we
14 use the concept of fingerprints. Right now if you enter
15 a secure building, you put your fingerprint on there and
16 they compare your fingerprint with a database of good
17 and bad ones and figure out whether to let you in or
18 bring up the gates and call security.

19 We used to do the same thing with images. You
20 take this image, it's a bunch of zeros and ones that's
21 encoded as a. Gif and you basically do a fingerprint of
22 it, also known as a check some or hatch. You then say,
23 this is a spam, I've got its fingerprint, I am going to
24 look at all the messages that come in with information
25 and I am going to look at fingerprints and if it's the

1 same fingerprint as a bad image, I know it's a spam and
2 I throw it away. So, again, unfortunately the spammers
3 didn't take our security response and give up, they came
4 up with something different.

5 This is an example of the very same image we
6 looked at, which was trying to get people to buy
7 Goldmark Industries, highlighting some of the features
8 that were not very visible to the human eye, namely
9 these small dots inside the image. They take an image,
10 which tells people to buy Goldmark Industries, and they
11 create many, many, many copies of the image, they all
12 look the same to your eye, but they all have dots in
13 different places. The human eye sees it as the same,
14 however a computer, when it interprets it, the actual
15 encoding of the image is very, very different, even
16 though there's only a few dots.

17 Many, many other techniques that they use so
18 that they basically get the same message out to lots of
19 consumers but they do it in a way that the
20 fingerprinting technique we used to use for images is no
21 longer useful. So a lot of people had to go back and
22 develop new techniques in 2006, and while different
23 companies were doing that to protect consumers, they
24 were getting a lot of these delivered and they were
25 making a lot of money.

1 Again, talking about spam types, on the left, we
2 have a text spam, which is telling people to buy
3 Goldmark Industries, on the right, we have an image
4 spam, in the middle of that is actually an image, and if
5 you look closely you can see the little dots and lines
6 that they use to make the image different inside the
7 gift and coding, but in addition, they've got text above
8 and below the image which was randomized to try to
9 confuse spam filters, and then down at the lower left we
10 have a text spam touting Goldmark Industries, but it
11 actually includes a legitimate press release. If you go
12 look up that press release at the bottom, it's actually
13 a true statement, it's on their website, they did
14 procure distribution rights for the film in question, so
15 now there may be legitimate copies of this press release
16 going out and they've attached those to their spam,
17 which is touting the stock and the likelihood that it
18 confuses spam filters to get it delivered. A few
19 examples of what they're doing today with the content of
20 their message.

21 Now, Joe later on is going to tell you why it's
22 not nearly as simple as I present here, but again, I'm
23 going to keep the training wheels on and say, here's
24 what happened. At the lower part of the screen, I have
25 an excerpt of the spam, which you saw a minute ago, most

1 of the time spam lies, in this case it tells the truth.
2 It's saying, there is going to be a big advertising
3 campaign in early July around Goldmark Industries and
4 the price is going to go up.

5 Sure enough, in early July, there was a big
6 advertising campaign, they dumped hundreds of millions
7 of spam touting their stock into people's inboxes. The
8 result is shown here on this graph that I got from Yahoo
9 Finance. It shows that a price of \$4.75 was the price
10 for Goldmark Industries until July 3rd, when the spam
11 started touting the stock the price went up to \$8.50.

12 This is an example of the success that people
13 have had in using spam, particularly the image spam
14 technique, to tout a stock, to have people purchase it,
15 to artificially inflate the share price, and then to
16 sell it at a significant profit.

17 Now, I have to say, many times I am somewhat
18 pessimistic and somewhat frustrated by our inability to
19 put a lot of these people in jail, but just yesterday, I
20 think there was some wonderful, wonderful news, and that
21 was that the SEC indicted two people, that are the
22 Useltons, in Texas, for this type of fraud. They had
23 actually made, these two gentlemen in Texas, they were
24 recidivists, they had been prosecuted for this type of
25 thing before, \$4.6 million in seven months and it looks

1 like the SEC has a very good case against them.

2 (Applause.)

3 MR. PETERSON: Yeah, are there people from the
4 SEC here today? Anybody from the SEC who can identify
5 themselves? Drinks on us for all the SEC people who did
6 a great job there. One really nice success story.

7 And the last thing I want to comment on here is
8 some statistics around the content in spam, the one
9 thing I'll emphasize is the growth of image spam in
10 2006, and the other thing I'll emphasize is I don't
11 think these statistics really matter. I've got some
12 statistics from IronPort, I've got some statistics from
13 MAAWG, the group which Charles Stiles chairs. You can
14 go get lots of statistics from Symantec, from McAfee,
15 from Trend, from a dozen other vendors. They're great
16 reading, they are very interesting, but fundamentally, I
17 think we can all agree, any set of those statistics show
18 that the problem is large enough that action is needed.

19 So, that's the one thing I'll emphasize and the
20 other thing I'll emphasize is whatever the technique is
21 today, the technique du jour, we'll respond to that,
22 they'll come up with a new one. We have to think about
23 it that way, and not think about it as image spam is a
24 tough problem, let's stop that and we'll all be happy.

25 So, next, we'll get to the last kind of meaty

1 subject, and that's the bots. The first thing is how
2 the criminals have evolved. So, I will get, and I
3 haven't actually done this, but if I was working for the
4 Drug Enforcement Agency down at the Mexican/U.S. border,
5 from time to time there would be people driving drugs in
6 across the border to try to get them in the U.S. If
7 those people were arrested, they would find that those
8 people were not the kingpins, those were not the ones
9 actually making most of the profits through these
10 illegal activities.

11 If you're a criminal, that's a wise move. Let's
12 have someone else take the rap, someone disassociated
13 from me so I can reap the benefits without the risk.
14 That's the exact same thing criminals have done as
15 they've moved from their infrastructure, their servers,
16 which they used to pay good money for, to run and send
17 spam in 2000 and 2001, to instead using consumers' PCs
18 for that purpose.

19 So when Special Agent Grasso kicks down the door
20 and goes in there to arrest the owner of the bot, he
21 finds my aunt, who double clicked on an attachment and
22 is in no way a party to the crime, but now he has to go
23 beyond the computer sending the spam, behind the bot to
24 actually get to someone.

25 So, it's really, again, a clever technique,

1 which has been very successful for them.

2 What is a bot? A bot is simply a computer,
3 which is running some application software to send spam,
4 without the owner's knowledge. I could have this PC
5 host a website, I could have it control a machine tool,
6 I could have it play an audio visual file, I could have
7 it send spam by installing that software.

8 And again, I've got some Hughes statistics, and
9 later on the panel is going to talk about the more
10 complex things which bots do. But let's just answer the
11 question at a very high level quickly, who in the world
12 would go install this spam sending software on their PC?
13 The answer unfortunately is a lot of people. Why are
14 they doing it?

15 So, on the right, I've got the picture of the
16 Trojan horse, this is how the Greeks finally besieged
17 Troy, after ten years of Odysseus and others pounding at
18 the gates, they simply left behind this gift and sailed
19 away. Inside this gift, of course, were the Greek
20 warriors, and once they were led in through the
21 subterfuge, they then took down the city.

22 On the left, I have the modern day Trojan horse,
23 actually this is two years old, which is ancient in
24 modern online crime, this is an email that purports to
25 be from the FBI, to try to get people to do what the

1 Trojans did, thousands of years ago, double click on
2 this complaint from the FBI, which then infects the
3 computer, and then they've actually installed this
4 spam-sending bot software and maybe ten or 12 other
5 nefarious things and now their computer is owned by the
6 bad guys.

7 That's what's happening today, generating all
8 these bots on the Internet. One other thing that I want
9 to comment on, very quickly, botnets is simply a network
10 of these bot computers, which are controlled by the
11 criminal, for all sorts of things. The panel later on
12 is going to talk about bot university, which is more and
13 more sophisticated things bots are doing to communicate
14 without us being able to check them and to be able to
15 send spam effectively for longer periods of time.

16 Then in particular I am excited about Ben,
17 because I focused on bots to send spam. They're
18 starting to use web servers and web forums to send more
19 and more spam and I think he's got some real expertise
20 there on kind of a cutting edge area to show.

21 Last comment is I want to give two quick
22 examples of what bots mean to us. The first one is
23 holding up a mirror to the bot computers on the
24 Internet, and in particular, the large service
25 providers. Now, I don't mean to pick on any of our

1 large service providers, they're all working very hard,
2 but the problem is they have the most consumers with the
3 least knowledge, they do not have a professional IT
4 staff to come by every day and take a look at their
5 desktop and their firewall, and so they are the ones
6 that are getting infected, and when they do, there's no
7 one there to help clean them up, unless perhaps they
8 have a young relative who works in high tech. Other
9 than that, they've been on their own.

10 So, what we have done is we have actually held
11 up a mirror to the Internet and said how infected is the
12 Internet? Now, this slide is a little complicated, but
13 the simple way to understand it is this is what a large
14 enterprise sees coming to them from the Internet. So,
15 this is a screenshot from an appliance, which is
16 receiving Internet email, at an enterprise, and it's
17 basically saying, in the last 24 hours, they tried to
18 send the Internet, eight and a half million messages.

19 Now, which were the networks, which were the
20 collection of PCs which sent the most? Well, number one
21 there is Polish Telecom, it tried to send this
22 enterprise 401,000 messages, of which seven were
23 legitimate. You can go down the list for yourself, the
24 point is, if you look at the mail coming out of the
25 large broadband consumer networks, it shows you the

1 magnitude of the level of infection, and the fact that
2 we do have a very serious problem here.

3 One other view on this is to actually see how
4 the criminal organization behind My Canadian Pharmacy is
5 using this. So we did an analysis over a two-week
6 period of all the spam that was touting the My Canadian
7 Pharmacy crime gang's websites. We saw that they were
8 capable of sending a million and a half spams a day,
9 like the one we saw with the excerpt from The Hobbit,
10 they were using 106,000 bots, the bot network was
11 incredibly spread out, over 3,200 networks and of course
12 there were the large ones like I have listed here,
13 Telefonica de Espana and others, but we also see bots on
14 other criminal networks, again, very large number of
15 bots, very successful, very easy for them to increase
16 their volumes and try to stay ahead of what the good
17 guys are doing and I think their profits show,
18 unfortunately, how successful they've been.

19 So, we've talked about the ways that they get
20 this delivered, how they get your email address, how
21 they get the content in your inbox and how they try to
22 have networks of bots to send it. Now let's talk about
23 what they want you to do once they get it in your inbox,
24 and that is to take action.

25 Lots of actions that I've listed, but today we

1 are only going to focus at least in the training wheels
2 version on the websites. Wanting you to go to a
3 website, take a look at the products they're offering,
4 and perhaps take advantage of this erection pack Cialis
5 plus Viagra offer, the special this week.

6 These are the training wheel components which
7 the panel is going to use later to talk about the more
8 advanced things. If you want to host one of these
9 websites, whether it's My Canadian Pharmacy or FTC.gov,
10 you've got to get the website, you've got to register
11 FTC.gov, you have to publish a phone book, a DNS server
12 who tells people how to get to you, how to get to your
13 IP address, you have to publish the records in that
14 phone books, that's the DNS server, you have to get the
15 server and put content on it.

16 Anyone who wants to run a website has to do
17 these components. When we talk about the ways that they
18 attack us, the way that they try to elude it, we'll talk
19 about it in terms of these components and that's why
20 we're emphasizing this a little bit more than we would
21 otherwise.

22 So, the last example, back to my favorite spam
23 game in the world, My Canadian Pharmacy, I picked one
24 from my random quarantine, I picked the website that
25 it's referring to and this is what I learned, they had

1 registered a domain called BigMouseTrack.info, a few
2 days ago, they registered at a registrar called
3 1877namebid.com, and they filled out the Whois
4 information to say who they were registering it, as I've
5 shown here.

6 The only two things I found out interesting
7 about that is that they used a country code that as far
8 as I can tell does not exist, there's no country in the
9 world that has a +68 prefix, and they used an email
10 address to contact them hosted at Dublin.com, which
11 happens to be run by Suresh's organization, which he
12 could comment on.

13 They also set up DNS servers, and the records
14 that they used, they used actual computers on broadband
15 residential networks. These are bots, to actually host
16 their phone book, to actually host their DNS servers,
17 and they had multiple ones of them for redundancy on the
18 biggest high speed broadband networks in Taiwan, Spain,
19 U.S., Brazil and other places.

20 The web server itself was running on a Korean
21 broadband server on their IP address, and the web server
22 itself had locations, multiple locations on the Korean
23 Telecom network, and one of the interesting things was
24 the images weren't hosted on that server, they were
25 being pulled from other bots on other broadband servers

1 around the world.

2 Now, I think the panel has a lot to say about
3 these techniques, I'm not going to dwell on it, but it
4 gives you a sense for what they're doing. In
5 particular, the My Canadian Pharmacy gang has been
6 integrating over the last 18 months using a number of
7 techniques to stay ahead of the good guys and make it
8 tough to shut them down and to obfuscate what they're
9 doing.

10 And then I wanted to mention two things and
11 we're not go to focus on them on the panel, there are
12 other panels, but to make sure we understand the full
13 scope, some types of spam, they actually get money
14 directly from the consumer. My Canadian Pharmacy, you
15 give them a Visa card number and they run that credit
16 card and in some cases they actually fulfill the order.

17 I'm sure a lot of people in law enforcement know
18 about it, but if you place an order from My Canadian
19 Pharmacy, you may get an envelope like this with some
20 pills, you may get one like this with some pills. It
21 may come from China, it may come from India, but in some
22 cases the spammers actually have large-scale
23 sophisticated distribution supply chain organizations
24 that are shipping product, may be legitimate, may not be
25 legitimate, around the world. These are things that are

1 important to understand because these are the things
2 that we are going to use to expose their weak links and
3 in particular Jon has a lot of expertise in this area
4 which I am looking forward to hearing about. Thank you.

5 (Applause.)

6 MR. ST. SAUVER: So, I'm going to go ahead and
7 talk a little bit about the way technology is impacting
8 spam, but also a little bit about the way it's not
9 really all about technology. When I go ahead and say
10 that, what I'm really trying to tell you is that even
11 though we can look at some of the technological
12 evolution that's occurring, it's really also evolving on
13 a business level. It's really also evolving on a
14 strategic level. It's the sort of thing where
15 illegitimate affiliate programs are allowing spammers to
16 scale up their operations in ways that really are fairly
17 amazing. It's also giving us some additional benefits,
18 things like the ability to go ahead and claim that
19 they've advised their affiliates not to spam.

20 These are the sorts of phenomena that are
21 occurring today that you need to go ahead and be
22 watching for, in addition to things like the evolution
23 of the image spam, in addition to things like the use of
24 botnets.

25 All of it really comes together in the fact that

1 we're really seeing the creation of a spam eco system.
2 There's specialization occurring, there are people out
3 there who are niche providers who go ahead and actually
4 serve this particular need. They may harvest addresses,
5 they may go ahead and produce bots, they may write
6 malware. These are all people who are specializing in
7 one particular part of the spam problem and together
8 they form a very powerful consortia. That's the problem
9 that we're facing today.

10 People are no longer needing to become experts
11 to go ahead and actually spam. They can go out and buy
12 what they need instead of having to build it themselves.

13 Because that eco system is so complex and
14 vulnerable, it actually is something that can be
15 attacked. Because these people have to go ahead and
16 learn an increasing body of spam trade craft, for
17 example, they need to go ahead and become educated. How
18 do they do it? Well, there are spam forums where they
19 can go ahead and trade notes with their colleagues. We
20 know that they go ahead and are going to need to
21 purchase particular products that will help them go
22 ahead and do their spamming activity. That's going to
23 generate financial records and we'll hear some about how
24 those financial records may be able to be worked.

25 The problem that we're running into is that

1 they're scaling up very efficiently and we need to make
2 sure that we're going ahead and doing so as well.

3 One of the things that is perhaps the biggest
4 spammer vulnerability is the money trail, and the U.S.
5 Money Laundering Threat Assessment Working Group did a
6 really great job of sort of highlighting some of the
7 financial channels that the miscreants are exploiting.
8 In 2005, they went ahead and released the U.S. Money
9 Laundering Threat Assessment, it's the sort of document
10 that I would encourage you all to look at because that
11 really explains how the money is being moved. It's not
12 surprising, given that kind of a document's emergence
13 that they're having fewer and fewer avenues available to
14 use.

15 For example, we went ahead and learned about a
16 lot of the pill samplers, they are down to one credit
17 card brand that will continue to accept their online
18 pharmacy sales, and if we can go ahead and attack that
19 service provider, that will have a potential impact on
20 the spammers.

21 I think it's also important to recognize that
22 just as everyone else pays taxes, it's going to be
23 critical that we have the spammers and their affiliates
24 also pay taxes. Talking about Al Capone and the fact
25 that he was eventually busted for income tax evasion,

1 well, I think we really need to focus on things like
2 income tax liability for some of these affiliate
3 programs. If you have someone signing up anonymously,
4 being paid anonymously, I really sincerely doubt that
5 they're getting a 1099 for their income. So, if they're
6 not going ahead and having these sorts of very basic
7 procedural and administrative things attended to, that
8 perhaps is an avenue that can be used to attack them
9 successfully.

10 We also heard about the envelopes coming in from
11 overseas containing the pills and so on. Those spams
12 are generating these orders for the pills, they need to
13 get those things to the customers, unless it's actually
14 a case where they're ripping off the customer directly
15 and sometimes that may happen, because after all, who is
16 going to go into the police and say, oh, I'm sorry, I
17 didn't receive the pills I purchased, my Vicodin didn't
18 come in today. No one is going to be willing to admit
19 that.

20 So, the spammers know that and in some cases
21 they may exploit it, but in other cases they may deliver
22 the honest product. When they do deliver that honest to
23 god product, it's coming in from overseas in many cases.

24 We have borders, in the physical world we do
25 have borders, we don't have borders electronically, but

1 in the physical world we do. Customs and the Drug
2 Enforcement folks should be able to start interdicting
3 some of those shipments as they come through our
4 borders, unfortunately they may not have the staff
5 that's really needed for them to go ahead and do so.

6 So, I think we need to look at some of these
7 physical issues, rather than treating it purely as an
8 electronic phenomenon. They do go ahead and have income
9 streams, they do go ahead and have product shipments.

10 We also know that spammers love anonymity, so as
11 we see things like these financial and fulfillment
12 channels being attacked, we know that the spammers are
13 adapting, and that's why we're seeing increasing levels
14 of things like pump and dump spam or mortgage lead spam,
15 it decouples the spammer from the spam. It decouples
16 the spam from fulfillment channels.

17 So, we know that there are things that the
18 spammers are relying on to have this sort of anonymity,
19 things like anonymized domain name registrations. If
20 you look at these domain name registrations, if you do
21 Whois look-ups on them, you will see in many cases they
22 have completely bogus data. We can begin to go ahead
23 and start attacking that channel by looking for those
24 incredibly fraudulent registrations.

25 There is also the issue of cheap and easy to

1 create off-shore shell corporations. These, again, are
2 the sort of things that spammers are using to go ahead
3 and provide insulation to go ahead and give them the
4 ability to continue to persist. There are also national
5 privacy laws, particularly in the European Union that
6 really go ahead and make it hard for ISPs and even
7 consumers themselves to take the sort of actions that
8 they would like to go ahead and take to protect
9 themselves.

10 And I would argue that we still have very
11 primitive methods for international law enforcement
12 cooperation.

13 One of the things we've heard this morning
14 repeatedly is that spam is an international phenomenon
15 and this really is true. That's one of the messages I
16 hope you take away from this today. Because spam has
17 been mitigated at least in part here in the United
18 States, spammers have responded to that. They have
19 evolved. They have gone ahead and moved their
20 operations overseas. Europe in particular has really
21 been badly infested recently.

22 So, it's the sort of situation where because it
23 is an international phenomenon, it's going to require a
24 coordinated international response. It's not going to
25 help if we clean up all of the America's PCs that may be

1 infected if we still have millions of infested PCs in
2 Poland, in Turkey, in Spain.

3 I would also point out that in some cases, we
4 may even be seeing phenomena that have more strategic
5 impact. Spam has really been a central level and has
6 had such a deleterious effect on our economy, it really
7 is a form of low intensity cyber warfare. What a
8 perfect way for those who hate the United States to
9 attack us. We don't even recognize we were being
10 attacked, and if we did, what we would do?

11 So, I just wanted to leave you with six quick
12 closing thoughts. One is that the Internet really is a
13 giant laboratory for spammers, and they can just try
14 different things and see what works. While we can and
15 have to respond to all those attempts to go ahead and
16 experiment online, we're not going to win if we just
17 continue to play that kind of a defensive ball game. We
18 really need to go on the offense.

19 Spamming requires a lot of stuff. By that I
20 mean the spammers don't live in their basement, they
21 don't just write all the code they need themselves.
22 They buy things. They go ahead and sell services.
23 There's an eco system out there and that's what we need
24 to attack, is that complex eco system.

25 There are choke points and those choke points

1 are the things that we need to go ahead and work on
2 relentlessly. Things like merchant account processing
3 and the interdiction of illegal shipments at our borders
4 are examples of that.

5 And spamming activity doesn't occur in
6 isolation. There are communication networks out there
7 supporting these spammer activities. We need to go
8 ahead and focus on those, just as we would collect
9 intelligence on a terrorist organization, you need to go
10 ahead and also be prepared to collect intelligence on
11 spam organizations. That needs to be done in a proper
12 way, with all appropriate court approvals and so forth,
13 but we need to go ahead and begin tackling this as a
14 system, as organized crime.

15 And we also know that the bad guys have done an
16 excellent job of scaling up their operations. If they
17 have thousands, tens of thousands of affiliates, it's
18 going to be hard for us to go ahead and have enough
19 prosecutions to go ahead and deal with all of them.
20 It's great to see people getting busted, I appreciate
21 each and every one of those arrests and prosecutions,
22 but if there are thousands or tens of thousands of
23 spammers, we're just not scaling.

24 And there's also the problem that spam is an
25 international issue, and one which is going to require

1 coordinated international effort. We really need to
2 have the United States show leadership in this area, and
3 actually have the same sort of success overseas that
4 we've had in the United States chasing these guys off of
5 what they would like to think of as their safe ground.

6 And with that, I'll turn it over to Jon.

7 (Applause.)

8 MR. PRAED: Good morning, I guess it's still
9 before noon, so good morning. Glad to be here. I am an
10 attorney in private practice, I for the past ten years
11 have largely made our focus the focus of the Internet
12 Law Group to sue fraudsters on behalf of corporate
13 victims. It's not that we don't care about the
14 individual, but quite frankly, the individual as an
15 individual is not going to catch these people. We have
16 to look for ways to leverage our resources and
17 everything that we do has to be focused on how can we
18 act more effectively to get a bigger lever, right? If
19 you have a big enough lever, you can move the world and
20 we have to catch every spammer out there, we just have
21 to look for those leverage opportunities.

22 The way we sue spammers in the end is by
23 catching them. We track them and identify them through
24 capturing a lot of data. We try to track them across
25 what we call the spam life cycle. I would like to talk

1 to you today a little bit about some of the observations
2 that we've been able to make over the past ten years of
3 doing this, and provide a little bit of our expertise on
4 what we think are the evolutionary concepts that
5 spammers implement.

6 At some level, though, I want to say, how are
7 they evolving? To be honest, they're not, in one
8 important way. Spammers do two things, as a result of
9 what we're trying to do, they will always do these two
10 things, and no matter what we do, they will continue to
11 do them. They disperse, and they converge. Everything
12 that we do to them is going to make them react in one of
13 those two ways. I don't care what they're doing, I
14 don't care what we do to them, they will react in one of
15 those two ways.

16 Everything else is a tactic. The strategy we
17 have to adopt is to focus on how do can we take
18 advantage of their dispersion, how can we take advantage
19 of their convergence, and I think some of the things
20 that we have done through our involvement in some of
21 these civil litigation cases, you will see there are
22 lots of things that we can do if they react in either
23 way.

24 I don't care, they're going to move one way or
25 the other, the trick is that we have to anticipate and

1 react to it.

2 Now, one of the things I would like to do is try
3 to echo some of the questions that Joe has raised, which
4 I think are fantastic questions. I think I have heard
5 lots of speeches on spam, Joe's presentation you just
6 saw is I think one of the most elegant in terms of
7 focusing on the macro solution to the problem. It is a
8 complex problem. We are not fighting mosquitoes as we
9 fought in the Panama Canal, having to build the Panama
10 Canal, we had to address the yellow fever problem.
11 Those mosquitoes didn't have nearly the brain that
12 spammers have. Spammers are extremely intelligent, they
13 react. This is in some sense a world health issue, if
14 you will, in terms of trying to deal with a macro germ,
15 but these are not germs, they're not mosquitoes, they
16 react, and we have to take that into account.

17 We have a current lawsuit pending that we filed
18 in Federal Court in Virginia that is targeting spammers
19 who are themselves targeting email addresses that they
20 have harvested through websites that their robots are
21 visiting. Our client is an enemy called Project Honey
22 Pot, which is a nonprofit organization that provides a
23 distributed network of spam-trapped honeypots that
24 basically install honeypots on websites, any of you
25 today can download one of their honeypots, install it on

1 your website, and if anyone visits that particular
2 honeypot, they will be handed out a unique email address
3 and their IP address and other characteristics of their
4 web browser will be captured by Project HoneyPot and
5 retained. Then Project Honey Pot sits back and waits,
6 and waits, and waits, until that email address receives
7 a response. They've been doing this for the past two
8 and a half years and in the past two and a half years
9 they have received millions of email messages that have
10 been sent from millions of spam harvesters, excuse me,
11 from millions of spam servers.

12 What's interesting, however, is that the number
13 of harvesters that have collected those millions of
14 email addresses is only in the 19,000 range. 19,000
15 unique IP addresses have harvested those millions of
16 email addresses to send those millions of spam messages.
17 It's a ratio of 178 spam servers, botnet spam servers
18 for every one harvester out there.

19 So, in the effort to try to catch these guys,
20 yes, we have to focus on botnets, yes, we have to take
21 it, but the moment you take on that fight, recognize
22 you're fighting an army that's 178 times larger,
23 artificially larger, than the true number of cadets on
24 the other side facing you. There really aren't that
25 many people doing this, and some of the resources that

1 they use and exploit, specifically the harvester
2 community, is a much smaller, narrower stream that we
3 have to find a way to bridge across in order to get to
4 the other side towards hard identity.

5 Our lawsuit is targeting those harvesters. We
6 currently have John Doe discovery. One of the things I
7 want to jump into is show you some of the strategy that
8 we use in some of the vulnerabilities that we see in the
9 spam community through the John Doe discovery.

10 One of the interesting statistics, though,
11 that's come from the Project Honey Pot harvesting
12 information is that most of the visits these honeypots
13 are being made by robots. Many of them are good robots,
14 but not all of them are. Obviously the ones that send
15 spam are bad robots. Of all the visits that they've
16 seen, about eight percent of all visits result in spam,
17 which means eight percent of all robots out there are
18 essentially bad robots. It's a very large community if
19 you take in mind how many people out there are using
20 robots for good on the Internet. Eight percent of that
21 universe is out there for one reason and one reason
22 only, they're looking for your email address because
23 they want to send something to you.

24 I said earlier, spammers evolve, but they really
25 only react in one of two ways, they disperse or they

1 converge. One way that I think spam is evolving, and I
2 thank Tom Grasso and the FBI for commenting on it, spam
3 is increasingly going into the criminal arena. It used
4 to be that spammers were kids or entrepreneurs, if you
5 will, trying to make money. They are still there doing
6 this, but most spam today, I submit to you, is not
7 designed to actually engage in any sort of commerce,
8 even illegal commerce, it is quickly running to a pure
9 criminal enterprise. I submit to you at the next FTC
10 spam conference, we will not even be addressing the
11 commercial aspects of this activity, what we're going to
12 see is spam being sent out for three purposes,
13 extortion, terrorism, and warfare, between nation
14 states.

15 Extortion in the sense that you are going to get
16 an email message that's going to have in it a photograph
17 of your child, and they're going to say, I know who your
18 kid is, I know when he gets dropped off at school and
19 I'm going to kill him on Thursday of next week unless
20 you wire money to this bank account. CNN is going to
21 report that that happened last week, a week later you're
22 going to get that message. What are you going to do?

23 Terrorism, obviously, we're already seeing links
24 between terrorism and spam and warfare between nation
25 states. I think we are seeing that to a large extent,

1 to a large extent that simply is not reported.

2 Eastern Europe, with the break-up of the Soviet
3 Union, we're seeing a lot of activity there take place
4 in the cyber arena, and we as a society have got to deal
5 with how are we going to deal with the Internet if this
6 problem that was a simple, gee, I get a lot of stuff I'm
7 not really interested in buying, converts into
8 extortion, terrorism and traditional cyber warfare.

9 Now, let me turn to, I'll go back instead of
10 forward. Let me turn to what do we use civil litigation
11 for? Civil litigation is that extremely helpful
12 supplement to the criminal law enforcement process.
13 Largely because, again, leverage. There are a lot more
14 civil litigators and lawyers out there than there are
15 official government law enforcement actors.

16 One of the things we have to find a way to do is
17 leverage what we as a society can know and can find out
18 about the bad guys by leveraging what we can learn
19 through John Doe civil discovery process. I outline for
20 those of you, if you can read this, the process that we
21 generally follow, the first step obviously is filing the
22 John Doe complaint.

23 We've done that in our Project Honey Pot
24 lawsuit, asked the court for permission to issue
25 subpoenas to various parties, then you issue those

1 subpoenas to the sources of information. They're
2 largely five sources of information. You have Internet
3 companies that are providing connectivity in one way or
4 another for the websites or the domain names, or the
5 drop sites that are being used. But you have lots of
6 other sources of information that you can go to besides
7 the Internet providers. You have telephone providers,
8 land line providers, cell line providers, as well as IP
9 telephony providers. Spammers need to have access to
10 telephones, and the telco providers are the ones that
11 provide it to them.

12 You also obviously have financial institutions
13 that are either providing them with banking services,
14 credit card card processing or sort of nontraditional
15 developing methods of payment. All of those are often
16 subject to subpoena, all of them often operate in a
17 multinational context and are extremely interested in
18 many of the changes that are coming about in law
19 enforcement rules and regulations concerning know your
20 customer rules, in gaining penetrability into knowing
21 more and more about the spammer community.

22 If you can get a spammer's bank account records,
23 you can get everything that you want to know about that
24 spammer. The John Doe civil litigation process is an
25 excellent way to start that off so that when we hand a

1 case off to law enforcement, they have an extremely well
2 developed case for prosecution.

3 Physical address owners can also be subpoenaed.
4 Private mailboxes are frequently used by bad guys, and
5 if you open a private mailbox in the United States, the
6 private mailbox owner is required by law to take a
7 driver's license or other government-issued photo ID.
8 Jeremy Jaynes was prosecuted on that, his accomplice,
9 Richard Ralsky showed his driver's license and that
10 driver's license photograph was copied, God bless him by
11 the private mailbox owner in North Carolina. He drove
12 all the way up to North Carolina, and explained because
13 of a government agent who asked him to do so, he crawled
14 through his attic and looked through dozens of boxes of
15 photographs of driver's licenses that he had made,
16 because that's what the law required him to do. He was
17 a first generation immigrant, and you have to applaud
18 that sort of citizen soldier who does the right thing
19 and because of it has in his attic a box of paper that
20 has on it the information we need to catch the bad guy
21 and put him away.

22 Jeremy Jaynes, of course, was sentenced to nine
23 years in prison, because of the spam activity. So,
24 physical address owners are an extremely useful
25 resource. Shippers, last of all, are extremely useful,

1 because most bad guys who are shipping anything, even if
2 it's a fraudulent product, have to have some way to get
3 it there.

4 So, all five of these sort of areas of discovery
5 are available to us, and each of them in their own way
6 can provide useful information. All of that information
7 then gets reviewed, and analyzed to ask, is there some
8 data point in the response that we have seen that leads
9 to actionable information, can we seize a bank account,
10 can we name and serve someone, put a complaint in their
11 hands that obligates them to appear in a court that has
12 some power over them to put it to them. Or can we give
13 the information to law enforcement who can put handcuffs
14 on these people.

15 If there is no information that's actionable in
16 that first, we simply rinse and repeat. We get lots of
17 information from subpoenas and we can repeat that
18 process almost endlessly until we find something to
19 catch the bad guy, and ultimately, ultimately they can
20 be caught because they all make a mistake. They all
21 seek anonymity, which is why they disperse or they
22 converge.

23 They seek to disperse across white hats so that
24 no one of us has the motivation to do anything
25 substantial to stop them or they converge across black

1 hats because they hope that the black hats will be able
2 to be paid enough to hide their identity.

3 I submit to you, if you think about the
4 complexity of dealing with those two reactions, we can,
5 within the room, deal with how do we deal with
6 dispersion? We share data amongst ourselves. How do we
7 deal with convergence? We have to find a way, as Joe
8 suggests, to build and enforce borders so that we can
9 keep black hats out of the rest of the network that the
10 rest of us use.

11 I appreciate the opportunity to be here. Thanks
12 very much.

13 (Applause.)

14 MR. HODAPP: Now we would like to have some
15 discussion within our panel and we would like to start
16 with some of the first topics that were raised in
17 Patrick's presentation, which is the email harvesting.
18 In fact, in Jon's lawsuit, he has alleged that Project
19 Honey Pot had 6.1 million spam messages received over 15
20 months because of the harvesting that he was suing the
21 defendants for. I'm wondering, Suresh, can you address
22 whether this same problem is occurring internationally?

23 MR. RAMASUBRAMANIAN: Well, chosen techniques
24 are much the same variable that are used and a spammer
25 in China or in Brazil can use the same techniques that a

1 spammer in United States can. He probably downloads the
2 same set of software or hires the same botnets from the
3 same set of people.

4 So, spam is truly international, and there's not
5 going to be anything much different about the spam that
6 somebody in China receives compared to the spam that you
7 receive in the United States. It's some local business
8 targeting you with localized spam so that you get
9 Chinese spam in China or you get a local business spam
10 in the United States as well. That's the general pump
11 and dump and stock product stuff.

12 MR. HODAPP: Suresh, you indicated that one of
13 the ways that people can protect themselves by having
14 their email harvested is having something in place that
15 is not actionable, such as using the word "at" instead
16 of a symbol, or using throw-away email addresses as an
17 additional protection. Do those still work?

18 MR. RAMASUBRAMANIAN: That used to work ages
19 back, but when you look at a botnet that can mine the
20 contents of an Outlook address book or files on your
21 desktop, well, you're out of luck. If you're looking at
22 web harvesters which do account for a good amount of the
23 traditional person that does this harvesting, yes, that
24 kind of thing will work, but to make it sufficiently
25 unreadable to a bot, you have to make it just as

1 unreadable or even more unreadable to a human being. No
2 point in that.

3 MR. HODAPP: If we can discuss briefly, if
4 there's any other methods that be can be used to try and
5 reduce harvesting, I think, Patrick, the one thing that
6 IronPort had mentioned was the possibility of reducing,
7 not bouncing invalid addresses immediately. Can you
8 address that?

9 MR. PETERSON: Sure. So, there's a lot of
10 vendors who make solutions and there's even lots that
11 plug into open source solutions for email security that
12 attempt, and in some cases are very successful, to
13 protect against the directory harvest attack. So, when
14 they say, JSmith, Jim.Smith, you don't actually just
15 say, yes, they work here, or no, they don't work here,
16 yes, this is a valid address, no, this isn't a valid
17 address.

18 Without going into the technical details, you
19 basically limit that amount of information and you apply
20 methods so that when you detect someone that seems to be
21 harvesting, you shut down their ability to have that
22 kind of information. So there's vendors on the market
23 that do it, and if you take some of the techniques that
24 you mentioned, if you take those techniques, you
25 definitely can reduce the amount that your email address

1 is disseminated, but if you have a friend and they've
2 got an Outlook address book with yours and they get
3 infected, that might be one place that it leaks out.

4 MR. HODAPP: Does that result in this evolution
5 basically resulting in harvesting by one means or
6 another being very effective and very difficult to deal
7 with that? Is that the conclusion of this?

8 MR. RAMASUBRAMANIAN: Well, you cannot avoid
9 getting your email address harvested. The one thing you
10 can do is be conservative about who you give your email
11 address to, and if you are using your email address
12 somewhere public, like a website or a mailing list or a
13 forum, make sure that you got it through the email
14 address that you use just for that purpose. Free email
15 addresses are downloadable from Hotmail, Gmail and other
16 servers. Use those and learn to keep your information
17 private as far as possible. It certainly won't stop
18 your address from being harvested, but it will minimize
19 or mitigate the risk.

20 In spam filtering and in trying to stop spam,
21 stop botnets, nobody will claim solution, because no
22 solution exists, any more than there exists a solution
23 for a disease, a pandemic. It's still going to be
24 there, it's going to be a fact of life. So, you follow
25 models that are current in the security and what you

1 call it, pest control or disease mitigation sectors,
2 where you try to minimize the factors that encourage
3 this from developing.

4 If you are trying to stop a disease, you drain
5 swamps nearby and you distribute rules to people and you
6 teach them to watch for signs of a disease and do things
7 like that.

8 MR. HODAPP: So, those are good analyses,
9 Suresh. I think we want to move on and address the
10 second spam requirement. The addresses are one thing,
11 but then they also need to have a subject matter, and
12 Patrick previewed an issue that occurred in one of our
13 discussions that perhaps you could address, Joe, which
14 is the different types of costs and risks that are the
15 choices a spammer makes when they choose the types of
16 products or services to sell.

17 MR. ST. SAUVER: So, obviously there are going
18 to be some differences in terms of connection between
19 the spam subject matter and the recompense that they
20 receive. So, for example, a mortgage spam might
21 actually result in a larger payback or a larger payment
22 amount than some other spam might. On the other hand,
23 you might have fewer people actually follow through on
24 those.

25 So, there's sort of the economic equation that

1 each of the spammers is mentally reviewing. Things like
2 stocks pump and dump spam is so popular these days
3 simply because it allows people to have huge leverage.
4 They can go ahead and make gains that are not going to
5 be attainable if they're promoting some commercial
6 product. I think that might be sort of the area that
7 you're attempting to highlight.

8 MR. HODAPP: It is, yes. There's the incidence
9 of returns, but there's another factor that perhaps Jon
10 could address which would be if there's differing legal
11 risks. For example, some of the pharma spam, is there
12 legal risk for some of the pharma spam?

13 MR. PRAED: Well, certainly you're violating
14 more laws if you're selling product that is more and
15 more illegal and not just illegal, but also is already
16 subject to a fairly robust law enforcement process. I
17 think you see a lot of pharmacy spam today, in fact I
18 know it, three years ago you saw hydrocodone being
19 advertised in the email themselves. That completely
20 disappeared. Two and a half, three years ago, because
21 they realized, whoops, that's the third rail, you're
22 dealing controlled substances openly, there are lots of
23 law enforcement procedures that have been in place for
24 40 years now, quite well developed, that are going to
25 take you out.

1 So, you see most pharmacy spam focusing on still
2 prescription drugs, but it's much less controlled
3 substances. Pump and dump is the same way. It's much
4 easier to get away with the money when you don't have to
5 tell your victim to go to some tree where you've got
6 their kid that you've kidnapped waiting to exchange for
7 the bag of money. Pump and dump, you get someone to
8 buy, you've already bought previously, or sold short,
9 and you don't have to have an individualized transaction
10 with the victim that is initiated through the spam.
11 It's a separate transaction, if you will. It makes them
12 much harder to catch.

13 MR. HODAPP: Looking at it from the point of
14 view of both spam and malware, using these bots for one
15 or the other, which I guess you can do either, Suresh,
16 you mentioned, I think, that the spam was pretty much
17 the same internationally. Is that true, also, of the
18 other techniques that the malware type of spam, the
19 malware operators will use, is it the same as a DDoS
20 attack, for example?

21 MR. RAMASUBRAMANIAN: Well, yes. A lot of the
22 malware economy is highly centralized. You've got a
23 very small subset of people that actually write the
24 malware and you've got a small subset of people who
25 create and rent out botnets. You have a completely

1 diverse customer base for those.

2 For example, right now, the Nigerian spammers
3 who used to be creative and use email to tell the world
4 about hidden treasure are buying lists of compromised
5 accounts on U.S. cable modem providers, Roadrunner,
6 Adelphia, places like that, and they are spamming
7 through those stolen accounts. The accounts that are
8 stolen are also accompanied by ID theft and the guy's
9 credit card information is gone as well and then he
10 finds his email address being used to send out these
11 scams.

12 So, the botnet economy is truly international,
13 there's no borders there, and any borders that do exist,
14 exist only in terms of the physical transaction, if any.
15 Like for example, there's no physical transaction
16 required now for stealing somebody's credit card, or
17 trying to pump up the value of a stock.

18 There is transaction required for trying to
19 convince the guy to buy a market share or buy pills
20 online and things like that. So, that's the thing you
21 have to take into account, and the tools and the
22 techniques are completely universal, they're not going
23 to be different as such. The difference you will get
24 internationally is that different countries have
25 different sets of laws and different sets of

1 competencies in dealing with spam, so that if you have a
2 country with a weak legal regime which doesn't have
3 appropriate laws to deal with the issue, and where the
4 ISPs are a few generations behind in filtering, then
5 that country has got problems.

6 MR. HODAPP: Thank you, Suresh. I would like to
7 move to one of the major areas for this panel, which is
8 the use of the bots, the dissemination of the message.
9 Ben, as director for network abuse for GoDaddy, Patrick
10 had mentioned that there were some other methods that he
11 didn't focus on for distributing spam, such as web
12 servers, or web forums. Could you address that, please?

13 MR. BUTLER: Yes. You know, we've talked about
14 bots being a situation where they've taken over home
15 PCs, personal computers, and are using those to send out
16 the spam. One of the, I guess, areas that we can get a
17 little success in dealing with PC-based bots is that
18 ISPs can filter on specific ports to try and limit
19 outgoing email and channel it through their legitimate
20 mail server, thereby being able to apply outbound
21 filtering and so forth, but what they have begun to do
22 now is they have begun to take over web servers and
23 websites that belong to legitimate companies, legitimate
24 web hosting customers, because those servers don't have
25 the same restrictions.

1 For example, think of any random website that
2 you might go to, and they have a contact us forum on
3 their website, it's a script that you can send feedback
4 to the site owner. That feedback goes in the method of
5 email and when they can take over a web server, they can
6 use that same permission to send email that the contact
7 forum is designed for and instead send whatever they
8 inject in there to whomever they decide.

9 So, web servers have become a major problem.
10 It's the same basic philosophy as a botnet, they get in
11 through script vulnerabilities, weak passwords, things
12 like that, but when they do that, they also create
13 another barrier to try and keep it more difficult for
14 someone to actually track down the spammer involved.

15 Abuse staff, for example, has to spend their
16 time in customer education efforts with the legitimate
17 customer, to help them understand how to secure their
18 bots, rather than being able to spend all their time
19 chasing down the actual bad guys. So, it's definitely
20 another head on the same dragon.

21 MR. HODAPP: What kind of success has GoDaddy
22 had in addressing that problem?

23 MR. BUTLER: Well, I mean, I'm not going to lie
24 to you and tell you we've found the ultimate solution.
25 Obviously one of the major components is customer

1 education, our legitimate hosting customers have to be
2 made aware of the seriousness of the responsibility
3 they're taking on when they get, say, a dedicated
4 server. They need to be aware that they have to keep
5 their scripts and their server-side software up to date
6 with security patches and that sort of thing.

7 The other thing that we can do is we've, even
8 with our dedicated servers, we filter all email through
9 our own relay system so that we can apply outbound
10 filtering. Not all hosting providers are able to do
11 that at this point. So, the same types of things that
12 protect you from getting it into your bulk mail versus
13 your inbox can be applied outbound by your ISPs, and
14 hopefully cut down the amount that's actually tracked.

15 MR. HODAPP: In addition to the things to
16 prevent the outbound dissemination of web pages that
17 have malware, can some other panelists mention some
18 things that could be done at the ISP level to prevent
19 that from coming in? Are there solutions at the
20 recipient level?

21 MR. PETERSON: For the web-based?

22 MR. HODAPP: Yes.

23 MR. PETERSON: There are some solutions, but I
24 have to say that I am quite pessimistic on this. So,
25 people receive things in email from time to time and

1 they become infected or they can be accessed over the
2 Internet with the network vulnerability. When it comes
3 to the web, people are so used to clicking on bright,
4 shiny things, free things, screen savers, accelerate
5 your bandwidth, new plug-ins, and they are so used to
6 downloading that new version of Shockwave or that new
7 version of the toolbar, that it's really, really easier
8 for criminals to convince them that there's some other
9 neat, new shiny thing, which may in fact be giving them
10 the screen saver, but also giving them some form of
11 malware.

12 So, there are Internet companies that are
13 providing web-based security, not just the email, there
14 are some ISPs that are providing value-added services
15 based upon protecting them around the web. But it's a
16 very challenging area because it lends itself to
17 criminals doing social engineering, because people are
18 trained and so used to downloading and clicking on
19 things over the web.

20 MR. HODAPP: Would this be a place where you
21 might apply reputation-based analysis and filter more
22 vigorously on something coming from let's say the back
23 alley website, a bad neighborhood website?

24 MR. PETERSON: That's a great segue into a point
25 I wanted to make and we've seen many technology vendors,

1 three or four years ago they said, we have this thing
2 for reputation, we can tell the difference between a bot
3 and a legitimate server, now a lot of those companies
4 are saying we have that same reputational concept for
5 the web. We know the difference between a good server,
6 GoDaddy, and some name that's been registered and hosted
7 on some kind of overseas provider who does bad things,
8 and we know that people shouldn't be going to that
9 server because it has attributes which are very much
10 like a bad server.

11 And I think this is a new frontier that's really
12 important for us to attack. Five years ago if you had
13 said to a lot of the providers here, hey, you've got
14 people on your network who are sending spam, I think a
15 lot of them would have said, they're paying me for a
16 service to access the Internet, I can't restrict them
17 from doing that.

18 Now if you talk to any of them, they are
19 absolutely, we know the problem, we know we have a
20 responsibility. I think unfortunately today, GoDaddy is
21 a bit of a minority of saying we're a web-hosting
22 provider, we're a domain name registrar, it's our job to
23 police our customers, it's our job to spend our money
24 and our time to basically keep our web infrastructure
25 and the domains that we use used for good.

1 Unfortunately, there are 699 other registrars
2 who don't and haven't been fighting the issue and I
3 think the bad guys are leveraging them and I think
4 that's a problem which is going to take a while to be
5 educated on and that means the bad guys are going to go
6 after it very aggressively.

7 MR. RAMASUBRAMANIAN: Yes, I would like to add
8 only one thing to it. A lot of the problem here is that
9 we get plenty of people in the same room and talking the
10 same things, they are taking the same measures.
11 Unfortunately, this just means that spammers are people
12 who distribute malware or launch D-DOS attacks, will go
13 to the registrars and will go to the countries and will
14 go to the ISPs that don't do this. You still have to
15 deal with them because those registrars, those
16 countries, those ISPs have lots of legitimate users as
17 well.

18 Simply blocking them may not always be
19 practical, in fact, in 99.99 percent of cases of
20 broad-based blocking, it's never that practical. So,
21 the one thing we have to do is engage them and there are
22 several international initiatives that try to do that,
23 with a small amount of success. The problem is that we
24 can't wait for those economies or those ISPs to come to
25 us and say what can we do? We have to go to them, we'll

1 have to use the contacts we have in those countries or
2 those ISPs to do things. I think a subsequent panel
3 will be discussing that a lot, so I'll stop right there.

4 MR. HODAPP: Okay. We had focused, Patrick had
5 focused on four of the spamming requirements, and the
6 fourth one was the action for recipients, which has
7 produced some other problems, I believe, and Joe, could
8 you mention the one in particular that's involved with
9 the hosting, of messing with DNS and the hosting? Thank
10 you.

11 MR. ST. SAUVER: So, I think what you're
12 alluding to actually is the problem of fast flux
13 hosting, so that if you think about the spammers, they
14 want to go ahead and host their web pages somewhere.
15 Legitimate hosting companies want to see those spammer
16 pages. When they get complaints about those spammer
17 pages, they take the spammer pages down. So, just like
18 any other business, the spammer basically faces a real
19 problem, they want to have a stable, reliably available
20 website that they can point customers at. Well,
21 legitimate hosting companies won't allow them to do
22 that.

23 So, what spammers have done now is they've said,
24 well, I've got millions of bots out there, millions of
25 compromised hosts, I can use some of them to host web

1 pages. Now, they don't want to have a single host used
2 for that purpose, they want to have multiple hosts used
3 at the same time. So, if any one host gets turned off,
4 if any one host gets cleaned up or blocked, they're
5 still online. That problem of fast flux hosting is
6 going to become increasingly difficult over time and
7 it's going to be crucial that the registration service
8 providers, the registrars all kind of chip in to go
9 ahead and start attacking that, because this is only
10 going to be able to be attacked at that level.

11 The thing that you are going to run into more
12 and more is spammers are going to start using all these
13 zombie machines for things other than sending spam.
14 Denial of service attacks, we've already seen them using
15 them for that purpose. We know that they're now hosting
16 their DNS service on that. They've basically recognized
17 that they have a very fungible and malleable type of
18 product that they can use for a variety of different
19 purposes.

20 So, these bots, even if you go ahead and block
21 them from sending spam on port 25, they can still be
22 used for a phenomenal number of other purposes,
23 including hosting web pages. When they begin to go
24 ahead and do that, you lose the ability to go ahead and
25 tear them down. It becomes a lot harder to go ahead and

1 attack those sorts of hosts.

2 So, that's an issue that's emerging. We know
3 that there are things that can be done to go ahead and
4 begin to deal with that, in part at the DNS level, in
5 part at the registrar, registry, registration service
6 provider level, but it's an issue that I am not sure has
7 received a lot of attention to date.

8 MR. PETERSON: Just more elaboration. You know,
9 for an example of what Joe is saying, they've hosted a
10 bad site at GoDaddy, I give Ben a call, he takes it
11 down, they've got to go set up another one, it costs
12 them money, it costs them time. We find another domain,
13 like the one I gave the example of earlier, they can
14 extract info from My Canadian Pharmacy, I say, ah-hah,
15 it's being hosted on somebody's PC on the Comcast
16 Network, so I give Michael O'Reirdan a call and he takes
17 it down.

18 And then I check the phone book again, the DNS
19 record, and it's pointing somewhere else. The exact
20 same domain is now pointing somewhere else. So I give
21 somebody else a call, and they could basically point to
22 where that domain goes to lots and lots of different
23 zombies, so as now, whereas before with one phone call,
24 hypothetically speaking, or one block of that, it was
25 effective, now they're doing the fast flux and they're

1 moving it all over their bot network.

2 MR. HODAPP: How fast are we seeing them change
3 the location of the DNS servers or the websites?

4 MR. ST. SAUVER: A lot of times the TTLs or time
5 to live is 60 seconds, so they could literally go in and
6 change it on a moment's notice.

7 MR. RAMASUBRAMANIAN: And the registrars are
8 right now the only single point of failure in this model
9 if you use a domain name, and quite a lot of them
10 currently do.

11 MR. HODAPP: And that has been done, actually,
12 GoDaddy has done that, haven't they, Ben?

13 MR. RAMASUBRAMANIAN: GoDaddy isn't, as somebody
14 else pointed out, the only registrar in the market.
15 There are other registrars who are perfectly happy to
16 take a spammer's money or a malware writer's money and
17 register it. There are other registrars who may not be
18 aware that these are spam or malware domains and they
19 might not have tools or techniques or capacity in place
20 to deal with these issues.

21 So, it is either ignorance or a whole bunch of
22 shades in between. But yeah, GoDaddy is not the only
23 provider in the area where you can get a domain from.
24 Unfortunately.

25 MR. BUTLER: The thing with domain names as a

1 single point of failure for taking down spam operations,
2 it's been that way for a long time, whether they leave
3 the domain name pointed to a particular host for a week
4 or a month or a day or 60 seconds. We are working
5 extremely vigorously within the IT field, the IT field
6 and the governing body for registrars in trying to
7 encourage our competitors to do the same thing. We
8 don't want to have a monopoly on taking down spam domain
9 names. It doesn't do the community, the Internet at
10 large, any good, if only one person does this, as Suresh
11 pointed out.

12 Fast flux is a slightly more involved method
13 that's coming along, and we see it as just another
14 opportunity to identify who the real bad operators are.
15 I can take down a spam website for a guy who maybe just
16 didn't realize that he couldn't buy an email address
17 list and start sending out emails. He can be educated,
18 that behavior can be corrected, but the bad operators
19 who are using fast flux, these are the guys that we
20 really want to identify and go after even more
21 vigorously.

22 So, it's another tool in the tool belt
23 essentially.

24 MR. HODAPP: Ben, that was --

25 MR. RAMASUBRAMANIAN: There's one thing, though.

1 A domain registrar's actions are quite often as much of
2 a force multiplier in this game as botnets are. When
3 you've got one guy who is able to command several
4 hundred thousand bot IPs, quite often he will go and
5 register 200 or 300 domains with the same provider.
6 When you know that there is a fraudulent domain and he's
7 got 300 other domains just like that, you can take the
8 whole lot down and that sets his campaign back by quite
9 a lot.

10 MR. HODAPP: Actually, Ben, your question is a
11 good transition for a question and answer period from
12 the audience. There is from the last panel one written
13 question that I think reflects that and I would like to
14 have anyone who feels they can respond to this. The
15 question was, is it more common to see legitimate
16 senders sending high volume mail from a single or few
17 recognized IP addresses versus a botnet that sends a few
18 messages across a distributed set of consumers' IP
19 addresses?

20 MR. BUTLER: Yes.

21 MR. HODAPP: So, in a way --

22 MR. BUTLER: They all have their own methods
23 that they choose. I mean, we're focusing on the botnets
24 and the very hard core relatively small group of people
25 that's responsible for a bulk of the spam, but all these

1 new tactics that we're talking about aren't replacing
2 the old ones. They're not replacing the misguided email
3 marketer who just doesn't understand the need for
4 confirmed permission. Spam in its old form still
5 exists. We're just trying to focus on what's going to
6 give us the biggest victory with this particular summit.

7 MR. RAMASUBRAMANIAN: Well, for a provider, spam
8 is spam, and when your users are clicking to report a
9 spam, they will report faulty emails from a static
10 service provider which generates a high number of
11 complaints, just like they will report those spams sent
12 from a botnet. Your job as a provider is to integrate
13 all those reports into something useful, and quite often
14 you will find that spam is spam, whether it's sent from
15 a botnet or whether it's sent from a hosting facility, a
16 dedicated hosting facility, the result is the same for
17 your users, it's spam.

18 Of course, the spam might be rather less
19 fraudulent and it just might be unsolicited marketing,
20 but in the interest of it's one piece of email versus
21 some other piece of email as far as an ISP is concerned.

22 MR. HODAPP: There is another question written
23 out that concerns remediation or prevention, and this is
24 a question of whether web hosting occurs over a
25 particular port, and if so, whether a consumer's

1 firewall program can block that port. Could someone
2 address that?

3 MR. RAMASUBRAMANIAN: Joe?

4 MR. ST. SAUVER: Well, if you go ahead and think
5 about it, normally web traffic happens on port 80, so
6 obviously that is something that could indeed be
7 blocked. However, what we have also seen is spammers go
8 ahead and host web services on any arbitrary port. So,
9 if you ever see a URL that says, some web address,
10 colon, and a port number, that's a very obvious way that
11 they can go ahead and get around any kind of filtering
12 that's done on a per port basis.

13 MR. HODAPP: So, when they have a spam message
14 that has a domain name in it, and they're relying on
15 fast flux to give them a different IP address, they
16 could direct it to a different port than port 80 to
17 prevent that?

18 MR. ST. SAUVER: That would potentially be
19 another strategy they could employ, sure.

20 MR. PETERSON: If I wasn't running a web server,
21 I could say don't let port 80 in, because I don't have a
22 web server, and then they would say, oh, if they
23 infected my PC, let's run some software and have it
24 access the web over port 25 or port 22, and if I didn't
25 block those, they could actually get to it kind of in a

1 sophisticated technique.

2 MR. RAMASUBRAMANIAN: Or if it's malware
3 filtering that you have on the PC end, it can always be
4 undone or reversed.

5 MR. HODAPP: Let's get another question. Steve?
6 Steve Baker, the regional director for our midwest
7 regional office.

8 MR. BAKER: One question we've got to ask
9 ourselves as law enforcers is why this matters. In
10 other words, what's the consumer injury? We've heard
11 the Pew woman say that 95 percent of people say this is
12 a nuisance, we can live with it, and a lot of people are
13 saying that 95 percent of the email out there, you guys
14 have identified as spam. Model law enforcers are used
15 to usually having somebody sell diet pills and then they
16 sell a half million dollars worth of those, consumers
17 pay a half million, the bad guy gets a half million, so
18 your consumer injury is equal to what consumers spend,
19 but I wonder if there are system cost is here where a
20 spammer who makes a half a million dollars is costing
21 all of us collectively more than the amount that he
22 takes from consumers. Or whether the costs are really
23 -- the filters and stuff are so low that the consumer
24 injury is really what consumers are losing.

25 MR. PRAED: We're not going to cure AIDS as fast

1 as we would otherwise because drug companies are not
2 recouping the cost of discovering new elements because
3 they can't sell the real stuff because somebody out
4 there is manufacturing counterfeit stuff out of some lab
5 in some basement in India or China, and he's selling
6 that at a third of the cost of what the legitimate stuff
7 can be bought for.

8 Real people are dying from taking those pills,
9 and real people are dying because profit can't be put
10 back into research and development to find new drugs
11 that are going to save us from things that are killing
12 us every day or they're going to start killing us
13 tomorrow. That's just in the pharmacy arena.

14 MR. RAMASUBRAMANIAN: Let's put it this way:
15 Spam is a philandering crime and it's a fraction of a
16 cent from somebody and a fraction of a cent from
17 somebody else and pretty soon you're talking real money,
18 but the generic drugs are doing it as well. You've got
19 quite a lot of legitimate companies in India and China
20 are manufacturing junk pills and you've got licenses of
21 drugs from those manufacturers, reputed alleged people
22 and selling those for a fraction of a cost for what did
23 it take to buy those from a mainstream manufacturer in
24 the U.S. or Switzerland, but the stuff that's being sold
25 by the underground economy is typically things that are

1 manufactured in underground labs or in facilities with
2 poor manufacturing tolerances, or, for example, they
3 might be stealth production runs, sneak into the plant
4 at night and bribe the foreman to run the pill making
5 machines for a little more and nobody is the wiser.
6 Things like that. That is what would typically cause
7 the loss of life or loss of health in pill spam that you
8 are getting when you buy anonymous pills off the
9 Internet.

10 MR. HODAPP: Okay, Suresh, let's see if we can
11 get a couple of more questions. The gentleman in the
12 back there.

13 MS. FOX: Jeff Fox from Consumer Reports. I
14 have two questions related to the use of PCs as bots.
15 One, do we know how many PC-based bots are within the
16 United States versus outside of the United States,
17 because if most of them are outside the U.S., all our
18 efforts to educate American consumers are not going to
19 really have much of an impact.

20 The second question is, it seems to me that the
21 behavior of a home-based PC as a bot, the behavior ought
22 to be quite different than normal everyday activities
23 that most consumers engage in. So, if my home computer
24 begins spewing email or a distributed denial of service
25 attack, perhaps at 3:00 in the morning or when not

1 running my email program, shouldn't it be possible for
2 client software, including firewalls, anti-malware or
3 the operating system, by behavioral patterns, to be able
4 to recognize this and stop it at the client?

5 MR. PETERSON: So, great question --

6 MR. RAMASUBRAMANIAN: Can I take some of that,
7 if you don't mind?

8 MR. PETERSON: Let me jump in first. The first
9 question is yes, unfortunately, the majority of bots
10 today are outside the U.S. There's lots of figures, but
11 I'm sure that no more than 20 or 30 percent of all the
12 worldwide bots, perhaps less now, are outside the U.S.
13 so, certainly we shouldn't, not educate U.S. consumers,
14 but that's not going to solve the problem.

15 On the second question, there are definitely
16 things which bots, even smart ones, the ones who have
17 gone to university, and cloaking what they're doing, are
18 doing, which can be detected, either by your local
19 security solution, your anti-virus or your firewall, and
20 lots of products do that today, and by your ISP. ISPs
21 are deploying techniques more and more to identify
22 things which are anomalous and to either alert the
23 consumer or to stop it from happening. Again,
24 unfortunately it's a boil the ocean problem. People
25 have to install that software, understand it, configure

1 it, but those things are happening today.

2 MR. RAMASUBRAMANIAN: And if I may point out,
3 the reason why you've got rather fewer bots in the U.S.
4 is because the U.S. has, at least according to some
5 figures I saw, less broadband collectively than Estonia
6 has in its own country. When you can get broadband for
7 very cheap, \$30, \$40 for a 50 (mg) broadband pipes in
8 countries, and if you also have a problem that you can
9 buy copies of Windows XP for cheaper than a coffee at
10 Starbuck's, in those countries, well, the bot problem is
11 going to be much more severe there. Even when you have
12 a provider there who is not aware of how best to fix a
13 bot problem.

14 MR. HODAPP: Thank you, Suresh, and thank you
15 for the panel. I found it very informative, and we
16 appreciate all the work you've done. So, thank you.

17 (Applause.)

18 MR. HODAPP: I would like to remind you you are
19 on your own now, and what time? 1:45 is the next panel.

20 (Whereupon, at 12:35 p.m., a lunch recess was
21 taken.)

22

23

24

25

1 AFTERNOON SESSION

2 (1:45 p.m.)

3 UNCOVERING THE MALWARE ECONOMY

4 MS. DREXLER: Welcome back, everyone. Hope you
5 all didn't get too wet out there during that afternoon
6 lunch storm we just had. My name is Sheryl Drexler, I'm
7 an investigator in our Division of Marketing Practices,
8 and I was also involved with the 2003 spam forum that
9 we've heard quite a bit about today, and one of the
10 things in the 2003 spam forum was a panel on the
11 economics of spam, and we're going to talk about that in
12 just a minute, but I just want to first remind you all
13 to please silence any of your devices that you have on
14 you, and if I can remind the panelists please to speak
15 into the microphones or the webcast will not hear you.
16 Also, feel free to fill out those question cards that
17 you have, we will use those during the Q&A session at
18 the end.

19 And so, without further ado, we will move on to
20 this panel. In 2003, as I was saying, we had the Spam
21 Forum, economics of spam panel, and this panel was very
22 different than what we're going to be talking about
23 today. That panel dealt more with what makes a good
24 email marketing campaign, it talked about why we should
25 be using email as opposed to regular traditional snail

1 mail. It really focused more on why we're using email
2 marketing.

3 This panel is going to have a very different
4 focus. We're going to be talking more about these
5 technological tools that we heard so much about in the
6 last panel before lunch. We're going to be talking
7 about why the cybercriminals use these tools. We're
8 going to be talking about what the incentives are.

9 We're also going to be talking about the cost
10 along the email chain to both mainly small businesses,
11 as well as consumers and other interested parties, and
12 one thing that you're going to notice in this panel is
13 we have a definite theme is going to emerge.

14 Previously, email was more about the idea of
15 sending an unsolicited commercial email, and we're
16 talking about spam, it's this unsolicited commercial
17 email that was touting a product. Now we're going to be
18 talking about this shift in we heard Tom Grasso in the
19 first panel and others talk about.

20 We're talking about malicious spam here. We're
21 talking about messages that are phishing messages.
22 We're talking about other messages where the idea is for
23 spammers to exchange data, whether it's credit card
24 information, or underground tools that they're using,
25 the bots, we heard a little bit about the sale of bots,

1 so we are going to be going into all these different
2 tools in this panel, and talking about that shift, and I
3 want to you keep in mind that idea of the exchange of
4 data and the exchange of the tools that we're using in
5 order to have these cybercriminals make money.

6 So, I am going to introduce to you our panel.
7 First we have Andrew Klein, and Andrew is the senior
8 product manager of SonicWALL and he has extensive
9 experience regarding the malware economy and he plans to
10 give us an overview by addressing some of these tools of
11 the trade and how the cybercriminals actually make money
12 with them.

13 Then we're going to hear from Jens Hinrichsen of
14 RSA, the security division of EMC, and Jens is the
15 product marketing manager for customer solutions, and
16 he's going to talk about phishing and crimeware and show
17 us an example of the damage that's actually done by a
18 malicious financial Trojan that's sent via email and he
19 also has some data on phishing that was another thing in
20 the first panel we talked about some of the data, the
21 hard core seeing what exactly is happening in this
22 arena.

23 And then we're going to have Greg Crabb, Gregory
24 Crabb, who is a postal inspector, and he is the manager
25 for the Postal Inspection Service's Global

1 Investigations Division. He's going to talk about some
2 of the places that the cybercriminals exchange the data
3 that they have gleaned from this malicious spam and
4 these other tools and where they're exchanged.

5 Last but not least on the end we have Heinan
6 Landa who is the founder and CEO of Optimal Networks,
7 and they deliver technological and business expertise in
8 the computer network support services arena to both
9 small and mid-sized organizations throughout Washington,
10 D.C., and he's going to talk a little bit more about the
11 financial and physical impacts and productivity costs of
12 spam on especially the small business community.

13 And, so, I'm going to turn it over now to Andy.

14 MR. KLEIN: Thank you, Sheryl. How are you?
15 How's everybody today? I hope you had a good lunch.
16 Let's see if we can get this going.

17 So, I started out in this business several years
18 ago actually trying to get spam, that was my first job,
19 in the whole email security arena. What it caused me to
20 do was to begin to think like a spammer, how would I
21 want to try to reach people. That's an interesting
22 perspective when you get on that side of things.

23 The next thing that kind of came along was
24 phishing, phishing came along a couple of years later,
25 it's been out there for four or five years in some way,

1 shape or form, and what happened there was the game
2 started to change a little bit, the economics started to
3 change a little bit, and one of the things that I
4 started to see was a little bit more organization around
5 the efforts, and we've heard some of that already today.
6 What I did was put together this model, and this is a
7 fairly high level model of what I think the economy kind
8 of looks like. Now, on the outside there is those
9 spammers and those phishers who are trying to do what?
10 Trying to make money. It's as simple as that, and they
11 need to construct attacks and launch them and actually
12 collect information.

13 Now, they used to do that all by themselves,
14 right, a very simple thing to do and at one point they
15 tried to collect everything and tried to turn that into
16 cash. They could turn it into cash in any number of
17 different ways, right? They could just use credit card
18 numbers and sell them through some type of a chat room
19 and sell them for ten cents or a dollar or something
20 like that, potentially they could use the credit cards
21 themselves for false transactions.

22 All kinds of different ways that they could try
23 and turn that into cash, but other information started
24 to show up as well. Account information, for example,
25 log-ins and passwords, and they had no particular thing

1 to do with those. But they kind of kept them around.

2 That outside circle worked for a while. But
3 what was starting to happen was, the inside. That whole
4 malware community, which has been around for years, they
5 talked about it this morning, it's all of these folks in
6 their basement and living in their mom's basement for a
7 number of years writing code, doing nefarious types of
8 things. But what started to happen was that code
9 started to become organized. People started to talk to
10 each other. They started to trade back and forth that
11 information. Let me kind of go through some of those
12 examples.

13 So, the first thing we talked about today, and
14 it's been talked about on a couple of different panels,
15 is botnets, right? One of the tools of the trade is
16 botnets. All right, they send out lots of spam, lots of
17 ways to compromise a machine so that I can use that
18 machine for whatever the purpose I want to use it for,
19 whether it's sending out spam or phishing or something
20 like that, whether I need to store images on there, so
21 on and so forth. There have been examples over the
22 years where people have done that.

23 For example, Mr. X, he was a Dutch spammer, he's
24 in jail now, by the way, and he had created his own
25 little botnet, 600 or 700 machines which he continually

1 replenished and he used those to send out spam messages.
2 So, you could create your own. Or, if you weren't that
3 industrious, you could go rent time on one, and here's
4 the typical or a couple of examples here.

5 You could get from about \$300 to about \$700 an
6 hour, renting time on a botnet. Now, what does that get
7 you? I have an attack and I want to launch an attack
8 and I need to send out 25 million spam messages. I
9 could do that in a couple of hours, \$600, \$1,000,
10 whatever the cost may be. That's my cost to start that
11 ball rolling, right? The example there, both of these,
12 by the way, have both been caught, and in parentheses,
13 that 19, is their age, all right? That's what they're
14 doing these days, and by the way, you can see the kind
15 of money they were making, and both of them got caught
16 not because they got caught, but because they got turned
17 in. Why were they driving a Ferrari with no visible
18 means of support? It was that kind of thing.

19 So, they're somewhat part of a community which
20 allows them to create these things and sell them, all
21 right, but there's no mass organization. There's no
22 building where all of these guys go to work in the
23 morning. All right?

24 So, but they still work together. The question
25 also came up about how many compromised machines out

1 there, and the estimates have been a little all over the
2 board. The low I've seen is like 49 million out of an
3 article in USA Today, 70 million from Trend Micro as you
4 can see there, and Vint Cerf, okay, estimates it at well
5 over 100 million. I don't care what number you want to
6 choose, that's a lot of machines. So, when the FBI says
7 they're going to contact a million people, okay, that's
8 scratching the surface.

9 Now, I applaud their efforts, by the way,
10 because I think that's an excellent thing to do to bring
11 this whole subject up, and get it distributed out and
12 let people know what's going on, there's still a whole
13 lot more work to do.

14 There's other tricks that we've seen out there.
15 Domains, and we've had a couple of folks on the panel
16 beforehand that were on there and dealing with domains
17 and domain registrations, all right? All of those that
18 are listed there on the left-hand side, all right, all
19 of those were active phishing domains when we got there.
20 All of them. By the way, that's just a short list, some
21 of my favorites. The list can go on and on and on and
22 on. All of them, by the way, are highly confusing to
23 potentially end users. Secure-ebay.com. That could
24 pretty easily fool somebody.

25 By the way, most end users, great survey, if you

1 want to run it some time, what's the difference between
2 a .com, a .net, a .info, a .US, a .org, okay, whatever,
3 as it relates to the businesses you're dealing with?
4 Most users can't distinguish that. So that's what the
5 confusion is out in the marketplace with the people that
6 we deal with on a regular basis.

7 Some of my favorite ones that have happened over
8 the years as it relates to things like domains, Experian
9 issued that as a self certificate, citybank.de.

10 By the way, that's not the only that happened,
11 but a phisher was able to get an SSL certificate so that
12 when you went to a site, it was actually secure, you
13 could give away your information in a secure
14 environment. All right.

15 So, but what this all points out is how hard it
16 is for these organizations to monitor and maintain that.
17 That came up this morning, too, you heard the guy at
18 GoDaddy say, we're doing lots of hard things, all right,
19 and they, paying them \$3.99 per year may not be the
20 right thing to do, okay? Maybe we should pay them \$4.99
21 and dedicate that other buck to security or something
22 like that, but that's the game they're in.

23 They're in a highly competitive space, and the
24 thing that goes first is security. Things like checking
25 the registrar records when somebody registered. I've

1 seen domains registered to Bugs Bunny, okay, Don
2 Corleone, I've seen one registered that went the
3 following, I need to type something into these fields,
4 return, because if I don't, return, it will be
5 suspicious. That's the kind of thing that could be put
6 into a record. All right?

7 Other tools of the trade. I bring these up
8 because these are all banks that have been hacked in one
9 way, shape or form or another to host phishing sites.
10 All right? One was a direct bank, it was a bank in
11 China about a year or so ago that was hacked and was
12 hosting ebay sites. So, the reason is that there's
13 people out there that do this for a living, all right?

14 There's another one that provided a service, so
15 the bank itself actually didn't host its own website, it
16 went to a service to do all of that, and actually run
17 all of those kind of transactions for it. That service
18 got hacked, and subsequently all of the sites got
19 hacked. Okay? Or not all of them, they couldn't get
20 through all of them before it was discovered.

21 And then even hosting services, so I want to run
22 my own stuff, but I don't run my own servers, I run them
23 somewhere else. Any time, okay, you are running an
24 institution like that, okay, good-old-fashioned, tried
25 and true methods of hacking your machine still work.

1 All right? Why do you get corporate phishing? Why do
2 people send phishing emails to companies, to get credit
3 card numbers from your employees? Well, that's one of
4 them. But there's also things like your log-in is going
5 to expire on your Outlook account, you need to redo it
6 kind of phishing attacks. Well, what are they really
7 looking for there? They're looking for a way to access
8 your network, so they can use your machine for some of
9 the things that they were talking about in the earlier
10 panel. All right?

11 So, there's lots of different ways, reasons that
12 they need to get into machines. What's happened is that
13 people are starting to make money with these things.
14 So, here's a spyware kit for sale, \$17, and it comes
15 with technical support. You can't get that from
16 Microsoft. Or any other company. My company, included.
17 All right, for \$17, you can buy a spyware kit.

18 Think about that. Somebody invented it, put it
19 for sale, and sold it. Then is offering to support it.

20 Earlier this year, there was the Panda Virus, I
21 think back in the February time frame. Panda was a
22 virus that a student created and then sold about to 120
23 different people at \$100 a throw. Now, there's two bad
24 things about that. One is there were 120 different
25 people that wanted to buy this, okay, and two, they

1 could buy it. The Panda Virus was written in a way that
2 he actually gave his source code and everything and you
3 could actually manipulate it so you could create
4 variants of it so it couldn't be caught. That's a very
5 typical strategy now, viruses mutate almost
6 instantaneously out there.

7 But it goes show that people are beginning to
8 not only create tools and sell it, but they're selling
9 the pieces of them for money. That creates that second
10 level of the economy.

11 On of the things that Jens will talk about
12 shortly as far as phishing, but there's this notion now
13 of phishing kits. Now these have been around for years,
14 but the breadth is really impressive. You have a
15 product portfolio of as little as \$30 up to \$3,000, with
16 all kinds of great capabilities in between. You can
17 just imagine a big checklist that says here's all of the
18 great features you get in this one and you get these
19 extra features in this one and you pay more and you get
20 this and this and this, just like a regular product.
21 You can go to sites and find those kinds of evaluations.

22 I like the one here, there was a little variant
23 that was done to improve phishing kits that you
24 incorporated what's called a universal man-in-the-middle
25 phishing kit, but it was a new technique that was out

1 there, and it was introduced as part of a phishing kit,
2 and it allowed the phishers to do some things they
3 couldn't do before, and the quote that came, from a guy
4 in RSA by the way, by the way, is that it offers a much
5 better return on investment.

6 We're talking about these things in terms of
7 regular business software. I would love to be able to
8 write software that somebody writes that about. Right?
9 That's what you strive for. I want a big product
10 portfolio, that lots of different people can buy so I
11 can satisfy lots of needs, right, that provides what? A
12 really great return on investment. That's where they
13 are today. That's where these folks in the middle are,
14 in creating these tools, sharing them amongst
15 themselves, right, not only the tools themselves, like
16 phishing kits, but all of the infrastructure pieces
17 underneath. Virus, right? Botnets and so on. All of
18 that moving around in that economy.

19 So, what I'm going to do now is I will introduce
20 Jens and have him talk a little bit more about phishing
21 as one of the drivers about it, he's got some really
22 cool slides, as she mentioned, about an attack. So,
23 thank you very much.

24 (Applause.)

25 MR. HINRICHSEN: Good afternoon, everybody, I'm

1 going to apologize in advance for my croaky throat. So,
2 if I change pitch a couple of times, it's just my cold
3 at fault.

4 In any event, thanks again, everybody. Just as
5 some background, I work within what's called our Online
6 Threats Managed Services Group, I know that's quite a
7 mouthful, but we're really focused on everything
8 external threats related, namely phishing,
9 crimeware/Trojans, as well as from an intelligence
10 perspective, and really much of what Andrew was
11 describing before, the sophistication, the demarcation,
12 the level of really specialization in the underground
13 economy across tools, across how the fraudsters
14 communicate, exchange monies and whatnot.

15 A few of you have seen a couple of these slides
16 that I have used at a couple of presentations before,
17 but I think they underscore an important point as to the
18 relationship between consumers and institutions. Really
19 what obviously the imperative is from the industry
20 perspective, about what's at stake here from trust, from
21 usability, and really return behavior from the entire
22 online channel.

23 This might be a little bit of an eye chart, but
24 we do a consumer study, we obviously have feedback both
25 obviously qualitative and quantitative from our entire

1 customer base worldwide, but we want to make sure that
2 we're capturing end user feedback, like you or I as we
3 navigate the web, we use the web, we do online banking,
4 we use our credit card for certain e-commerce purchases.

5 Two key things: The first in the light blue
6 background says, "Are you less likely to respond to an
7 email from your bank because of the phishing
8 phenomenon?" And clearly, you can see about half are,
9 that shouldn't be a surprise, so that's just kind of a
10 level-setting statistic. The more pointed statistic in
11 terms of really how it impacts the economy, and I think
12 the trend here is interesting, year over year, the other
13 question in white says, "Are you less likely to sign up
14 or continue to use your bank's online services because
15 of the phishing phenomenon?" And this is just couched
16 within phishing. This is not, obviously, the emerging
17 and rapidly emerging crimeware or broader malware space.

18 So, what we saw here a couple of years ago was
19 17 percent of users said they were much less likely to
20 use their bank's online services. Again, I know this is
21 couched within financial institutions, but obviously it
22 relates to other industries.

23 Then we fast forward a year and we go to '05 and
24 it's an encouraging trend. Basically more than half of
25 an improvement to just seven percent of users saying,

1 gosh, you know what, because of phishing, I'm more leery
2 and I'm not going to use online services because of
3 that.

4 Now, interesting, though, then when you fast
5 forward a year again to the end of last year, that
6 number jumps right back up again. Really, the
7 supposition here is that the collective ground swell of
8 concern about all of the threats that encompass a user
9 experience in their online experience, whether it's the
10 crimeware or whether it's spyware, ad ware, ransom, or
11 all the wares that are out there, there is certainly an
12 impact on customer comments.

13 Phishing, whether you get down the stream of
14 what role education plays, certainly it goes up to a
15 point. I think a lot of folks were basically saying,
16 I'm more used to this, I get phish emails a lot, I
17 either ignore them or delete them. That's all great,
18 when we think of how that breaks down in terms of the
19 crimeware economy, I think the key point that's been
20 already touched on today is that blurring or that
21 blending.

22 Phishing, crimeware, malware, and really that
23 tandem use of fraudsters for social engineering and
24 infecting users with whether it's a botting form of
25 malware or whether it's a multipurpose piece of malware

1 that's not only going to bot their machine but also has
2 very specified crimeware. Crimeware again being either
3 identity theft or session hijacking to actually
4 ultimately take out funds and transfer funds out of an
5 account.

6 So, again, from a consumer's perspective,
7 there's still a certain level of trepidation that
8 exists. The key point that I want to talk away here,
9 and I do apologize, when we had submitted these, we
10 didn't have our most recent monthly data. We're seeing,
11 again, about 200 unique institutions that have been
12 targeted on a worldwide level that are being targeted by
13 phishing.

14 The key point here is not so much the number of
15 institutions by month, and I didn't even bother to put
16 up the number of unique attacks, because certainly given
17 some of the forces at play here, whether it be rock and
18 others, depending on how you count it, it can be
19 possibly misleading, but the key take-away here, if you
20 fast forward to just last month, so I apologize it's not
21 in the chart, but in June, of around the 200
22 institutions targeted just by what we call classical
23 phishing, nearly 35 had never been attacked before.
24 Thirty-five. It's a staggering number.

25 So, when we think about this fear of phishing,

1 phishing is not going away anywhere soon. We keep
2 raising the point as well about ROI, it's darn easy.
3 One of the recent discoveries of our team, and Andy
4 described it best, when you look at the spectrum of just
5 phishing kits that are out there, whether it's really
6 sophisticated phishing-based man-in-the-middle kits or
7 your original kind of static HTML kit, we discovered an
8 interesting other revolution to bring, the newby
9 fraudster in with a plug-and-play phishing kit.

10 Instead of having to go in and insert different
11 files into different folders on a compromised server,
12 within a double click, just as you would install any
13 other software, a newby fraudster or even a fraudster
14 who wants to become more efficient and launch an attack,
15 within two seconds, two seconds an entire phishing
16 attack is ready to go.

17 That's a pretty staggering improvement when you
18 think about just ease of use and productivity and when
19 you continue to use these economic terms within the
20 fraudster economy.

21 So, of those 35 institutions that we had never
22 seen attacks against before, about a dozen of them, if
23 we think just from a U.S. perspective, about a dozen
24 were federal credit unions. That's another point. I
25 mean, we have certainly seen for many, many months now,

1 a transition, actually years, I should take that back,
2 the transition to well beyond the financial sector.

3 So, it's targeting any kind of institution that
4 has valuable credentials to be had, or gets a lot of
5 traffic. If there's the cover story there to lure
6 somebody using what might be considered either a spam
7 email or as a phish email, but if it's a cover story
8 that's nebulous enough, and the user isn't suspicious
9 about, oh, this is a financial institution related kind
10 of phishing attack, they might follow it. Whether it's
11 viewing certain kinds of content, web albums, E-cards,
12 you name it, the whole point of the fraudster is to get
13 the user obviously to a page where they can infect
14 either with a botty piece of malware or potentially
15 crimeware.

16 The real take-away from this slide, and we all
17 read about how looking just again within the spirit of
18 what we call phishing has been evolving, the real
19 take-away here is not so much the technologies and the
20 methodologies and the approaches, I think what we're
21 really seeing from our anti-fraud command center
22 perspective is the prevalence by which these
23 technologies and methodologies are taking place in
24 upticking.

25 When you look at, for instance, phishing-based,

1 man-in-the-middle attacks, they were kind of rare some
2 time ago. It's common practice. You know, even over
3 the last six to nine months when you looked at the price
4 of phishing-based, man-in-the-middle kits, selling
5 curled spam pages, it went from several hundreds of
6 dollars or thousands of dollars down to a hundred or
7 less, and we're really seeing a lot of price
8 compression, certainly, in terms of the kinds or tools
9 available, and we'll touch on that again in just a
10 second.

11 A couple of take-aways here, not only from a
12 growth perspective, we all see it. We all see crimeware
13 growing rapidly, but clearly is the notion of how do we
14 from an end-to-end perspective as an industry collected
15 best protect. I think many of us who are involved with
16 the anti-phishing group, there has been some terrific
17 work going on there from either a registrar or
18 registree's best practice.

19 Number one, just making everybody aware of how
20 big and nefarious and problematic this issue is, but
21 what are some of the very simple steps that we can do to
22 expedite, once you identify sites or domains that are
23 hosting whether it's phishing attacks, whether it's
24 crimeware or what, how can we really expedite that time
25 to shut down, blocking and shut down, obviously, and do

1 that, because when we think about signature-based
2 desktop protection not being enough, and with the arms
3 race ever continuing and with thousands of new variants
4 always out there in the race to write a new signature.

5 In one example, our Trojan lab we looked at,
6 we've heard of Gozi, or bank snippit, as it's also known
7 as, in a single month it affected 30,000 users and
8 before it was detected by AV. Just one variant out of
9 the whole lot of them. It gives us obviously an idea of
10 how big and problematic this issue is.

11 So, in terms of the price compression, or
12 actually, I'm sorry, I jumped a slide there. Another
13 point, and again this is a slide I've used in a couple
14 of forums, is back to the consumer confidence and that
15 impact on the relationship with whatever entity it is
16 that they were working with, whether it's a financial
17 institution or what.

18 This study, remember, this data point was from
19 about six months ago, so it's a little bit long in the
20 tooth, but the take-away is more than half of users,
21 online users worldwide were already increasingly
22 concerned about Trojans or crimeware, and while in our
23 circles, we obviously know about this and we've known it
24 intimately for some time.

25 Phishing, yeah, we can understand. We can

1 understand users being more and more educated and aware
2 of phishing, but it's a rather telling statement when
3 nearly half of online users, particularly in some areas
4 that haven't yet been hit a lot by crimeware, the U.S.
5 being one, relative to Brazil and Germany and other
6 regions like that, or countries like that, it's a rather
7 telling take-away. Certainly we expect this to uptick
8 very rapidly.

9 Here's just one of a whole lot of examples that
10 we could use, in terms of price compression. This is a
11 fairly substantive and fairly capable Trojan and we've
12 got to love the moniker super Trojan, as this fraudster
13 who is a trusted reviewed vendor on one of the forums,
14 had referred to it as. But you can see, and again, it's
15 an eye chart, but for those who can't see it, just \$600
16 for this piece of a rather sophisticated piece of
17 crimeware. Compressing everything, all the tools in the
18 economy coming down at I think a rather alarming rate.

19 Here's just one of many, many examples that we
20 see as well, unfortunately we don't have a flash working
21 behind this, but this is one example of some flash
22 demoing or I should say flash advertisements that are
23 being used in the underground. They are trying to get
24 attention. They are trying to raise their hand and say
25 buy my wares, buy my materials, and to the a service

1 support perspective, not only have we seen a lot of
2 crimeware, obviously there are a lot of these these
3 days, but the vendors of these are offering patches or
4 updates that if the latest AV detects it, they're going
5 to sell for \$3.95, \$5.95 a patch to what you have
6 purchased. To basically say, okay, now this will bypass
7 the latest AV and your crimeware that you bought from me
8 will continue to be meaningful and be accretive in
9 actually deliver the ROI that you were hoping.

10 This is one example, and again, unfortunately,
11 we weren't going to be able to show a video for the
12 webinar purposes, so I'm going to go through a few
13 screenshots. To qualify it, this is a very, very, very
14 basic piece of crimeware. I had mentioned briefly
15 before, there are two general classes that we are
16 focused on, one is the identity theft crimeware, which
17 will infect your machine through a number of ways,
18 whether it was social engineering related, you think of
19 all the social networking sites out there these days,
20 Web 2.0, drawing people to possibly hit content or
21 interact with content that will silently infect their
22 machines.

23 The majority, still, will steal credentials when
24 you, the infected user, go to a targeted site. It could
25 be ten financial institutions and a few e-commerce

1 sites, for example, or hundreds of financial
2 institutions, that identity theft, whether it's the key
3 log-in screensaver or the local harming Trojan, will
4 wake up when that user hits that target site, and then
5 silently steal the credentials.

6 The other more nefarious, which we have
7 obviously seen in places like Germany which is really
8 driven by one-time password and strong authentication
9 are those session hijacking or funds transfer pieces of
10 crimeware that are going to be either in the background
11 or take over that session once the user has logged off.
12 This is a very, very basic version, and really it's just
13 to demonstrate for maybe a few of you who haven't seen
14 it in action before, how it operates.

15 Here's one called Limbo, version 1.5, gets back
16 to our service statement, 1.6 is coming out next week
17 and be ready for it, it's only going to cost you \$2.95
18 as an example. It plays itself off to be a browser
19 helper object, and so if we go to the genuine log-in
20 page of our friends at Barclays, this is how the page
21 looks, and down below you can see the log file for the
22 Limbo, basically the log manager call it for in terms of
23 what credentials are being stolen, et cetera, et cetera.
24 Here is the genuine page, and you can go through, you
25 would enter your surname, membership number, just as a

1 genuine user would. So, that would be the real
2 experience, and the machine is still clean.

3 What we do, then, is if this has actually
4 infected a machine, the user would experience something
5 different, and as I mentioned, this is a very, very
6 basic piece of crimeware. This is injecting new
7 credential-stealing fields. Name the field, and
8 depending on the target, depending on the cash-out
9 mechanism or vulnerability or whatever the fraudster is
10 aiming at, they would obviously change the injected
11 questions.

12 In this case, it's as basic or as simple as ATM
13 number, ATM PIN. That obviously wasn't there before.
14 Now, grant it, it's not perfect and there's still going
15 to be a percentage of users who go, oh, someone is
16 phishing, and I don't mean that in the pun sense, but
17 something is not right here, but stepping up the game,
18 certainly a more credible from a fraudster perspective
19 approach than simply sending out phishing emails and
20 relying on people actually responding in that sense.

21 So, what happens is the user would go through
22 and if they fall for this, they would do the usual
23 surname membership number, and oh, maybe this is some
24 increased violation, maybe I have to put my numbers in
25 here, my ATM number and pin, and they do that and you

1 can see you down below in the log the fact that it's
2 actually being captured there and readily available or
3 accessible by the fraudster to either use his or
4 herself, or as we've discussed time and time again, sell
5 it in the underground for a specified amount per
6 credential.

7 You see here your Trojan configuration file
8 contains special actions for different targets. That's
9 a key point, you're always pushing out new variants. Do
10 you want to do something different for a certain
11 institution, aside from just trying to bypass AV, they
12 might have different actions. They want to do per
13 institution, and you can see some of those that have
14 been censored here, but that's there in the code that
15 you can see that goes into more detail about the
16 Barclay-specific modification as well.

17 So, that's just one of the many, many, many,
18 many examples that I know, actually many of us could
19 probably share in this forum as well, to give an idea of
20 the spectrum of tools that fraudsters are very, very
21 commonly and frequently utilizing and employing.

22 One other, and I'm going to take just a quick
23 tangent here. There's a whole scale or I should say
24 assemblage of slides that I would often go into from a
25 fraudster economy, latest trends, where is a lot of the

1 fraudster chatter focused on. You know, this is one
2 that we're seeing in the U.S. While wire transfer has
3 been and still is the prevailing cash-out mechanism for
4 fraudsters, there's been a huge increase, and we've
5 certainly seen a lot of chatter about fraudsters looking
6 for certain vulnerabilities and easily setting up bill
7 payees. Either getting access to an account that
8 already has billpay set up or getting an account and
9 setting up a fake billpay address. Then that is one of
10 the many mechanisms they might use to actually cash out.

11 So, a little tangent, but just kind of
12 connecting the rubber to the road here a bit.

13 In terms, though, of what we should do, there
14 are obviously many things. There are a lot of things
15 that, whether it's financial institutions or other
16 entities can do, but I think the real value here
17 certainly, and going back to the comment before about
18 what the collective, just for instance one entity, the
19 Anti-phishing Working Group has been doing is raising
20 the awareness of how big, how nefarious and how fast the
21 threats are evolving, and from that baseline across all
22 the entities and players involved in this system that we
23 have here and all of us here is obviously then being
24 able to put some very basic processes, levels of
25 understanding, ways to engage in terms of saying, okay,

1 we have a site that's being hosted by this party here,
2 this is the best way ultimately for us to get, say, that
3 infection point shut down.

4 Again, we could wax poetic and/or prosaic for a
5 while on best practices, but that's the quick overview.
6 So, thank you for the time today, apologies for the
7 throat, and I am going to pass it now on to Greg.
8 Thanks a lot.

9 (Applause.)

10 MR. CRABB: Good afternoon. Thank you for
11 giving me an opportunity to speak about a problem that
12 I'm very passionate about, and I think that in the law
13 enforcement community, it's kind of hard to understand
14 all this stuff about malware and computer viruses and I
15 think we as law enforcement officers have challenges
16 trying to contend with these challenges, the
17 complexities of these crimes, they're not user friendly.
18 Most of our law enforcement officers, my law enforcement
19 officer colleagues don't necessarily get cybercrime, but
20 I think it's an important problem, because it goes to
21 the heart of our business.

22 We've talked, heard about every panelist talk
23 about the business impacts of these crimes, and I come
24 representing an organization that is a provider to all
25 of you, and that's the U.S. Postal Service, and as a

1 proud Postal employees, I hope that the work that we're
2 doing in the cybercrime arena can help to improve the
3 economics of the Internet, and that kind of gives you a
4 perspective on why I come from a law enforcement
5 perspective into supporting this arena, because it's
6 about the business.

7 We need to be able to support the business users
8 that rely upon our mail delivery services, our package
9 delivery services, because these criminals are stealing
10 the identity information of our consumers, and using
11 those against our business infrastructures.

12 To talk about the malware economy, I came at
13 this from a very odd perspective. I came at this
14 looking at it from a financial crime perspective. This
15 to me was not about a computer crime, it's about stolen
16 identity information. It's about financial crime. All
17 of the sudden, you end up in the middle of a bot network
18 with tens of thousands, hundreds of thousands of U.S.
19 consumers' data on a laptop that's recovered from
20 Eastern Europe, and who are the people that are behind
21 these crimes that are responsible for this? And, so,
22 that's the focus of my presentation.

23 My experience comes from a joint investigative
24 intelligence initiative that I've been running with my
25 good colleagues that Tom, the X-man Grasso opened up

1 this morning, and Special Agent Man Keith Mularski will
2 talk about the National Cyber Forensics and Training
3 Alliance tomorrow afternoon, but we've been working
4 together for a number of years around this problem, and
5 I think that we need not only law enforcement
6 assistance, but we also need private industry
7 assistance, because these are highly technical
8 investigations.

9 The base of our knowledge is the work around the
10 forums and a couple of speakers have talked about the
11 forums, and together with the FBI, we've successfully
12 conducted operations against a number of these forums.
13 At one time, we were monitoring over 3,000 criminals
14 that were engaged in some of the forums that are listed
15 here. Fortunately, most of these are defunct now, but
16 you can be assured that we are currently engaged in a
17 number of operations that relate to the active world of
18 these cybercriminals and their forum activity.

19 My perspective on malware from an investigative
20 perspective has been around phishing. I had the
21 investigative experience and fortune to be out in San
22 Francisco for a number of years and worked some early
23 cybercrime cases that related to the phishing
24 sub-culture that developed in some of these forum
25 arenas, and it's just, as you know, exploded over the

1 last five years.

2 Interpol is very active in combatting phishing,
3 we've got an operation that we call Operation Gold Phish
4 that has the participation of over 20 countries, law
5 enforcement, plus private industry participation to
6 attack the criminals that are using the malware to be
7 able to steal identity information, and Gold Phish is
8 kind of a misnomer now, because it started off as a
9 phishing focused operation, and as soon as you figure
10 out that you need some spam in order to facilitate
11 phishing, you're well into the malware economy. Through
12 this operation, we've shared and worked with law
13 enforcement on over 500 subjects around the world.

14 So, who are these subjects? Who are the
15 criminals that are behind this activity? And I've
16 pictured, put pictures up of some of these people that
17 we've run across in our investigations. Some of them
18 have strong connections with Russian organized crime.
19 Others are of Middle East dissent. Others are kids here
20 in the United States who are engaged in the criminality
21 of this activity. There is a prevailing youth behind
22 these photographs. You know, a lot of these kids are
23 young. You know, anywhere from typically 18 to 25 years
24 old. However, that doesn't mean that organized crime in
25 Eastern Europe or elsewhere have not gone to these

1 individuals and leveraged the capabilities that they've
2 been able to develop to attack the computers of our
3 consumers to be able to further their crimes.

4 So, I've got a couple of examples of forums,
5 postings that relate to the sale of malware. This is a
6 posting that's on a Russian forum that we've been
7 watching that the seller of this, his screen identity is
8 Barracuda, and Barracuda sells a computer virus I think
9 for about \$300 U.S., and he will gladly take your money
10 in a transfer on a digital currency called WebMoney.
11 This particular virus will do everything from steal
12 identity information on the computer that it's loaded
13 onto, or facilitate spam, you name it, it will do it.

14 And not only do these criminals conduct these
15 activities for spam, it's also denial of service
16 attacks. This particular bot was used in the highly
17 publicized Estonian D-DOS attacks. Here's his avatar
18 logo, and some of the controlling channels, screenshots
19 that some of the controlling mechanisms behind his
20 particular bot.

21 And then a target that has been a thorn in my
22 side for a long time, but is definitely something that
23 needs to be recognized as a problem, and that is these
24 criminals are outside the United States, not only was
25 the writer of Barracuda outside the United States, but

1 this individual, Smash, who he's been written up in the
2 press quite a bit, remote access Trojans, RAT systems,
3 was the website that he sold his particular virus from,
4 he is definitely not in the United States, from Eastern
5 Europe, and we have trouble as law enforcement officers
6 being able to bridge the gap between these crimes and
7 something that's recognizable on the books of foreign
8 law enforcement.

9 In monitoring the cash flow, we do a lot of
10 different types of investigations against these
11 subjects. We'll trace the communications, we'll trace
12 their money flow, we will try to do whatever we can in
13 order to get back to the true identity of the
14 individual, and in this particular instance, we were
15 able to trace some of the proceeds, and some of the
16 communications of this particular individual with some
17 subjects in the United Kingdom, and for me it wasn't a
18 financial crime investigation.

19 The subject was using this particular virus that
20 was sold by Smash to steal identity information,
21 identity information of UK citizens, and it looked,
22 smelt and felt like financial fraud to me, and in
23 November of 2004, I had an opportunity to write a report
24 to the UK on a subject that was using this virus to
25 steal identity information.

1 We provided the report to him, the subject we
2 monitored some of his communications, who was a Muslim
3 living in the UK, and this particular chat that we
4 recovered, the community thought that he was trusted
5 because he was of Muslim decent. Fair enough. But when
6 it came down to it, he was later arrested by New
7 Scotland Yard, their National Terrorism Financial
8 Intelligence Unit, for conspiracy to murder, incitement
9 to commit terrorist acts and possession of articles for
10 terrorism purposes.

11 Now, obviously the financial crime that was
12 related to that is maybe not as significant, but these
13 criminals not only have financial intent, but we're
14 starting to see more and more where the subjects are
15 based in the Middle East, and have terrorism as a
16 motive.

17 There was a nice write-up in the Washington Post
18 a couple of days ago, about this particular case, and
19 its tie of how spam and email was associated to stealing
20 identity information that was used to be able to fund
21 this activity.

22 So, I hate to leave or end on this particular
23 note, because the mass majority of the crime that
24 relates to the malware economy relates to financial
25 crimes, but we have to be cognizant of the fact that we

1 are on the verge, I think, of seeing more and more of
2 these terrorism organizations and others trying to
3 penetrate our networks, to further their schemes.
4 Fortunately in this case, all three of these individuals
5 pled guilty, I think it was July 4th, and were sentenced
6 on July 5th to sentences between I think seven and ten
7 years, but we need to take these crimes seriously.

8 And on that note, I want to turn it over to my
9 colleague, Heinan, and thank you very much.

10 (Applause.)

11 MR. LANDA: Hi. Oh, good, I love it. My name
12 is Heinan Landa, and let me give you some context. I'm
13 going to actually be flipping a coin a little bit,
14 looking at the other side. We've seen a lot about how
15 spammers and those perpetrating malware can actually
16 make money. Now let's look at the side from the point
17 of view of small businesses. And small, medium-sized
18 businesses in the United States and what kind of damage,
19 financial damage, and other types of damage, that these
20 types of malicious software can cause.

21 Let me give you a little context. My company is
22 Optimal Networks, we're located right up here in
23 Gaithersburg, and we are providing IT outsourcing and
24 network support services to small and medium-sized
25 businesses, exclusively in the D.C. area. So, my

1 clients might range from a small size of about ten
2 employees all the way up to about 200.

3 And when I first accepted the honor of being on
4 this panel, I was thinking, oh, this will be fun, I'll
5 come out and talk a little bit about spam, we do quite a
6 lot with spam. In fact, we are now offering what are
7 called managed services, which is a fixed price per
8 month per PC where we basically promise our clients to
9 do all the preventative measures against all the
10 malware, spyware, anti-virus, anti-spam, patching, all
11 that kind of stuff, so the cost of this prevention and
12 the cost of recovery is actually very important, because
13 it affects our day-to-day business operations.

14 So, I said, this will be great, I'll come and
15 talk about our clients, the effects of spam and the
16 effects of spam prevention on our clients. But when I
17 was starting to do research, and I'm not sure if you're
18 aware, but as far as an economic force, small businesses
19 in the United States comprise about 50 percent of our
20 nation's GDP, non-farm. So, it's 50 percent of the
21 gross domestic product, which is six and a half trillion
22 dollars.

23 That's a major, major economic force we're
24 dealing with. So now I feel like I have to actually
25 stand up straight and wear a tie and talk about it.

1 So, let me start with a few anecdotes. So, you
2 can understand qualitatively what malware can do to
3 these small businesses, and I actually solicited some
4 input from all of our clients to see if I could give you
5 some actual hands-on stories, and one of the first
6 places where our clients were affected very dramatically
7 by spam, and you saw this in the previous panel, was in
8 the directory harvest attack.

9 So, this is when the spammers are trying to
10 acquire the addresses to spam to. They are bombarding
11 email servers with false emails. Right, trying to
12 figure out which emails addresses are correct for those
13 servers.

14

15 Now, let's take a look at this, away from the
16 consumers. Most consumers are using the email servers
17 in their Internet service providers, Verizon, Comcast,
18 they're using those email servers. Most large
19 businesses have their very robust email servers. Most
20 small businesses also have their own email servers, but
21 they are not quite as powerful as what you might see in
22 the large businesses and the Internet service providers.

23 So, when a spammer tries to harvest addresses
24 from one of my clients, and I'm talking particularly
25 about one of my first clients who got hit with this, a

1 30-person trade association, and they started pummeling
2 that server with tens of thousands of email messages
3 every day, and opening up direct connections into the
4 server, trying to find out the addresses, and that
5 server said, oh, I don't know any of these people, and
6 started trying to bounce back, hey, this is not
7 deliverable, this is not deliverable, this is not
8 deliverable, and then they couldn't get it through those
9 messages, had to wait four hours and do it again and
10 again and again. It was a matter of two days before the
11 server collapsed, just knuckled under.

12 This started happening client after client after
13 client, because I don't know if you're been following,
14 but there's really been an explosion of directory
15 harvest attacks and it's increasing dramatically, and
16 you can see why.

17 The only solution was for them to incur yet
18 another cost and put in more spam filtering software on
19 the network and engage in outside spam filter, which put
20 them out of commission for a week. On average. Across
21 our client base. So, that's one aspect of it.

22 Another aspect of it is a church. One of our
23 clients, when we first got to them, one of their senior
24 pastors had received a spam, clicked on it, malware
25 infected their system, lost years and years worth of

1 documents, spreadsheets, Word documents, just wiped out
2 his system right there.

3 My client writes me that it cost him thousands
4 of dollars to recover from that, and to this day, four
5 years later, they're still not out of the effects. They
6 needed that information, they were storing that
7 information for their parishioners and they were using
8 it to run their church. So, how do you measure that?
9 I'm not quite sure.

10 One of our clients is about a 70-person company
11 in Rockville that manufactures specialized baby food.
12 They are using the spam filtering service, they have
13 about 25 salespeople spread across the United States,
14 and their IT director estimates that even with the spam
15 filtering, the multiple levels of spam filtering that
16 they have, they have still lost ten full days of
17 productive salesperson time because of malware, caused
18 by spam.

19 He also says where he used to work, it was a
20 200-person organization, \$50 million a year, and some
21 worm got in, via email, and attached itself to their
22 anti-virus program, incapacitated the entire company for
23 three days to an estimated cost of \$160,000.

24 So, I'm just trying to give you a sense of the
25 magnitude of what's going on here. If we look at it

1 financially, there's two main areas where I see the
2 financial damage that malware is causing. The first is
3 once the spam gets through, the malicious spam gets
4 through, and does something, it wreaks havoc in one way
5 or another. There's a cost to recover from that.

6 The second are all the measures that we have to
7 take on an ongoing regular basis to prevent this from
8 happening. So, let me talk about the first first.
9 Because that's good engineering. One, two, three.

10 The damages. What kind of damages can we have?
11 We can have lost data. Right? Very common. This is
12 like what happened to the church. So, the malicious
13 ware can come in, it can wipe out your documents, it can
14 compromise your accounting data, it can wipe out your
15 customer lists, it can do all sorts of damage to data,
16 specifically.

17 So, the cost can be measured in several ways.
18 The first is, what does it cost to restore or recreate
19 that data? Right, now this may be an hour of a
20 consultant's team, and you should know most small
21 businesses do rely on outside consultants, so it is more
22 expensive than having your own internal person.

23 It could be an hour of a consultant's time to
24 restore from back-up, or it could be hiring an army of
25 temps to retype in data. So you really don't know. It

1 depends on the specific situation, but that's one cost.

2 Another cost is you have a bunch of employees
3 and they're sitting there twiddling their thumbs while
4 the data is being restored, right? They may not be able
5 to use their system, they may work on secondary tasks or
6 low priority tasks or in some cases they get sent home.
7 So, what is the cost of that lost productivity?

8 Then there's the issue of lost opportunities.
9 If a client calls in and wants to open up an account, or
10 wants to do a transaction and you can't because you
11 don't have their data right in front of you, that's a
12 lost opportunity. This could be immeasurable, but it's
13 very large.

14 Finally, you have what I'll call the soft costs,
15 the reputation. What is the harm of your reputation if
16 your clients calls you and you can't pull up that last
17 invoice that they're talking about, because you don't
18 have it. All right, what is the cost to your
19 reputation? And then what is the cost to your internal
20 morale? I don't know if any of you have ever
21 experienced this, when you get a new computer, your
22 morale goes up, it's fun. Hey, my company cares about
23 me, my agency cares about me, I got a new computer, I'm
24 really happy. The opposite is true when you can't use
25 it. It's frustrating, you feel powerless, and morale

1 goes down.

2 So what is the cost of that to a business?
3 Especially a small business whose employees are really
4 what make it run. So, that's one aspect of the damage,
5 lost data.

6 Second might be, or is, how should I put it, a
7 crashed system or the inability to actually use your
8 systems. Now, in some cases, with the directory harvest
9 attacks, or also there was a situation where a bot got
10 inside of a network and was broadcasting spam out,
11 effectively denying that company its use of its Internet
12 access, so email servers go down, you can't use email,
13 you can't use your machines, your server has crashed,
14 this is basically inability to use your system.

15 So, you have costs again. Your costs to
16 recover. Your costs to restore your system to an
17 operating state, right? Are you reformatting your
18 server? Are you buying a new one? In some cases, you
19 look at it and you say, oh, my God, this server is three
20 years old, and it is going to be more cost effective to
21 buy a new one, install it, set it up and run it than it
22 is to try to recover from this disaster that just got
23 hit by malware.

24 Whatever it takes to restore it to an operating
25 state. These clients that I recommended they go on a

1 spam filtering service, like Postini or MailWise, in
2 order to prevent from that, they had to do it, and that
3 wasn't a one-time cost, that's an ongoing monthly cost
4 that they need to spend to make sure it doesn't happen
5 again.

6 You have opportunity costs. Yesterday, I had a
7 conversation with the president of one of my clients,
8 they're a real estate firm, and they're involved,
9 they're local, they own quite a bit of land, they're
10 very small, about ten people. They are involved in a
11 huge, huge deal in California. It's all secret, it's
12 all hush-hush. This guy said his email is now so
13 critical because this deal is going to close in two
14 weeks and he's watching this minute by minute to make
15 sure and to let him guide it in case it starts going
16 south, he can pick it back up. You know? If he loses
17 that, the ability to use his email, if his server goes
18 down, due to malware, if it chokes up his Internet
19 connection and he can't get his email, he could be
20 looking at multiple millions of dollars down the tubes.
21 Huge. That's lost opportunity.

22 Again, there's the soft side of reputation. I
23 hate to see mea culpa, but a little while ago, we were
24 putting out a new website, and it got infected with a
25 bot, where every time you go to the site, it tries to

1 download on your Internet Explorer something to ravage
2 your mornings or I don't know, luckily I didn't want to
3 know what it was going to do.

4 Now, what kind of reputation is that for an IT
5 company to have a website where people go to it, and
6 there's a bot there? You know, it's horrible. I mean,
7 luckily we were able to recover inside of 30 minutes or
8 an hour, but that can go on a wider scale, and it's
9 something that you can't quantify. Again, it goes to
10 morale. What do you think my staff, my employees
11 thought when our website had that, but even more so,
12 when people can't use their systems. Because they need
13 to work.

14 Finally, the last area of recovery is in terms
15 of compromised data. All right, whether it's through
16 phishing, whether it's through key loggers, whatever it
17 is, it has a few areas where cost come up on that, the
18 first is the loss of competitive advantage, loss of some
19 sort of information that's critical to your business
20 that you don't want your competition to get. That's a
21 major area of cost. Dollars stolen. Issues, again,
22 like reputation.

23 We had a client who this actually wasn't
24 malware, somebody broke into their office and stole
25 their server and walked out with it, but the effect is

1 the same, they lost 5,000 credit card numbers that they
2 had to take and fax each and every one of their
3 customers and say, we lost your credit card number, you
4 might want to change that credit card. What does that
5 do to your reputation?

6 So, because these potential damages are huge,
7 they're monstrous, companies, small businesses, large,
8 everyone is doing whatever they can, and are spending
9 significant money to mitigate these risks, and that's
10 where we get into the preventive measures, okay? You've
11 got firewalls, you've got like physical hardware that
12 you can put on your system, Andy from SonicWALL, can I
13 say, can I say? SonicWALL. There's your plug.

14 MR. KLEIN: I'll give you a dollar.

15 MR. LANDA: Thank you. Firewalls, VPNs,
16 encryption, SSL subscriptions, all of those networks in
17 place to increase security, prevent this type of
18 malicious ware. Anti-virus programs, on each and every
19 computer, on servers, on your email, on laptops.
20 Anti-spyware program, same thing across the board. Spam
21 filters, on the network, off the network, many, many
22 different solutions, many, many different companies
23 putting them out.

24 Patch management, all of the operating systems
25 and the software, Microsoft Office, Internet Explorer,

1 so on and so forth, are vulnerable, and become more
2 vulnerable, and need to be patched. So, how do you make
3 sure, now that you're patched. You know on your
4 computer you can go and click on the little button and
5 do Microsoft Update. How do I as a business owner make
6 sure that every computer in my company, whether it's on
7 the network or off the network, is going to be patched?
8 That takes software, it takes hardware.

9 User education, which ranges from the Draconian,
10 if you're not expecting an email from someone, delete
11 it. All the way to classes on how to detect phishing
12 and so on and so forth. There are significant costs in
13 user education. The cost of professional IT management.
14 Consultants, managed service plans, whatever it is that
15 these small businesses often don't have in-house and do
16 need to contract outside. So, the cost of prevention is
17 rather high. The cost of the professional management,
18 the outside consulting and support and the user
19 education is often as high or higher than the actual
20 outlay for hardware and software. To execute the
21 security measures.

22 So, let me leave you with a few thoughts. Small
23 businesses represent 50 percent of our nation's GDP.
24 Over six and a half trillion dollars a year. While they
25 are the most powerful group in aggregate, the most

1 powerful economic force, when you break them down, each
2 one of them is actually the poorest, because they're
3 small. They don't have the resources, the financial
4 resources that these large companies have to prevent
5 against this, and it's not as economical for them to do
6 so. They don't have the internal IT management
7 infrastructure to do this, so they have to turn to
8 outside consultants and outside services like my company
9 and thousands of other companies are providing across
10 the nation. So, they have to spend a disproportionately
11 large, a disproportionate amount of money for the
12 preventative and recovery efforts.

13 With the advent of managed network services,
14 that I kind of briefly touched on where it's a fixed
15 price per month, per computer, that helps, that helps
16 contain the cost, but this is some very new stuff and
17 very, very few small businesses are on these kinds of
18 services yet, and it's still a lot more expensive,
19 proportionately.

20 So, I guess my plea here is that anything that
21 can be done to help mitigate the cost and the complexity
22 of fighting malware, especially if it's geared toward
23 the small and mid-sized businesses. Not only will we
24 have a significant negative impact on the malware
25 economy, but I think it will have a very significant

1 positive impact on our nation's economy. Thanks. Thank
2 you very much.

3 (Applause.)

4 MS. DREXLER: Thanks so much, Heinan, and all of
5 the other panelists. I am going to ask one quick
6 question before we move into a short period for audience
7 questions and answers. I'm hearing that some of the
8 incentives for these cybercriminals are the low cost and
9 you can attack thousands of people at once and that the
10 cybercriminals don't need to re-invent the wheel because
11 they're trading this information back and forth in all
12 these forums and then launch these anonymous remote
13 attacks and what this results in is there's damaged
14 business reputations and lost data and many other costs
15 and we could go on and on.

16 So, what I would like to know is who exactly are
17 these cybercriminals? We've heard everything that
18 they're kids in their basements to these organized
19 groups online, whether it's organized crime that's
20 moving online, or whether it organized crime that's
21 being set up as a result of that. I'm wondering who
22 they are and whether these public forums contribute to
23 that and where are they all going? Would someone take a
24 moment, whoever wants to start?

25 MR. KLEIN: Sure, I'll start. I think it is a

1 combination. The interesting part about it is there
2 doesn't need to be, like I said earlier, a building
3 where they all go. As a matter of fact, that probably
4 makes no sense at all, but the Internet infrastructure,
5 the communication infrastructures that are out there
6 that allow people to congregate and talk in chat rooms
7 and such are where they come in, and what their age is,
8 age is only because they're youthful because they've
9 been brought up in that environment and they're not
10 afraid of it. Many of us were around before computers
11 really took off, and so not that we're afraid of it, but
12 we just weren't brought up in that environment.

13 So, I think you see youth, but you see youth
14 because they're the ones getting caught. I think
15 there's a fair number of professional organizations in
16 some of the foreign countries, over in Europe and such
17 that utilize these resources, these youngsters to do the
18 types of things that are necessary, pick up those pieces
19 and develop the pieces and then organize them and take a
20 small cut out of that whole process, but I don't think,
21 like I said, there's no malware building where you can
22 just go and arrest a bunch of people, because there
23 doesn't need to be, it's just a cyber community and
24 nothing more.

25 MS. DREXLER: Anyone else?

1 MR. HINRICHSEN: I'll take a slice of not so
2 much the who or the what, but the how. You know, you
3 think about many of the exchanges or the communication
4 or dealings between fraudsters and the underground and
5 you can bring him on separate forums, they had even
6 created their own communication channel called Carter IM
7 as an example, some time ago, but a recent instance in
8 an actual automated online store for credit cards.

9 So, when you think about being able to expedite
10 a particular fraudster, whomever, wherever they are,
11 whether they're part of an organized ring, whether
12 they're an independent individual of any age, it just
13 shows you how easy it is now for the passage of goods
14 and the commerce of goods to occur.

15 So, instead of having to go off into an ICQ
16 channel, barter with that individual, get to a certain
17 price, it's a store. Just like any other e-commerce
18 store that's available in the U.S. and Russian language.
19 You know, you pay with WebMoney. So, the process itself
20 continues to evolve, very much like our very public
21 e-commerce as well.

22 MS. DREXLER: Great, anyone else?

23 MR. CRABB: Great, and I'll add on to that,
24 having had an opportunity to chase a number of these
25 criminals around the world. I refer to it as networked

1 criminality, in that the organized crime cells or the
2 individuals can hook into the network, get what they
3 need out and do with the information that they've stolen
4 or the services that they've provided into the network
5 as they may.

6 I don't really care what you've done with the
7 information, I just want my money out of the operation
8 perspective. It's organized crime in Eastern Europe,
9 we've seen Ukrainians, Lithuanians, Russians, organized
10 crime all connecting into the network.

11 I've had the opportunity to go to Nigeria on a
12 number of occasions that relates to this type of
13 activity, where in an economy that is so desperate that
14 it doesn't cost a lot for large groups of people to be
15 able to connect into the infrastructure, get out of it
16 what they need, and go on, so all they need is a cyber
17 cafe. They're hooked into the network, and they can
18 amass the lists that are necessary to spam and be off
19 and running in a very good phishing operation in a very
20 short order.

21 You know, you also see the Eastern Europeans, or
22 not the Eastern Europeans, the Middle-Eastern nationals
23 engaging in this as well. I've had the opportunity to
24 do law enforcement actions in Egypt and Jordan and
25 Lebanon. We see more and more of these criminals, just

1 wherever they may be in the world. The modus operandi
2 is all connected into the malware economy, and we are
3 going to see more and more of it.

4 MS. DREXLER: Great, thanks. I assume, Heinan,
5 you don't have anything to add. We will take some
6 questions from the audience now. If there are any. One
7 of the questions is, are there any estimates of how much
8 revenue per year the spammers make and what the total
9 costs are to the U.S. economy?

10 (No response.)

11 MR. LANDA: I don't have any of those.

12 MS. DREXLER: I think during one of our breaks,
13 we may have had actually a question regarding this, just
14 generally about cybercrime, I don't necessarily know
15 that it's more geared towards spammers, but I don't know
16 that we have the breakdown right now, but maybe we could
17 try and find out that.

18 MR. LANDA: It's very tough to break down the
19 costs, because you have, for example, the stuff that I
20 talked about. When you look at each one of those
21 individually, it's so situation-specific, and some of
22 those costs, especially when you are looking at
23 opportunity costs, lost reputation, loss of morale,
24 which can lead to turnover costs, and they're very, very
25 hard to pin down. I can tell you that internal service

1 delivery costs, people estimate, are between, for IT
2 service, are between three and 15 percent of the revenue
3 of the company, but I would hate to take that and try to
4 draw a dotted line to six and a half trillion dollars.

5 MS. DREXLER: Okay. We have a question
6 specifically for Jens at RSA regarding the Barclay
7 browser helper example. Would this attack be
8 ineffective if scripting was disabled in the browser or
9 if it was limited through tools like the Firefox no
10 script extension?

11 MR. HINRICHSEN: One more time.

12 MS. DREXLER: It says for the Barclays browser
13 object helper example that you gave, they would like to
14 know would this attack be ineffective if scripting were
15 disabled in the browser or it was limited through tools
16 like the Firefox no script extension?

17 MR. HINRICHSEN: I can't speak to the specific
18 variants, but certainly there are ways that it becomes
19 ineffective or is otherwise disabled. You know, if I
20 were in our CTO's office, I would wax more prophetic on
21 that.

22 MS. DREXLER: Thank you. Are there any other
23 questions from the audience?

24 (No response.)

25 MS. DREXLER: Okay. Another question I had is

1 if we could look at a little bit more into the role of
2 fear and trust, and how social engineering plays a part
3 in allowing this to happen and as one of the incentives
4 for these cybercriminals. Exactly what would you say
5 are the biggest factors in allowing these attacks to
6 happen, that motivates these cybercriminals? Anyone can
7 respond.

8 MR. KLEIN: Well, I would say about three years
9 or so that we've been running something called the
10 phishing IQ test, which is a fairly straightforward
11 mechanism for people to go in and see if they can
12 identify phishing or legitimate emails. It's consumer
13 focused, it works pretty good. But over the length of
14 that time, we've seen the way people perceive these
15 messages change.

16 Initially, when people were taking tests, there
17 wasn't much out there in the way of phishing, for
18 example, but they were actually, weren't very good at
19 detecting phishing emails. Which made perfectly good
20 sense. It was kind of unknown to them, they didn't
21 know, and they were very good at picking out legitimate
22 ones. Over the three years or so, that's flip-flopped
23 completely, so that now they're fairly good, about 90
24 percent, at picking out phishing emails, but legitimate
25 ones, about 50/50. It all goes to the notion of trading

1 trust versus protection. That's kind of the general
2 conclusion we've come to when you talk to folks about
3 it, and you see it in the data that's out there.

4 So, I think that's the trade that people make.
5 We've heard earlier that people are going to continue to
6 use email, and I think I certainly agree with that. But
7 it's what they have to do on a day in and day out basis
8 in order to utilize that is make that trade of
9 protection versus trust.

10 MS. DREXLER: Anyone else?

11 (No response.)

12 MS. DREXLER: Any other questions? We have a
13 question over here, if you can just wait for the
14 microphone, please.

15 MR. FOX: Hi, Jeff Fox, Consumer Reports. Just
16 wondering how easy it is for someone to find their way
17 into this economy. There's so many people doing this
18 and you've got all these kids and young people. I know
19 they're tech savvy, but I mean, do you just find it by
20 Googling the right term, do you have to wander around
21 all the IRC chat rooms? You know, I'm not asking for
22 specific details.

23 MS. DREXLER: Are you looking for a new job?

24 (Laughter.)

25 MR. FOX: Is it that easy to find, because so

1 many people obviously have found it. Do you have to be
2 friends like with a bunch of criminals?

3 MR. LANDA: I think it's fairly simple. I could
4 give you an example, I might not want to share, but my
5 daughter hacked into my iTunes account, so you think,
6 oh, my God, how could this happen, this is an IT man,
7 doesn't he secure his systems. So she went and she
8 hacked into my iTunes account in order to give herself
9 money in her iTunes account so she could buy a few more
10 songs. So, it was more or less innocent, but we --

11 MR. CRABB: We call that friendly fraud.

12 MR. LANDA: Friendly fraud. How did she do it?
13 She went into my iTunes account, said she forgot the
14 password, clicked on the forgot password button and just
15 started answering the questions. What's your mother's
16 maiden name. She knows. She didn't know my birthday,
17 so one day at the office I got a call, daddy, what's
18 your birthday, and I'm thinking, cool, she's buying me
19 gifts. But it's not that hard. She's --

20 MS. FOX: Social engineering.

21 MR. LANDA: She's 11, she's very, very deep into
22 all of that cyber world, and she's a good kid. I don't
23 think it would be that difficult for someone to really
24 get involved in the negative aspect of it.

25 MR. CRABB: And just to comment, the forums are

1 very easy to find on the Internet. The forums are easy
2 to find, criminal organizations are talking about
3 cybercrime. You know, the statistics show that
4 cybercrime is as lucrative as the drug economy is today.
5 So, why not go to cybercrime? The criminals will talk.
6 They direct themselves into those areas.

7 MS. DREXLER: The second part of Jeff's
8 question, how easy is it? I mean, do you have to be in
9 the organization? They're obviously very easy to find
10 and go to them, but are you able to actually purchase
11 these without knowing somebody?

12 MR. CRABB: It's very easy. It's the
13 development of untrusted relationships and the
14 underground economy. The anonymity of the types of
15 transactions, the financial transactions that they make
16 between each other, the criminals do not know each
17 other. They're sitting in remote locations. I say that
18 the criminals do not know each other, the disparate
19 criminals do not know each other. Criminals that are
20 operating as organized crime cells that hook into this
21 network obviously know each other, but it all depends on
22 where you get stuck into the economy of the criminality.

23 MS. DREXLER: Do you have another question?

24 MR. LEIBA: Hi, I'm Barry Leiba. In relation to
25 the last two questions, by putting these

1 I-forgot-my-password questions, we're inviting problems
2 with this sort of thing. First of all, those sorts of
3 questions, what's your favorite pet's names, what's your
4 mother's maiden name, are ideal social engineering sorts
5 of questions, and apart from that, we're basically
6 asking people to pick insecure passwords to get their
7 real passwords from. You know, I could guess that your
8 mother's maiden name is more likely to be Johnson than
9 some other stranger thing, and many times I might be
10 right.

11 On the general thing, we're doing a lot of
12 things, the legitimate sites are doing a lot of things
13 wrong that are making people, I guess it was to Andy's
14 comment that people are less sure about real sites now,
15 because the real sites are making mistakes, that make
16 them look less legitimate. They're hiding the SSL
17 behind a Javascript button or something so that you
18 don't see the little lock symbol because your
19 conversation with the server isn't secure until you push
20 the button, and then whatever you entered is transmitted
21 through using SSL, but it's hidden from the browser
22 interface.

23 We're doing a lot of things like that,
24 self-signed certificates, expired certificates that are
25 causing pop-ups to users, and they're starting to get

1 used to seeing these things, and sometimes it means they
2 trust untrustworthy sites because they're answering yes
3 to these untrusting pop-ups. The second thing is the
4 sites look bad because of these pop-ups. I think we
5 have to fix that. Legitimate sites have to be very
6 careful to do the right things.

7 MS. DREXLER: Thank you.

8 MR. LEIBA: A bit long-winded, sorry.

9 MR. CALSON: Hughy Calson. There's one other
10 cost that I don't think I've heard anyone mention yet.
11 It occurs to me that the one reliability method that has
12 been found to make spammers stop sending spam is to take
13 away their computer and give them a room that has no
14 door knob on their side.

15 Now, we've heard the FBI say they've had some
16 success, we've heard the FTC say they've got a dozen
17 cases, we've heard Jon Praed say that civil attorneys
18 can handle a lot of the investigative work and push a
19 lot of these cases much better than government can.

20 My question is, there's hundreds of them,
21 there's dozens of you. Who's going to pay for ten more
22 Jon Praed's, for ten more FTC staff attorneys and legal
23 clerks? We're going to need some more FBI guys.

24 MS. DREXLER: I think that's a great question.
25 We're actually tomorrow going to be having a panel on

1 law enforcement issues, so hopefully we can address that
2 a little bit more in that. It looks like we have
3 another question, and I think we have time for about one
4 more question. So, go ahead, thank you.

5 MR. CROCKER: Dave Crocker. I was listening to
6 Barry Leiba's comments about the various things that
7 make it easy for users to make the wrong decision and I
8 was trying to listen to that as if I didn't have any
9 background in it, and I went kind of crazy, because
10 there is no way it's reasonable to expect any normal
11 person to be able to make the kind of distinctions we're
12 forcing on them.

13 It isn't enough to say that a given site needs
14 to follow some good practices, because what he was
15 describing was an Internet-wide systems design problem.
16 We have established patterns that no single site can
17 fix, and it struck me, this is a category of problem
18 that's exactly perfect for an organization like the FTC
19 to look at. There are guidelines, guidance, conformance
20 rules, I don't know what that needs to make the life of
21 the user vastly simpler for making assessments about
22 trustworthiness of where they are and when they're
23 clicking.

24 MS. DREXLER: Thank you. I think tomorrow we
25 also, in our consumers panel, we will definitely be

1 addressing some of those issues as well. I want to
2 thank all of our panelists for being here today, thank
3 you all for listening, and we're now going to take a
4 short break for about 15 minutes, and we'll convene
5 again at 3:30. Thank you all very much.

6 (Applause.)

7 (Whereupon, there was a recess in the
8 proceedings.)

9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

1 EMERGING THREATS

2 MS. CHRISS: Okay, everyone, we're going to go
3 ahead and get started here. So, feel free to take your
4 seats, and welcome back. Please, congratulate
5 yourselves, this is the final panel of the day, and you
6 all have been a wonderful audience. So, thank you.

7 Has everyone settled in? All right, terrific.
8 My name is Sana Chriss, and I am the spam coordinator
9 here at the FTC. Admittedly when I first mentioned that
10 to someone, they said, well, that doesn't sound very
11 good. So, I had to clarify, I'm against it, I don't
12 actually coordinate it, I am against it, and I work with
13 many of my brilliant colleagues to develop strategies
14 for fighting this ongoing spam problem.

15 So, this panel is called Emerging Threats, and
16 what does that mean and why is it important? We're
17 going to examine all of the things that you've heard
18 about today in terms of how they are affecting other
19 platforms, whether it's mobile devices, social
20 networking websites, or Voice Over Internet Telephony.
21 We're going to examine what are some of the future
22 threats that are happening and how can we best protect
23 consumers, because at the end of the day, that is what
24 it's about, whether it's consumers or customers for you,
25 we're all trying to achieve the same goal.

1 This panel is important because it gives us an
2 opportunity to really be proactive, and I think I'm
3 going to speak for the agency in saying that's something
4 that we really do best. Our first spam-related case was
5 in 1997, okay, and CAN-SPAM, the CAN-SPAM Act became
6 effective in 2004. So, that's pretty proactive, if you
7 ask me, using our authority under Section 5 to combat
8 fraudulent and deceptive acts, regardless of the
9 platform.

10 So, the industry members before you, they are
11 similarly situated in that they are on guard in terms of
12 being vigilant in protecting their customers from these
13 emerging threats and they, too, are very proactive. So,
14 let me introduce some of these wonderful panelists
15 today.

16 Next to me is Mike Altschul, he is the senior
17 vice president and general counsel of CTIA, The Wireless
18 Association; Dave Champine, he's the senior director of
19 product marketing at Cloudmark, which is a provider of
20 carrier-grade message security; next to Dave is Scott
21 Chasin. Scott is the chief technology officer for
22 MXLogic, and MXLogic is a provider of managed email and
23 web security services. Scott is also the chairperson on
24 the MAAWG subcommittee fighting spam bots. So, he will
25 have something interesting to add there as well.

1 Next to Scott we have Rick Lane. Hi, Rick.
2 Rick is here, he's with News Corp., he's the vice
3 president of government affairs, and as you all know,
4 News Corp owns MySpace, the social networking website.

5 Next to Rick we have Christopher Rouland.
6 Chris, he's a chief technology officer and IBM
7 Distinguished Engineer working with IBM Internet
8 security systems, which advises thousands of the world's
9 business organizations and governments.

10 So, I think that you will all agree that we have
11 some experts here on this panel, and so without further
12 ado, Mike, would you like to get us started?

13 MR. ALTSCHUL: Are the slides controlled? Oh,
14 you can control the slides. I don't have to stand
15 upright. I will. Thank you.

16 Well, and thanks, again, to the Federal Trade
17 Commission for inviting us to participate on this panel,
18 and convening these two days.

19 I was fortunate enough to participate in the
20 first of the spam forums, a little more than, what is it
21 now, four years ago, May 2003. At that time, we
22 recognized that wireless spam and malware was going to
23 be an important thing to our industry, CTIA represents
24 wireless carriers and their suppliers and indirectly the
25 240 million Americans who are wireless customers.

1 We were a bit behind the rest of the world in
2 rolling out text messaging and some of the data
3 applications, and had observed overseas the explosion of
4 spam, which really colored and spoiled the user
5 experience. So, sometimes being second isn't such a bad
6 idea.

7 We have the opportunity to learn from overseas,
8 and we're able to deploy our first generation of these
9 data services in a way that has been, I think, while not
10 perfect, remarkably successful in protecting and
11 filtering spam and malware from wireless users and
12 devices.

13 I'm going to be talking about where the industry
14 is going, though, and as we move forward into basically
15 converged Internet devices, where phones are
16 increasingly web browsers, we will leave the protection
17 of the walled garden and some of the filters and
18 protections we've provided.

19 So, that's a little bit of background as to how
20 we got started and what I'm going to be talking about.
21 We now have, by our measurements, as I said, 240 million
22 subscribers, and more than half of them have devices
23 which can be used as Internet browsers of one kind or
24 another, 56 percent of wireless devices in the U.S. can
25 access the public Internet.

1 The first slide that we see before you just
2 makes the point that anywhere you can go from your
3 desktop, using a cable modem, DSL line, a satellite
4 broadband over a power line, WiMAX, WiFi, whatever,
5 increasingly you can use commercial wireless device to
6 get to.

7 A little bit surprising, if you haven't used it
8 yourself, but in the last year, 18 months, our industry
9 has aggressively rolled out what are called 3G, third
10 generation services that now offer true broadband
11 speeds. Now there's a debate in broadband policy
12 circles as to what is broadband speeds.

13 So, we haven't used that term so much as
14 identifying equivalents to DSL, which is the typical
15 telephone company offering, or cable modem services, but
16 each of the national carriers, regardless of their
17 technology, is now offering DSL-like speeds to their
18 customers, particularly in the major markets and
19 increasingly in the smaller markets across America.

20 Sprint has announced for later this year the
21 deployment of the first fourth generation broadband
22 wireless service, WiMAX is the name of the technology
23 that's offering a theoretical maximum download speed of
24 20 megabits per second, which puts it in sort of cable
25 modem territory.

1 We're going to have the opportunity in the
2 Washington market and in Chicago to be the early
3 adapters and to actually see how early adopters, not
4 adapters, early adopters, to see how close they come to
5 these speeds, because Washington and Chicago are going
6 to be the first test markets, trial markets, to be
7 turned on.

8 As this third slide shows, consumers
9 increasingly are using wireless phones and devices to
10 access information and the form factor is changing
11 accordingly, so that we are all familiar with the iPhone
12 and I almost brought our office one today, but somebody
13 else had checked it out. The screens and functions are
14 less and less like a traditional telephone, and more and
15 more like the screen on a laptop or PDA.

16 So, there's a couple of wonderful websites that
17 you can go to and see all the different products that
18 are available in the market in the U.S. We've counted
19 more than 200 of these 3G broadband devices. They
20 include something called air cards, it's basically a
21 card that slides onto any port in a laptop and is
22 basically a wireless broadband connection that will
23 allow a laptop to do anything a wired connection to the
24 Internet will provide.

25 This is just a partial list of the number of

1 hand sets with web browsers. You may recognize some of
2 the names, and similarly, another way of accessing the
3 Internet using wireless devices is with WiFi, there's
4 WiFi in this room, if you have a WiFi enabled smart
5 phone, you can get to the Internet, either using the
6 carrier's commercial spectrum or using WiFi from any
7 WiFi hot spot.

8 The industry has the benefit of the CAN-SPAM Act
9 that I think you're all familiar with. In particular,
10 the FCC implemented CAN-SPAM with particular rules for
11 commercial mobile services so as to prohibit the sending
12 of any unsolicited commercial messages to wireless
13 devices, and the FCC has created a website and registry
14 much like the Do Not Call Registry where wireless
15 carriers are obligated to list or provide lists of the
16 domain names that they have in use for wireless device,
17 and spammers, at least law-abiding spammers, are
18 obligated to go to that website, download the list and
19 not send messages. Carriers have been aggressive in
20 going after and suing those spammers who they can find
21 in the U.S. and who have not been diligent about this,
22 as heard on the earlier panel, and you all know most of
23 the spam seems to come from outside the U.S.

24 But we do have legal protections which are
25 unique to wireless device. You probably all know that

1 there are at least two types of wireless messages. One,
2 I'm going to hold up my own personal BlackBerry as an
3 example here, one is something called SMS, or short
4 message service, and MMS messages. These are primarily
5 peer-to-peer text messages sent from one mobile device
6 to another. Then the other are email addresses which
7 are sent just as an email message is sent from any
8 computer to any other email address.

9 The distinguishing feature for an SMS message is
10 it uses a telephone number, a North American ten-digit
11 telephone number as the address, and is limited to 160
12 characters as a message cell. An email uses the
13 traditional Internet domain address with the @ sign and
14 a high-level domain name. This one BlackBerry has five
15 different addresses. I can get the identical message
16 sent to this device and then I can send the identical
17 message from this device five different ways. First I
18 can receive and send SMS messages just to my phone
19 number. For those lawyers in the room, SMS messages
20 probably are not covered by CAN-SPAM, but they're
21 covered by the Communications Act, because they use a
22 phone number as an address.

23 I also can use a PIN, BlackBerry has its own
24 server, and all of the BlackBerry devices have a serial
25 number, basically a PIN, and if you know, and we know

1 within our office the PINs of all the users, you can use
2 that PIN as an address, the message will never go to the
3 public switched network or the public Internet, it will
4 just go to the BlackBerry service and then back down to
5 another BlackBerry device.

6 As it turns out, during September 11th, PIN to
7 PIN BlackBerry messages were probably the most reliable,
8 least delayed ways of communicating because it really
9 didn't touch the public Internet. Also, at that time,
10 there were a lot fewer BlackBerry users than there are
11 today.

12 I also can get, receive a message sent over the
13 Internet using the AT&T Gateway to this device, if you
14 use my wireless number @ATT.net. That is something
15 subject to CAN-SPAM, it's a traditional email message
16 that is sent over the public Internet. It goes through
17 a Gateway that AT&T provides for its users.

18 There is spam filtering and malware filtering at
19 that Gateway and it's delivered to this device. Because
20 it's a BlackBerry, it also mirrors my desktop at work,
21 so my office email address, all those messages show up
22 on my BlackBerry device, and I can respond and send
23 messages using my office email address. I have
24 downloaded a Google application which also synchronizes
25 by personal Gmail account to this device. So, just as I

1 can get all the email sent to me at my work address, all
2 of the personal email sent to my Gmail account also
3 comes. If you count those, there are five different
4 addresses with at least two sets of legal rules, and
5 five different ways of introducing spam and malware into
6 this device.

7 So, those are some of the challenges that we're
8 all facing. While it's possible to send spam messages
9 through the carrier's gateways, one or two messages at a
10 time, carrier's gateways have been effective in
11 identifying and filtering out real spam attacks. So,
12 one or two may slip by. First, that may be cumbersome
13 to send multiple messages to a large list or certainly
14 to all the users using phone numbers, and they're very
15 effective in identifying spam-like messages.

16 When you start moving into email, and email that
17 comes to devices like this from outside of carrier
18 gateways, my protection from spam on my office email is
19 only as good as our office IT department's protection.
20 My protection from spam on my Gmail account is only as
21 good as what Google and Gmail provide, or what I may
22 provide for myself.

23 I'm not going to get into the debate about net
24 neutrality and the proliferation of devices. I know
25 someone from Consumer Union is here, Consumer Reports,

1 every February reports on wireless devices, and I hate
2 the fact that there are so many different operating
3 systems, so many different technologies, we have GSM,
4 CDMA, Symbian OS, Microsoft OS and so on.

5 In an ironic way, that has been very good
6 protection from users of malware, because there are so
7 many different standards and technologies being used,
8 and no one truly dominant operating system or
9 technology, the diversity and robustness that we have as
10 an industry, I think, has been a benefit. Just as sort
11 of the Apple Microsoft operating systems have been more
12 of a benefit to the Apple model.

13 Similarly, as we move from closed systems and
14 walled garden kind of applications, to more open access
15 to the Internet, more open access to side loading and
16 downloading content and applications on these devices,
17 carriers' ability to protect and vouch for the security
18 of the network and the applications is going to
19 diminish.

20 This is just natural, the same thing happened
21 when the users demanded more openness than the original
22 Prodigy model, or even the original AOL walled garden
23 model provided.

24 So, we started in an environment where carriers
25 operated under pretty much of a closed walled garden

1 environment. As users have gotten more and more
2 experience with the Internet and with wireless devices,
3 they're demanding more openness, more applications, and
4 with that, users are going to have to start taking more
5 responsibility just as we do with our own desktop
6 situations, for protecting themselves against malware
7 and spam, and we will not be able to rely as heavily on
8 carriers and networks to do it for them, because
9 carriers and networks are going to have much less
10 control over the user experience. It's not good or bad
11 or trade-off, it's just what's going to happen as the
12 industry responds to the public's desire for more open
13 access.

14 So, I think that's pretty much it. I just, I
15 also want to close with this final slide, which at least
16 to me I find amazing. This is a graph taken from the
17 FCC's most recent report on high-speed Internet access
18 services. They're so-called broadband report. They
19 measured the last six months or the time frame from
20 basically January 1 to June a year ago 2006, and in that
21 time, which is just coinciding with the rollout of 3G
22 networks by the national wireless carriers, 60 percent,
23 59 percent of all new broadband services or customers
24 were wireless. Not our own growth, from a low base, but
25 we added more subscribers, subscriber lines, whatever

1 you want to call it, than DSL and cable combined. We're
2 quite confident when this year's report comes out, we're
3 going to see continued extraordinary growth and
4 acceptance of these wireless services.

5 So, with that, thank you very much.

6 MS. CHRISS: Thank you, Mike, that was a
7 terrific overview.

8 (Applause.)

9 MS. CHRISS: 240 million American wireless
10 customers and 56 percent of them are accessing the
11 Internet on those wireless devices, so this is certainly
12 an important problem that touches a lot of people.

13 Next we have Dave. Dave, please come on up and
14 tell us about how we can secure all of these customers.

15 MR. CHAMPINE: Sure, thanks. Let's see, there
16 we are. That's me.

17 Good afternoon. Thanks, everybody, for sticking
18 it out through the last session here. It seems like
19 we've had some great discussions and a lot of
20 consistency, that's great to hear as well because that
21 means we can start to standardize on practices as well
22 as policies around these issues.

23 Michael did a great job of kind of painting the
24 backdrop of the wireless industry, particularly, and
25 some of the advances there. That's one of the areas

1 that I will touch on in terms of my take on emerging
2 threats.

3 Just two seconds, if you're not familiar with
4 Cloudmark, we do work largely with many of the service
5 providers in both the fixed and wireless space. We're a
6 global business, so we do see a lot of spam, and so some
7 of the insights will be from a consumer perspective, but
8 some of the insights will also be from a carrier
9 perspective, since those are our largest customers in
10 our base.

11 So, a lot of the economics has been covered, and
12 that's actually great, because we need to start thinking
13 about this more as a business problem and less as a
14 technology problem, if we're really going to make
15 progress. A lot of people have already brought up the
16 points that I have made on this slide, so this will help
17 me kind of get through these quickly as well.

18 We've already identified that these are, in
19 fact, businesses, and we talked about the different
20 products, so I will be able to skip over my next slide
21 pretty much specifically, but the one area is kind of
22 market expansion, so I'll drill into that a little bit.

23 So, there's new technologies that they're able
24 to exploit, new tactics that they're able to exploit,
25 and we've heard about those and will continue to hear

1 about more. But one of the things that we need to
2 understand to predict the behavior is where will they go
3 next. If we are successful in regulating their behavior
4 and their current tactics, where will they go next?

5 That's the nice thing about wireless is that it
6 interferes with microphones.

7 (Laughter.)

8 MR. CHAMPINE: Yours will be even worse, I
9 think. He's got an iPhone, so he's going to have a lot
10 more interference. He's just showing off now.

11 In any case, if we see these like a free market,
12 and the beauty of the Internet is that it creates a
13 global free market, well they will move on, they will
14 find other places to ply their wares, so let's try to
15 predict those movements and not be caught by surprise
16 like we have been for the last ten years.

17 So, we've talked, you've heard about some of the
18 new products or tactics that these businesses are using,
19 image spam was a big deal last year, starting to
20 actually see somewhat of a tail-off in that in respects.
21 It's hard to tell whether that's a trend or that's
22 people just shifting around their tactics. Botnets are
23 big, and Scott I think will drill into that quite a bit
24 more and we've heard about that.

25 But the targeted scams, social engineering,

1 we've started to see a huge increase in those. Social
2 engineering, I've heard in a number of contexts, in the
3 session so far. What I'm referring to here is a
4 combination of things. It's really just playing on
5 human nature, as opposed to using specific technical
6 capabilities. One of the things that we've seen most
7 recently, particularly with new viruses and new
8 outbreaks of spam with the things like the Storm Worm
9 and different variants of that is the timing of their
10 release.

11 So, in one aspect, you can use social
12 engineering to use a compelling subject line, such as
13 take a look at the video attached from the latest
14 European storm. That's one context for social
15 engineering. Another is sending out that message on a
16 day when traditional anti-virus firms are going to be
17 slow to respond, because they have researchers who are
18 humans, who need to be able to take a look at that, they
19 need to be able to reverse engineer it, in order to put
20 out a patch.

21 Well, the attackers are getting more
22 sophisticated and are saying, well, why don't I release
23 that Saturday night just before Easter when those people
24 will be home with their families and they won't be able
25 to respond and I will have a window of opportunity to

1 infect more computers if I take advantage of that social
2 aspect of engineering.

3 So, there's a number of sophistications along
4 social engineering. We have heard about some of the
5 terrorist aspects and ransom aspects, so I won't go into
6 those, but I think it's interesting to point out that
7 there are other trends along those lines.

8 So, let's talk about the new markets. It's not
9 just for email anymore. Wherever you look, instant
10 messaging, people are spamming, constantly. People are
11 doing harvesting attacks against all of the major
12 instant messaging providers. Comments in blogs are
13 pretty much becoming saturated with spam, and it's
14 pretty annoying, and there's a whole debate over whether
15 capture is effective anymore in actually registering
16 blog users and things like that, but you are finding
17 spam becoming an issue in blogs and news feeds.

18 Social networks, I'm sure we'll hear much more
19 about with respect to MySpace, but Web 2.0 is a concern
20 there as well, it's another vector for people to
21 exploit, because you're out there double clicking on
22 stuff and that's a great way to get into your computer.

23 So, the big area, though, that we really ought
24 to pay attention to is mobile, and really if you take a
25 look at this from a macroeconomic perspective, this is

1 ready to burst. What we've been creating, and what CTIA
2 has been doing a great job of creating, is an
3 environment in North America, in the U.S. particularly
4 is what we're concerned with here in this audience, that
5 is ready to explode as it has in other markets. We're
6 not used to being late technology adopters in the U.S.,
7 we're used to being a mass exporter of technology, but
8 if you take a look at different markets around the
9 world, particularly in Asia and Europe, where they've
10 had these 3G networks in place for longer and there is
11 no such thing as a smart phone in Korea, for instance,
12 it's just a phone. It happens to be smart.

13 And in that region, as well, spam on those
14 devices is incredibly high. In fact, in Korea, spam on
15 phones is more common than spam on desktops. So it's a
16 kind of a topsy-turvy model for us to think about. So,
17 we do have an opportunity, and because we've got
18 industry support and people working together, we do have
19 an opportunity to get in front of it.

20 So, but let's think about it, let me drill into
21 it just a tiny bit more. This is a very large, very
22 grilling audience, and typically they're uneducated with
23 respect to what the threats are, and we are kind of in a
24 mode to borrow a phrase from another Washington person,
25 we are in a phase of rational exuberance, with the

1 applications and the data services that are being
2 deployed to mobile handsets.

3 Mobile advertising is expected to exceed \$10
4 billion in the next couple of years. We don't know
5 who's going to get all that money, exactly, but somebody
6 is planning on spending it, and they're expecting the
7 consumers to respond in a positive way.

8 There's also a lot of expectations on mobile
9 commerce and mobile banking and mobile peer to peer
10 payments and things like this. Well, there's a lot of
11 high expectations that require a lot of trust and a lot
12 of security that just isn't there. A lot of education
13 that absolutely isn't there. So, we need to be very
14 careful and very cautious.

15 Basically I'll break these down into two
16 categories. I won't go into a lot of technical detail,
17 just kind of spell out where these things are coming
18 from. Michael mentioned that at the wire line to
19 wireless convergence, fantastic technology in gateways
20 that's starting to bridge all these. You're starting to
21 see a lot more triple play and quad play, convergence
22 between your online carriers offering wireless services
23 as well.

24 This is great, but as he said, it opens up the
25 walls to the walled gardens that have been protecting us

1 to date. There's also convergence in the handsets,
2 convergence in the operating system which has been a
3 barrier and provide more abuse or a wider opportunity
4 for abuse.

5 So, then we have wireless-specific threats. So,
6 spam is an obvious one, but we are not a great user of
7 SMS here, and so we haven't experienced it all that
8 much, although people who are heavy users, according to
9 some surveys, 18, 20 percent have already experienced it
10 here in the U.S. Smishing, SMS phishing, you can
11 imagine.

12 The problem here, as we've talked about with
13 phishing, a lot of it is education and being able to
14 determine what's a legitimate link and what is not.
15 Well, on a screen this big, you don't really have the
16 same kind of tools or the same visibility into whether
17 that is a legitimate link. All you have is a button
18 that says okay. Well, if my choice is to click okay,
19 I'm going to do that pretty often.

20 There are a number of exploits already on
21 Symbian OS, which is the most popular operating systems
22 for mobile. There are new threats all the time. iPhone
23 creates a great opportunity as we're starting to see
24 convergence between desktop operating systems and
25 applications and mobile operating systems. There's a

1 number of threat vectors already out there.

2 So, what I would leave you with is what are the
3 considerations about this, and why is this one worth
4 particular consideration? As opposed to kind of just
5 doing a doom and gloom scenario on this, let's think
6 about these issues, let's address them before they
7 become a real problem.

8 Young people are the primary users of mobile
9 messaging. As I look around this audience, with all due
10 respect, I would not expect that you are heavy SMS
11 users. If you have children, though, I would expect
12 that they are. If you haven't already gotten an
13 unlimited SMS plan and you have a teenager, I highly
14 encourage you to, because you're spending lots of money.
15 I'm sure CTIA members appreciate that, but it's
16 interesting. They have a nearly unlimited appetite.
17 But that brings up a negative side. That makes youth
18 more of a target because they are the largest segment
19 using this, and so that's a concern that we should pay
20 attention to.

21 There's a different aspect, mobile bullying is a
22 big deal in the UK. People sending images of kids who
23 have been beaten up. People sending threatening
24 messages to other people. The problem is, that a lot of
25 parents give their kids cell phones as a safety line, so

1 that they can always get in touch with them, so they
2 always want them to have them, but that same safety line
3 is being abused by their peers to bully them. I don't
4 know what you can do about this, necessarily, but you
5 need to take some of the same stands, but the point is
6 that there are different issues at play than we would
7 find in a fixed line world, and they're harder to
8 monitor because they're so distributed.

9 Again, the ISPs, in this case the mobile
10 carriers, often have more at stake as well. This can be
11 an identification device, this can be a payment method,
12 and the wireless carrier has a different relationship to
13 that subscriber than an email provider does. An email
14 provider basically is just a flow through and they bear
15 no responsibility, they're just a channel. Whereas with
16 the wireless carrier, they have a totally different set
17 of regulations, they have a totally different set of
18 expectations, and on a regular basis, they are bearing
19 the liability for this fraud.

20 And as I mentioned already, it's difficult to
21 manage this, it's difficult to deploy the right kind of
22 tools because there are so many platforms.
23 Fundamentally, consumers want features first and
24 security later. So, it's being widely marketed that you
25 have Safari on your phone, and you have OSX on your

1 iPhone. That is a great feature, but it's also
2 potentially a security challenge.

3 So, we need to keep these in mind. It's coming
4 our way. We have a chance to get in front of it, so
5 thank you for your attention and on to the rest of the
6 panel.

7 MS. CHRISS: Thank you, Dave.

8 (Applause.)

9 MS. CHRISS: Next we have Scott Chasin to tell
10 us a bit more about this area, and Scott, as you make
11 your way, Dave used a term, smishing, SMS plus phishing.
12 I want to tell you, I read today that ginormous is now a
13 word in the dictionary, gigantic and enormous. So, I
14 encourage you all to use smishing, spim, spit, as often
15 as you like, I think there's some legitimacy to that.
16 So, let's continue. Scott, tell us your point of view
17 on this.

18 MR. CHASIN: I'm just here to demo the iPhone, I
19 think. I'm the local fan boy. So, in the interest of
20 time, I have a presentation that I'll give you that
21 really is regarding botnets and the evolution of
22 botnets, that's where I spend a lot of my time these
23 days. The CTO of MXLogic, we're managing a filtering
24 service, we have about 18,000 businesses that we filter
25 mail for in the cloud. Some of this presentation is a

1 bit technical, so if you are not an engineer, I will do
2 my best to bring it up a level.

3 One interesting note, on mobile spam in Japan,
4 I've been spending a lot of time in Japan recently.
5 Spam is a huge issue on the mobile phones there. DoCoMo
6 has an incredible amount of saturation of spam on their
7 networks, and the biggest solution that the end users
8 have found is simply to change their email address.
9 That's partly because there's not a real good technology
10 solution that won't impact the operator's revenue since
11 each of the phone users actually pay per message that's
12 inbound, right? And that's a challenge that I think
13 that we have that spans across a lot of different
14 devices, a lot of different markets, and I'm going to
15 talk a lot about push and pull of how this problem is
16 going to emanate and evolve, and impact a lot of
17 different economic infrastructure.

18 So, that said, I'm going to talk about the
19 evolution of botnets, and really I only have three
20 slides. I know we're getting into the stretch here.
21 I'm going to talk historically about what we've seen, on
22 the botnet evolution, and then really where we're going,
23 and give you some I think examples that will highlight
24 the future.

25 For those of you that probably remember this, in

1 1988, Robert Tappan Morris created the Internet worm,
2 which used remote scanning vulnerability checks to
3 saturate the Internet and it spread very, very quickly.
4 That was almost 20 years ago. Here we are today, where
5 remote vulnerability testing is still a very valid
6 opportunity for the propagation of worms. Not only
7 worms, but the infection of Trojans to create botnets.

8 This push evolution, though, quickly, I think,
9 scaled into the email medium, in that the social
10 engineering aspects of email laden viruses in the
11 associated attachments quickly, I think, became news
12 topics and had a lot of success in the nineties, if you
13 remember Melissa and Kournikova, and then obviously not
14 too long ago, the Sobig and the MyDooms and we saw just
15 this huge wave of email worms hit the net, largely being
16 propagated by kind of the egocentric hackers.

17 I think that everybody's in agreement here that
18 times have changed, we have now moved away from the
19 ego-driven motivations of those that want to create
20 viruses to make a name for themselves, like the eighties
21 hackers did, and now into this new world of organized
22 crime and financial motivation.

23 But that's always, I think, impacted the
24 evolution of how these technologies are developed and
25 deployed. So, we've seen email with social engineering

1 wrapped around attachments which were malicious, we are
2 now seeing email obviously that have social engineered
3 URLs, click on this link and then something malicious
4 happens to you, if you do.

5 We have seen within the last couple of years the
6 push mechanic of simply sending out an email that takes
7 advantage of some kind of exploit, let's say, in your
8 mail client, which then infects your machine, simply
9 just by viewing the email message. And then we've also
10 seen the automatic execution of attachments that are
11 embedded in messages.

12 Now we're seeing, quite common, other exploits
13 that are being taken advantage of in common attachments,
14 right? So, whether you're talking about office
15 documents, PDFs, these are things that are being
16 targeted. But I would say that the push method, which
17 has largely been a random shotgun opportunity for the
18 hackers, is slowly going to decline in its favor, and
19 make way for the pull evolution. That's a random, rogue
20 bullet point that's infiltrated my presentation. But
21 the move to pool I think really represents a reaction to
22 what the industry has done over the last few years, and
23 that is we've created inbound filtering barriers.

24 So whether you're talking about inbound content
25 filtering or home firewalls or other inbound security

1 solutions, we've started to derive in essence the threat
2 vector to a pool mechanic. What that means is that
3 we're seeing often times the threat come down off of an
4 end user click off of a download where you have some
5 kind of bundled malicious application that's co-existing
6 with some kind of Trojan carrot, screensaver, I think,
7 application was mentioned earlier.

8 You have even bigger of a threat, the web
9 injection techniques that are being used, taking
10 advantage of browser exports, leveraging I-frames,
11 Javascript, and then within that, I think you have what
12 quite could be the big sleeping giant here, which is the
13 cross-site scripting, cross-site scripting forgery
14 issues, which are just now coming to light really over
15 the last couple of years and I think will have an
16 enormous impact on the Web 2.0 infrastructure in
17 industry, and I will talk more about that, hopefully
18 with the panel as well.

19 So, this push versus pull evolution is
20 interesting when you start to really look at the
21 technology. What's driving botnets really, which is
22 going to be the command and control channels, and we're
23 seeing this evolve very rapidly. I mean, we've come a
24 long way from IRC command and control. It's still,
25 however, a low-hanging fruit for what we would call the

1 script bots out there, bots that you simply download and
2 install, creating your own little botnet or using IRC
3 channels to communicate. But these things are easy to
4 detect.

5 One of my roles is the chairman of the botnet
6 subcommittee at MAAWG and so we get to explore a lot of
7 the different methodologies of detection models, and
8 obviously the low-hanging fruit here is to be able to
9 detect outbound IRC packets, essentially command and
10 control packets for these bots which are infecting these
11 very large pools of consumers inside of an ISP's
12 network. That's pretty easy to do. What's difficult is
13 when they start using peer-to-peer technology. Or
14 what's difficult is when they start using encryption.

15 So, encryption is a very powerful weapon when it
16 comes to how the facilitators of these botnets are
17 controlling each of infected peers. It means that we
18 can't do deep packet inspection. It means that we can't
19 use heuristics within the network layer to look for
20 certain characteristics or behavior which might allow us
21 to tell whether this machine was infected or not.

22 So, in a lot of ways, the use of encryption is
23 going to spoil a lot of detection capabilities that we
24 know today.

25 So, when I look out to the future, I see two

1 things, with bot command and control, again which is a
2 very powerful thing from a detection perspective that we
3 have to understand. One is the use of encryption and
4 the second is the use of peer-to-peer networks, where
5 essentially there is no single facilitator. Each of the
6 infected machines in the network itself has the ability
7 to pass along command or control instructions to each of
8 its peers. Thus, in fact, if you cut the head off the
9 snake, it still lives.

10 And so this is a very difficult thing on the
11 detection side. The other aspect of that is that we are
12 starting to see more and more advancement in the stealth
13 capabilities of the bot infection, we're starting to see
14 the use of basically embedding any kind of command and
15 control packets in high volume common transactions,
16 HDTP, from IRC HDTP, I mean, it's only a matter of time
17 before things like TCP knocking and other types of
18 arbitrary data that's passed through traditional heavily
19 used protocols will also hamper detection efforts,
20 putting us again behind from a technology perspective in
21 understanding who's infected and exactly how that
22 infection is occurring.

23 And then we have now the Web 2.0 cross-site
24 scripting. So, you have these criminal organizations,
25 which are building these botnets and facilitating them,

1 going out and doing whatever they can to hijack public
2 websites. Either because of web server insecurities,
3 because the website is misconfigured, because the
4 website allows for user contributed content to somehow
5 allow the attacker to manipulate those configurations,
6 or because of some other affiliate that is injecting a
7 banner ad that has Javascript I-Frame embedded into that
8 site where it's passed from four different sites and is
9 presented to a trusted website.

10 So, these are very serious issues in the pool
11 mechanic as the facilitators are quickly learning that
12 by placing malicious code on a compromised website, they
13 could now very easily test different forms of malicious
14 Javascript or browser vulnerabilities very easily
15 without that shotgun random approach of the push
16 mechanic.

17 The Web 2.0 cross-site scripting issues are very
18 real, in that it really comes down to stakeless
19 authenticated sessions, allowing an attacker basically
20 to use your own credentials, let's say you being logged
21 into Amazon, you go to a malicious website, the attacker
22 instructs you, or your machine to do a one-click
23 purchase on Amazon. It just so happens that you were
24 logged in to Amazon. That's a cross-site scripting
25 forgery, it's a very real threat and one that could

1 become even more prevalent.

2 I know very recently as of a couple of weeks,
3 there are some very high level community security device
4 and commercial security devices, firewalls, whatnot,
5 that were found to be very vulnerable to cross-site
6 scripting attacks.

7 Another mechanic of the pool evolution of
8 botnets is the use of obfuscation, and this is very
9 challenging, again, from a researcher perspective, it's
10 a very challenging issue in that botnets are leveraging
11 more and more stealth, in especially the ones that hang
12 out on hijacked web servers, they're obfuscating that
13 Javascript code. Even more than that, they're using
14 invasion tactics where they'll present themselves one
15 time to an infected user, and if a researcher tries to
16 go back to that website to see exactly what's being
17 presented from a code perspective, it's gone.

18 So, they're actually becoming very smart about
19 who they attack, and so evasion, stealth, and
20 encryption, in more distribution of these technologies,
21 is going to enable more infection and even more
22 important I think the survival times, the longevity of
23 these infections to occur at higher rates.

24 So, that said, some other points that I have
25 that are not in this presentation, it's spam, spam,

1 spam, but it's really about bots. So, bots are the
2 majority driver of spam today, around the world, and I
3 see the future of bots continuing to evolve. I see lots
4 and lots of challenges, not only on the detection side,
5 by also on the remediation side.

6 So, with botnets, historically, it's all really
7 centered around resource acquisition, right, and we saw
8 very early botnets go out and the botmasters, the
9 facilitators go out and try to harvest as many bots as
10 they could to gain control of as many machines as they
11 could in order to spam victims or in order to hijack
12 credentials, et cetera. That's changed so much,
13 somewhat, as we've seen lower volume, high value attacks
14 occur, where bots are targeted towards specific
15 institutions or specific individuals. This is also, I
16 think, relevant to some of the newer waves of government
17 phishing attacks that we've seen, government represented
18 phishing attacks that we've seen, very recently over the
19 last few months.

20 So, botnet resource acquisition is interesting.
21 Today, obviously, they focus on your consumer broadband
22 connected PC, but you could easily imagine tomorrow it
23 will be your television, or perhaps your Apple TV box.
24 Or perhaps your iPhone.

25 So, the acquisition of resources is vital for

1 their survival, but even more so, what they are doing,
2 which is also testing our capabilities in the reactive
3 detection methodologies that we have today, is that
4 they're testing us, so for every defense or barrier that
5 we put into place, they now benchmark us, as to our
6 reaction time, when we release a new signature, how we
7 distribute that signature.

8 So, it's very common for these facilitators to
9 now create very polymorphic binaries for these bots and
10 do so at a scale which can't compete with our existing
11 resources that we have on the reactive anti-virus
12 signature side. So, that's a key, I think, and crucial
13 point that we have to look at for the scaleability today
14 versus the scaleability that we have today as well as
15 tomorrow and how that evolves.

16 A couple of more points and then I'll release
17 this, the podium. Another thing that I think that you
18 have to look at, I think this is a nice segue, is when I
19 look at spam, and I look at spam in the context of not
20 just email, but all the different communication mediums,
21 it's spam or spit or whatever, it's spam. Obviously
22 today it's email-focused, it's blog-focused common spam.
23 It's social networking focused, but that's rapidly
24 changing.

25 The definition is basically whatever the

1 consumer's attention span is, that's where you'll find
2 spam. So, today, it's in your inbox, tomorrow it's in
3 your voicemail, but also, think about virtual worlds,
4 virtual economies, online mass multiplayer games, all of
5 these are experiencing record amounts of fraudulent
6 transactions and spam that's associated with these
7 different mediums.

8 MS. CHRISS: Great, terrific, thanks so much,
9 Scott.

10 (Applause.)

11 MS. CHRISS: I think a little bit later we are
12 going to want to explore those bot theories and actually
13 how it is affecting or could affect mobile. So, let's
14 reserve that for the discussion period. Rick Lane, come
15 on down. MySpace.

16 MR. LANE: Thank you very much. First of all I
17 would like to thank the Federal Trade Commission for
18 asking me here today. This is another important problem
19 that needs to be addressed, not just from MySpace and
20 its 182 million registered users, but the problem needs
21 to be addressed because it's negatively affecting the
22 user experience for all users across all social
23 networking sites.

24 MySpace, as you know, is a social networking
25 site that allows members to create unique personal

1 profiles online and communicate with their friends.
2 MySpace's extraordinary success and good will is based
3 in large part on the special experience it creates for
4 its users. A critical part of this experience is the
5 user's ability to access the large network of members on
6 MySpace; however, like all large communication networks,
7 from the telephone to the fax machine to email, there
8 are always those who are willing to misuse the
9 technologies to the detriment of others in order to make
10 a profit that we've been hearing today.

11 MySpace is committed to making our community as
12 safe and enjoyable as possible for all of our members.
13 This is an ongoing process that we are constantly
14 reviewing and updating under the leadership of our chief
15 security officer, Hemanshu Nigam, and a world class
16 technology and product team and a 200-plus person
17 support organization. In fact we're looking for another
18 lawyer and two investigators if anyone is out there
19 looking for a job.

20 MS. CHRISS: No one from the FTC, not allowed.

21 MR. LANE: But because we believe there's no
22 single solution to the challenges of Internet security,
23 MySpace employs a wide variety of methods to help
24 protect our community. Every policy we create, campaign
25 we launch, and tool we employ, will always be part of a

1 larger solution.

2 At MySpace, we have taken a comprehensive
3 approach, which includes both technology partnerships,
4 legal tools and education. Some of our back end
5 features that we have instituted at MySpace, one is
6 Phish Lock. Phish Lock is a technology, a tool we use
7 that will automatically lock someone's profile if we
8 believe it's being used for phishing purposes, and in
9 order to stop the massive amount of bulletins that can
10 go out from one site. A user must change his password,
11 once they realize it's locked, in order to unlock that
12 phish lock, and gain access and to hopefully gain
13 control of their profile.

14 We've improved filters and used advanced
15 filtering technology to prevent spam. We've also
16 eliminated the amount of emails one user can send out
17 each day. As some of you may know, MySpace is an
18 internal email system, it's not an email system that
19 goes outside of the site. We've also implemented
20 MySpace links which I think is a very interesting tool
21 that helps us remove bad URLs across all of MySpace.
22 What basically happens is we tag and create a URL, our
23 own URL, so that way once we find a bad URL, we are able
24 to delete it across the entire MySpace network.

25 On the front end, we have obviously the ability,

1 like most of the Internet service providers and others
2 out there, to report spam at any time through a link at
3 the bottom of the MySpace page. You can also block and
4 flag friend requests, which is a mechanism to allow
5 folks who are trying to gain access to your account and
6 block them from getting on. We also block comments, a
7 new feature in the comments section, as we heard, some
8 of the spamming that is going on is through blogs and
9 comments in other areas. So, this allows our users to
10 block that as well.

11 MySpace meets with technology partners, like we
12 all do, and law enforcement around the country to
13 solicit their view points on how we can not only enhance
14 our user security, but also support their efforts at
15 every level. One of the more exciting areas obviously
16 is working with Microsoft as part of its IE7
17 Antiphishing Referral Program. Obviously when we find
18 someone phishing on our site and we find the URL,
19 handing that off to Microsoft who puts it in the
20 database and once that URL is identified, hopefully it
21 will be blocked by others if they're trying to gain
22 access to that URL.

23 MySpace has also taken a series of legal actions
24 over the last two years to combat spam, phishing and
25 other misuse of the MySpace site. We have filed suits

1 against Sanford Wallace and Scott Richter for violations
2 of State and Federal laws, including the CAN-SPAM Act
3 and California's anti-spam statute. In fact, over the
4 past year, we found over ten million spam bulletins or
5 email advertising from Richter's websites and affiliates
6 on MySpace alone.

7 Assisting law enforcement in taking on criminal
8 action against the Sammy Worm, it says Sammy Work here,
9 but that's because I was doing it on vacation and
10 sometimes you just don't pay attention to what you're
11 putting on a slide show, and the operators of the
12 MySpace plus.

13 One of the most notable cases that we've had,
14 and successfully, was against theglobe.com in June 2006.
15 One of the best things that we felt that came out of
16 that was that the Federal Court found that theglobe.com
17 liable for violations of MySpace's terms of service,
18 which prohibited unsolicited electronic communications
19 and imposed liquidated damages of \$50 per email. The
20 Court ruled that MySpace was entitled to recover \$5.5
21 million in liquidated damages, and this was the first
22 court ruling in the United States enforcing the
23 liquidated damages provision such that the one that was
24 found in MySpace's terms of service.

25 Educating our users is one of the most critical

1 issues that we all agree, I think, in this room, is
2 necessary of trying to ensure that they are protecting
3 themselves, as was mentioned by Michael, that as we lose
4 control, it's going to be the empowerment of our users
5 to help protect against unwanted spam. One of the
6 mechanisms we use is a very popular use of Tom Anderson.
7 Tom is your first friend on MySpace, so when you sign up
8 for MySpace, you see Tom. In fact, for my nieces who
9 are 17 and 18 years old, the only reason that I have any
10 coolness at all is because I know Tom. But besides
11 that, he's somebody when he sends out a message, people
12 respond, people read it, and we have used that to help
13 explain to our users about spam phishing and provide
14 them with safety tips so that way they have the tools
15 and knowledge to help protect themselves. That, when we
16 send those out, that has led to members of our community
17 telling us about phishing URLs that they're aware of so
18 that we may be able to take the appropriate action.

19 When I testified in front of Congress in 2001,
20 it seems like it's been longer than that, but 2001 on
21 the spam legislation, I emphasized that the goal of any
22 legislation regulating the use of commercial email must
23 not hinder legitimate businesses from reaching out to
24 potential clients, but must specifically target the
25 clear abuses. I believe the CAN-SPAM Act has provided

1 the Federal Government and businesses with effective
2 tools to go after those individuals; however, we may
3 have reached a time to examine if additional legislation
4 is needed to create an even greater deterrent for those
5 who continue to catalog our email systems, social
6 networking sites and in the future mobile devices with
7 unwanted spam.

8 Right now it seems as though some spammers are
9 treating fines just as a cost of doing business. One
10 step that can be taken without additional legislation is
11 sending more spammers to jail, not just giving them
12 fines, but on the legislative front, some ideas that we
13 have looked at include adding civil forfeiture to the
14 CAN-SPAM Act and creating even more accountability for
15 spammers who hide behind affiliates who do their dirty
16 work from which they profit, and that was something that
17 was mentioned earlier today during the first panel about
18 the problems of affiliates and control thereof.

19 With that, I'm happy to answer any questions and
20 thank you very much for inviting me here today.

21 (Applause.)

22 MS. CHRISS: Thank you, Rick. Well, terrific,
23 thanks to all of the panelists. Oh, my goodness.
24 Chris, I apologize. Talk to us, I know you have some
25 very unique topics to address, so let's hear it.

1 MR. ROULAND: Thank you for not forgetting about
2 me. Thank you for having me here.

3 I made a connection with the FTC at the RSA
4 conference earlier this year in February, I had dinner
5 with Dale Fuller, the former CEO of McAfee, one of RSA's
6 general managers for PassMark and Chairperson Majoras,
7 and I got to talk to her about the future of the FTC No
8 Call List, and she was very interested when I submitted
9 that No Call List would be completely obsolete in 24 to
10 36 months as we move to sifting Voice Over IP
11 infrastructure and that we have limited ability to
12 enforce no-call measures against, say, spammers sending
13 messages from Nigeria or Canada or Brazil or China, and
14 subsequently came up to brief her team on that, and
15 that's something that I would like to talk about across
16 the panel.

17 What I have in my slides, however, is kind of a
18 profile of propagation patterns we're seeing for
19 malware, and I thought this was important to frame where
20 threats are going in that most of the spam threats we
21 see today are really just payloads from infected
22 machines and understanding how infection patterns are
23 moving across the network, how they're changing and
24 being optimized for maximum impact is important to
25 understand as we come up with new strategies to defend

1 consumers' machines.

2 I got a little nervous when a couple of the
3 other panelists started to drive into the top of this,
4 but they fortunately didn't spend too much time on it
5 and left me some depth to go into this. This slide is
6 in here, one of our engineers is actually an artist as
7 well, and came up with these icons as well. My favorite
8 is the sequel injection hypodermic needle there, but the
9 point I'm trying to make here is that if 79 percent of
10 consumers already have anti-virus, why is there a
11 problem today? And obviously there's a technology gap
12 with the protective measures that are being used by end
13 users today, and the propagation methods that are being
14 executed by VXers, which is the term for the virus
15 writers.

16 There is another term I heard in here today
17 called drive-by malware. That's a continuing trend.
18 There was a study by a consumer researcher, if you do a
19 search on drive-by malware, you'll find this, and he
20 actually took out an ad on Google, and it was a pop-up,
21 it wasn't a pop-up ad, it was an ad on the side of the
22 Google search bar and it said, "Is your computer virus
23 free? Click here to get inspected," and he had over
24 1,200 hits in a few hours of people clicking to infect
25 their computers.

1 So, I would submit that if consumers are
2 actually asking to get infected, they may actually not
3 have a chance, and there are some things that we need to
4 learn from there, and technology I think remains to be a
5 method to solve some of those problems.

6 I like to use this model, because it's a model
7 of typical viral propagation, and for those of you who
8 can't see it up here, it's basically a bell curve with a
9 long tail. This infection pattern represents kind of
10 what we had typically seen in viral attacks. This one
11 has an existence of about 20 hours on it.

12 And what we see is the 100 percent intensity
13 here represents the maximum infectable population of
14 users, and there's a similar model in epidemiology, it's
15 called the SIR model and actually maps pretty well onto
16 computer malware and malware infection rates, and SIR
17 stands for susceptibility, infection and resistance, and
18 in the computer world, the susceptible population is the
19 population that is using or operating on a platform that
20 is potentially vulnerable to infection from a piece of
21 malicious code.

22 The infection occurs when that malicious code
23 then takes a foothold on those machines and the
24 resistance or inoculation is actually applied when a
25 sample of that malware is transmitted to them, just as

1 we get resistance from disease by becoming inoculated
2 from it or developing resistance, our computers today
3 have to develop resistance to malcode by receiving a
4 small sample of that malcoding, and we call those
5 signatures, or updates from anti-virus companies.

6 The last slide, 79 percent of our consumers
7 claim to use anti-virus software, so what's not working
8 here.

9 One of the changes we're seeing in propagation
10 models is that this model is not very profitable to a
11 spammer or VXer who is operating for profit, because in
12 this long tail, infection, we're seeing users get
13 cleaned up, they develop resistance, they receive
14 resistance and the malcode goes away. So, this model
15 has been gained so that operators can gain the maximum
16 foothold during their propagation attempts, and the
17 least amount of population can develop resistance. So,
18 ideally, in a bad guy's shoes, you're going to infect
19 the most mal population with no resistance being
20 deployed.

21 There's obviously also a technology gap in that
22 we are depending on a sample to be transmitted. So,
23 that means we have to find a piece of the virus itself,
24 transmit a tiny piece of that out to hundreds of
25 millions of PCs.

1 So, we began to see a change in the patterns for
2 malcode propagation a few years ago and we call this
3 first change of attack short span attacks, and it's
4 interestingly enough working in the AV and security
5 industry for quite a while, you may not know the fastest
6 way to get an anti-virus company to put out an update.
7 The fastest way to get an anti-virus company to put out
8 an update is to have the media write about it or publish
9 something about it. It can be the smallest, most
10 innocuous virus or Trojan horse that only affects 100
11 users, the fastest way to get an update on it is for it
12 to get profiled in the media. It doesn't matter if
13 100,000 users are infected, that's secondary to media
14 coverage.

15 So, it's interesting, and the VXers seem to have
16 recognized that, they want to get their malcode out
17 under the radar, if you will, not that the media is a
18 very effective malcode detection source, but they're
19 simply one vector or source of potentially notification
20 to these AV companies.

21 So, what they began to do was combine spam
22 distribution methods with malcode propagation methods to
23 get a quick shot of malcode out and then subside or stop
24 the propagation very quickly. These two, these two
25 characteristics generally lead to fewer notifications,

1 fewer emergency updates, and fewer complaints from
2 customers, forcing AV companies to transmit out
3 inoculation to population.

4 In the last two years, a more modern type of
5 attack has emerged, and I'll expand a little bit on what
6 Dave had talked about, and we're calling these attacks
7 serial variance attacks. These serial variance attacks
8 are completely gaining the inoculation model we have
9 today in the AV industry and they're doing it to extend
10 this window of infection.

11 What we actually see in software engineering, we
12 have a term called QA testing or quality assurance
13 testing and that's where we test or QA our products to
14 make sure they work the way they're supposed to. We're
15 actually beginning to see QA testing of viruses, so
16 we're seeing computer viruses are going through rigorous
17 software engineering technologies to make sure they
18 function properly and most important that they are not
19 detected by the AV products.

20 So, we see entire families, a family of viruses
21 is a group of computer viruses or bots derived from a
22 similar code base that are pre-engineered at once but
23 signed so that the same inoculation pattern or signature
24 pattern won't catch them and nobody can see them
25 released on these iterative cycles and closely based

1 intervals, again using the spam-based propagation
2 techniques to transmit these out, and you'll see the
3 timing on these serial windows is designed to really tax
4 both our ability to update our systems as well as tax
5 the traditional AV industries method.

6 So, there are two examples here. One is the
7 Storm Worm, which was mentioned earlier, another one was
8 the WZ Stration, which is really one of the most
9 aggressive types of these serial variant storms we've
10 seen. So, Stration was interesting, because it almost
11 iterated on a weekly cycle, and operated on kind of a
12 normalized schedule.

13 In the first attack we saw, we saw 32 variants
14 in ten hours. Exactly a week later we saw 61 variants
15 in 24 hours. You can read the rest of these, again,
16 with the Storm Worm, starting this year, we saw a
17 maximum of 55 variants in 19 hours. Of course, if
18 you're updating your antivirus software once a day,
19 you're going to be 54 variants behind on this attack.

20 And so one of the things I think we have to do
21 is challenge industry to invent new ways to detect and
22 block malicious code. This does, however, lead us to
23 some of the more interesting propagation methods we're
24 seeing in the next generation platform, specifically
25 around mobile devices. I was actually called out last

1 year to a large mobile carrier in Europe, and with over
2 100 million users, it was an emergency and they wanted
3 us to clean a piece of malware off their network, and
4 they were seeing about 5,000 infections a week. I said,
5 well, 5,000 infections a week, you're doing pretty good
6 with 100 million users. And they said, well, Chris,
7 this malware destroys cell phones, the users basically
8 throw away their cell phone and they have to buy a new
9 cell phone.

10 I said, that's kind of expensive, if you have to
11 replace 5,000 cell phones a week, we'll get on this and
12 fix it for you. And we found a way to detect it, but
13 what we were seeing were variants of a phone virus
14 called the Commwarrior Virus, and it's very interesting,
15 there have been about 30 variants of this virus that
16 affect mobile phones and they were experiencing with
17 diurnal propagation method, which allows for one
18 propagation method during the daytime and a different
19 propagation method at night time. In this case they
20 found the most propagation method for this virus was to
21 actually propagate over the Bluetooth vector during the
22 daytime so it actually turned on your Bluetooth on your
23 phone when you're commuting to work, say on a train,
24 infect everyone around you via Bluetooth. At night it
25 would turn off your Bluetooth, interestingly enough to

1 preserve battery life, and transmit to all of the people
2 in your phone book by SMS and the next morning would
3 start the whole thing over again.

4 We actually saw a version of the worm that
5 propagated only over Bluetooth but your battery life was
6 limited to a few hours, what was happening is consumers
7 were taking their phone into the store and asking for a
8 new battery on their phone, which was expensive costs.

9 So, I think the last point there, to tie in
10 voiceover and PDA, we will talk across the panel on
11 this, we were seeing the methods applied to propagation.
12 I think the code knows no boundaries as to platforms
13 whether it's iPhones, Symbian, Windows Mobile, or other
14 mobile platforms. But the last convergence we're going
15 to see that will really sew all this together is in the
16 next 18 months in the United States, our mobile carriers
17 will converge voiceover IP and mobile handsets. When we
18 get a VOIP stack, a voiceover IP stack on our handsets,
19 that becomes a very attractive target, not only for
20 transmission of spit or spam over mobile telephony, but
21 for receiving unsolicited calls.

22 Today we've got dribs and drabs of voiceover IP
23 by PDA users, two and a half million a year, five on
24 Vonage, a few on Comcast, but when our carriers cut over
25 50 or 100 million voice users overnight, we're going to

1 have a very target rich population in which we will
2 begin to see attacks against that population over this
3 new protocol.

4 So, I think that was it for me, and we'll go to
5 the panel.

6 MS. CHRISS: Yes, thank you so much, Chris.

7 (Applause.)

8 MS. CHRISS: So much of this information is just
9 jaw dropping when you hear about some of these potential
10 threats, but what I want to do is spend just two minutes
11 honing in on exactly what are these threats? I want
12 Scott, for example, to tell me how can my mobile phone
13 be turned into a spam bot? Just tell me how that works.

14 MR. CHASIN: Well, if you have an iPhone, it
15 can't. Spoken like a true fan, I believe. You know,
16 it's largely going to depend on the security of the
17 operating system. The open paths into that device, I
18 think obviously it's been shown, Chris has mentioned
19 that Bluetooth can be an enabler. I think there's lots
20 of different threat vectors that exist. The problem
21 that we have is that we want these things to become more
22 and more advanced, which means more capabilities, and so
23 they are resembling truly a mobile desktop, and I think
24 that the iPhone is a really good example of a device
25 that within its first few hours of being born was hacked

1 over and over and over again and continues to be.

2 So, it's only a matter of time before we see
3 that transmission the bridge that's built. We've seen
4 it in spots, around the world, but I think that
5 it's around the corner, it's not here today, simply
6 because the bot resource acquisition is just so enamored
7 with our consumer broadband PCs, but there's a lot of
8 different paths in there.

9 MS. CHRISS: Okay, okay. That's good. Thanks
10 so much, Scott. Now, a few of us here on this panel, we
11 talked about how what's happening overseas is really a
12 good way of determining what we're going to see here in
13 a few years. I want to hear concrete examples. What's
14 happening? Chris, you gave a good one.

15 MR. ROULAND: Sure. Actually, we studied
16 malicious code from overseas quite a bit, and in certain
17 parts of the world, we're seeing some more advanced
18 online technologies. A great example is Latin America
19 where PayPal type functionality is standard in all
20 online banking.

21 The new malcode we see from there is
22 particularly scary, we're calling it stakehold phishing
23 bots. The way they work is your computer gets infected
24 with this bot, once you've logged into the bank, it
25 hijacks your credentials and withdraws, via their

1 built-in PayPal functionality, money from your bank
2 account.

3 Normally it wouldn't be a big deal because you
4 would expect to see that money missing, however it
5 actually maintains stake or keeps track of the money you
6 withdrew from your account and when you go to re-render
7 or review your HTML page, it adds that balance back in,
8 so your balance appears to be whole.

9 Typically for online fraud you've got 90 days in
10 our country for an ACH, to remit a fraudulent ACH and
11 after that it's over. So, we're seeing this very
12 sophisticated, multi-factor authentication theft, and
13 maintaining stake on the transaction is actually made to
14 defraud the consumer, I think we've got a lot of
15 exposure there as we move to those types of online
16 services.

17 MS. CHRISS: Okay, terrific. Dave, you talked
18 about how in Asia, they've been using 3G for a while.
19 What can we expect based on what you know?

20 MR. CHAMPINE: Well, I mean, we see a number of
21 exploits that, again, are jaw dropping. There's an
22 example that I run across a few days ago called FlexiSPY
23 that there's consumer products that are available for
24 sale by pseudo legitimate businesses, and you can
25 literally download this on to Symbian, BlackBerry or

1 Windows Mobile and it is a complete espionage tool. You
2 can record voice conversations, you can intercept all
3 SMS messages and emails, you can remote control the
4 device over SMS. So, things like this already exist,
5 and they're already serious problems. It's just that we
6 haven't experienced them here, because we don't have the
7 same usage profile as Europe and Asia.

8 MS. CHRISS: Okay. Are you seeing solutions
9 being developed in Europe and Asia?

10 MR. CHAMPINE: Yeah, definitely, and some of it
11 is coming through traditional security vendors. A lot
12 of it is coming through a collaboration of the carriers,
13 the handset manufacturers, and the security firms, and
14 that's probably something that because it is a bit more
15 of a closed loop, there's more constituents, but at
16 least it is a bit more of a closed loop, we're seeing
17 that more in the mobile space than we have historically
18 in the wired space.

19 MS. CHRISS: Dave, you used a great word,
20 collaboration, that's an ongoing theme for this summit,
21 and I think that's what we'll see here in the States and
22 in the U.S. and North America that it will be about
23 collaboration between public and private entities, for
24 example, global cooperation. So, that's good to
25 highlight.

1 MR. CHAMPINE: And I think we have a better
2 opportunity, because there aren't as many national
3 boundaries and nationalistic tendencies, hopefully.

4 MS. CHRISS: Yeah, yeah. Well, good. Well,
5 Mike, I know that you work with hundreds of wireless
6 providers and your organization can be such a good
7 source of information. Are you guys considering whether
8 or not to kind of get consumer feedback on their
9 experience with malware on their cell phones? Is that
10 something you anticipate being able to study?

11 MR. ALTSCHUL: We don't have the visibility as
12 an industry association that any of our members and our
13 large members have. But there are industry forum, or I
14 guess we should say fora, where the subject matter
15 experts from the industry gather regularly and share
16 this information and we've participated and observed it.

17 So, it is being monitored, it's not necessarily
18 being monitored by CTIA. Again, because it is a global
19 industry of global platforms, we have the benefit of
20 knowing what's going on elsewhere.

21 One of the earlier questions you asked is what
22 else have we seen and what are some of the responses. A
23 couple of years ago, I think that everyone was aware of
24 Bluetooth's vulnerability and identity theft base.
25 There was something that was nicknamed I guess blue

1 snarfing, where if your phone was turned on a Bluetooth
2 port, malware could actually access a lot of the stored
3 information in a device, and be exported not over the
4 commercial spectrum, but over the Bluetooth space.

5 Just last month I was visiting a Bluetooth
6 special interest group here in Washington State, and
7 they were talking about how they have re-engineered the
8 Bluetooth specification and interface has now released
9 2.1 or whatever. So, as to make Bluetooth more secure.
10 So, it's that kind of iterative learning of
11 vulnerabilities and engineering solutions and then
12 releasing them that will allow us, we hope, to remain a
13 little bit ahead, a half a step ahead of most of these
14 threats.

15 MS. CHRISS: Well, terrific. Rick, we watched
16 in amazement as you talked about the different cases
17 that MySpace has brought against one of our very own
18 panelists from earlier today, in fact. It sounds like
19 the exploits are really taking advantage of
20 technological vulnerabilities. MySpace, it's uniquely
21 situated. You've got a community, you've got a captive
22 audience, and these technological tools seem to be easy
23 to use.

24 Can you tell me about what technological steps
25 your guys may be using to thwart the efforts of the bad

1 guys?

2 MR. LANE: We're always trying to develop new
3 and innovative ways of protecting our users. I mean,
4 that really is the biggest complaint we get from users
5 of especially when somebody has hijacked their profile,
6 and their friends think that they're sending out these
7 bulletins on different ads for different types of
8 products and services that are out there, and it is
9 really hindering the user's experience.

10 I mean, obviously there are things that we are
11 looking at and doing and testing that we don't talk
12 about, because you don't want to give a roadmap to the
13 bad guys of what we're doing, but looking at working
14 more closely with law enforcement and the FTC and others
15 to go after those individuals who, again, someone who is
16 talking about social engineering I think is the term
17 that someone used. I mean, MySpace and social
18 networking sites are created for interaction, and they
19 are using those vulnerabilities across Bebo, Facebook,
20 MySpace, Xanga and the rest as a way to hijack or sell
21 products or other malicious things. So there's an
22 educational aspect.

23 As you mentioned, in talking about the
24 technological side, I think the phishing, our stop
25 phishing programs that we have and in other areas I

1 think are helpful, but sometimes it's just overwhelming
2 and you just need to try to figure out through the
3 entire community what can be done. I think giving more
4 tools to our users and having them help report when
5 things are going bad, as we were talking about earlier
6 on the CTIA, it is going to be one of the most effective
7 tools that we have.

8 MS. CHRISS: Wonderful. That's good. Getting
9 effective tools, technological tools, that is just
10 another theme that we're hearing throughout the day and
11 we'll hear more about that tomorrow. So thanks for
12 sharing that. Another thing you said, Rick, was the
13 arrests being perhaps the greatest deterrent for these
14 bad guys, and I just want to put a plug in for
15 tomorrow's panel with criminal law enforcement will be
16 here and present and telling us all about it. So, I
17 hope everyone comes back for that.

18 Now let's open it up to the audience just for a
19 few moments here. Do any of you have any questions for
20 these panelists? It looks like I have one here. Let's
21 take a look. Great, let's start with this one.

22 We've heard about financial motives earlier,
23 what are some of the other motives that spammers have
24 going on for them and what are some of the motives
25 regarding these emerging threats? Is it financial also,

1 are there other motives here for these guys in terms of
2 targeting mobile phones and social networking websites?

3 MR. ROULAND: I would say no, it's all about the
4 money.

5 MS. CHRISS: All about the money, okay. Anybody
6 care to add to that?

7 MR. CHASIN: I mean, there are trends that we
8 have seen in recent news, very recent, of using, in
9 particular botnets as weapons. So, whether that's in
10 denial of service attack to take down or cripple the
11 infrastructure of a government and we've seen throughout
12 the last four years, lots of examples of that, and
13 that's a growing trend.

14 We've also seen the terroristic use of botnets
15 for dissemination of hate messaging, such as the Sober
16 Worm and its infections. So, there are outside of
17 economic gains, which I would say is primary today, the
18 motivation, there are trends that can point to botnets
19 and the delivery capabilities of them, and the
20 destruction capabilities of them to be used for
21 malicious purposes or to promote certain ideologies.
22 So, they are good examples of that.

23 MS. CHRISS: So, not just about the money, we've
24 got issues like terrorism, we've got some serious issues
25 here that are at play. So, that's a good thing to

1 raise, thank you, Scott. We have an audience member.

2 MS. SAULNIER: This is in a similar vein, I
3 mean, I don't understand the economics.

4 MS. CHRISS: I'm sorry to interrupt, could you
5 state your name and affiliation.

6 MS. SAULNIER: I'm Julie Saulnier with the FCC.
7 I don't understand the economic incentive for a worm
8 that destroys cell phones, I assume it's not made by the
9 manufactured equipment or the security company. What's
10 the economic incentive?

11 MS. CHRISS: Good question.

12 MR. ALTSCHUL: Let me answer a different thing
13 that we have observed, which is just a variation on an
14 old fraud and it's not very high tech, but in the U.S.
15 we've had 900 area code numbers which end up generating
16 a premium charge to the caller, and there are some
17 countries in the 809 Caribbean area code that have
18 similar numbers that look like order numbers. This has
19 been a problem for 20 years or so from wired and
20 wireless phones. The etiquette of wireless phones where
21 you actually will have a call record and many people
22 will take a look and see that they have missed a call
23 and want to call back, has generated sort of a phishing
24 kind of scam, where people will call and either through
25 spoofing or whatever leave one of these numbers on the

1 caller's phone, solely to generate revenue to one of
2 these sites, and drive additional revenues to the site.

3 MR. ROULAND: Also, so a piece of malware that
4 destroys a mobile phone is a bulky piece of malware.
5 Other things that are available have been leveraging
6 premium SMS services or reprogramming your phone book to
7 dial through an alternate long distance carrier. An
8 example of a phishing attack is asking you to send a text
9 message in response to a premium service to unsubscribe
10 you to a Spanish dating service so it keeps sending a
11 text message to your phone to see if you want to
12 unsubscribe to a dating service you've joined for \$10.
13 So a lot of people say, geez, I want this thing off my
14 phone and they just pay.

15 MR. CHASIN: Let me add on the bright side it's
16 not a pathogen's best interest to kill its host.

17 MR. CHAMPINE: I would say that some of this is
18 related to the new frontiersness of it, so a lot of it is
19 testing the waters, how much can we do. There are
20 instances in India, for instance, where they sent out
21 bulk SMS messages saying that there was a virus that
22 would actually pass from the phone to the user, and they
23 had many, many thousands of people responding in great
24 fear. They had SMSes that went out in Lebanon saying
25 that you've won a new car, and they had something like

1 100,000 people show up at the dealerships. Just
2 creating that kind of chaos in itself is a tool.

3 MR. LANE: And also, I mean, in terms of sending
4 out malicious code to distract, you send it over here so
5 everyone is focusing on the right while you are doing
6 small attacks on the left while no one is focusing
7 because they're focused on the right, and that's a
8 standard technique as well.

9 MS. CHRISS: Very good. Very good. Yes, sir?

10 MR. SETTLEMYER: Carl Settlemyer, Federal Trade
11 Commission.

12 I just have a question that sort of anticipates
13 what is going to be discussed tomorrow in terms of your
14 own views with the emerging threats. What steps,
15 nontechnological steps, do you think that agencies like
16 the Federal Trade Commission or the Congress should
17 mandate in terms of trying to get out ahead of this and
18 trying to prevent some of these things from happening
19 and what sort of suggestions would you all make in terms
20 of maybe your top one or two things you would see as
21 being beneficial to consumers in terms of heading off
22 these problems and reducing the aggregate costs of the
23 problems can entail and impose on consumers collectively
24 over the next decade?

25 MR. ALTSCHUL: Certainly consumer education from

1 as many different voices and corners as possible.
2 Industry, the government, everyone has an important role
3 with emerging technologies and emerging threats.

4 MR. CHAMPINE: I would say along those lines,
5 working closely with the carriers and service providers
6 themselves, they are going through a transition time,
7 particularly in the U.S., and so both helping to
8 reinforce the education, helping to standardize the
9 policies and practices, but also acknowledging that they
10 are switching revenue streams and that you can't be too
11 Draconian about this, it still needs to be a business
12 venture.

13 MR. CHASIN: I would say it's definitely
14 collaboration and research, more research is needed, and
15 this is a global epidemic, it's not just in the U.S.,
16 and the threat vector is so distributed worldwide is
17 that we can't take that perspective.

18 So, I'm also, in the context of just spam,
19 there's a lot of research I think that still needs to be
20 done around how we manage identities online. There's I
21 think a good opportunity there. I, for one, would
22 really appreciate just having a new sort button on my
23 mail client that could tell me whether or not that
24 message was human originating versus machine
25 originating. That one little thing obviously impacts

1 the entire eco system of identity, but nonetheless, it's
2 those kind of thoughts that we need to look at from a
3 long-term research perspective, but research and
4 collaboration.

5 MR. LANE: One of the things I mentioned was
6 providing civil forfeiture. Right now you have at the
7 Federal level in the government, you have criminal
8 forfeiture, but the government and law enforcement can't
9 go after everybody. They just are limited in their
10 resources, and creating some more teeth that we have on
11 our side to go after individuals I think would be a
12 great deterrent, so it's not just a cost of business.

13 On the education side, I can't agree more that
14 it's very important. The problem that we find, though,
15 on the education front, is that no one listens, as we
16 heard earlier, and it's the same problem we find on the
17 online child safety front is that those who listen are
18 the ones who already know and the ones who don't listen
19 are the ones who don't know. I mean, it's a very
20 frustrating situation, and hitting to those 30 percent
21 or 40 percent of the folks who aren't being active on
22 this front is the difficult part, but that's where, as
23 someone had mentioned earlier, the vulnerabilities are,
24 and I just don't know how to answer that one.

25 MR. ROULAND: There's been some really

1 interesting work done around sovereign network borders,
2 and treating the 26 undersea cables that come into this
3 country as ports of entry and having the borders, the
4 customs and border protection agency enforce those.
5 Just as they would secure physical ports of entry,
6 inspect and block all this crud that's coming into our
7 country and allow law enforcement to focus on problems
8 inside this country and sending our own law enforcement
9 guys to Nigeria or Egypt to take these guys down.

10 So, I think it's something worth exploration and
11 consideration as to treat ingresses as ports of entry.

12 MS. CHRISS: Terrific. I think that is our time
13 for today, and I just want to share with you a few of my
14 own observations, and that is, I'm echoing the
15 brilliance of these panelists when they talk about
16 collaboration, when they talk about filling the
17 technological gap, as someone put it, and this outreach,
18 making sure people listen to what we're telling them
19 about how to prevent problems and how to make our
20 education efforts even better than they are, and
21 business education, right? CTIA members. They need to
22 know, all of these providers, they need to know how to
23 secure their systems as they enter into the world of
24 convergence more and more. So, I want to thank you all
25 for highlighting those very important points for us, and

1 I invite everyone to join us again tomorrow, bright and
2 early, let's hope for good weather, and thank you.

3 Thank you all.

4 (Applause.)

5 (Whereupon, at 5:15 p.m., the workshop was
6 adjourned.)

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1 C E R T I F I C A T I O N O F R E P O R T E R

2

3 CASE TITLE: FTC SPAM SUMMIT: THE NEXT GENERATION OF
4 THREATS AND SOLUTIONS

5 DATE: JULY 11, 2007

6

7 I HEREBY CERTIFY that the transcript contained
8 herein is a full and accurate transcript of the notes
9 taken by me at the hearing on the above cause before the
10 FEDERAL TRADE COMMISSION to the best of my knowledge and
11 belief.

12

13 DATED: 7/24/07

14

15

16 SALLY JO BOWLING

17

18 C E R T I F I C A T I O N O F P R O O F R E A D E R

19

20 I HEREBY CERTIFY that I proofread the transcript
21 for accuracy in spelling, hyphenation, punctuation and
22 format.

23

24

25

SARA J. VANCE