<meta name="viewport" content="width=device-width; initial-scale=1.0; "\>Event ID: 1932884
Event Started: 5/24/2012 6:00:00 PM
---

Please stand by for realtime captions.
>> Hello everyone, thank you so much, I am Sandra Shirer, I am the training manager, I want to welcome you to the webinar. We are focusing on minimizing IT security risks while using social media.
>> When we first that the webinar up I was going back and thinking of several years ago there was a huge awareness on IT security especially when it came to spyware and now where for computers -- now where -- malware for computers.
>> There is a lot of information on how to prevent cyber criminals from getting access to your computer. Today that same awareness is just as critical for social media. To help us learn more about that we have two experts that will help us today. First of all we have Kurt Garbars who is the senior security officer and has been over that program for the past 11 years, he comes with a wealth of knowledge when it comes to security and other information.
>> Then of course we have Kevin Haley who is the director of project management for Symantec Security Response. He has been around for 12 years and he has led development of the company's antivirus solution.
>> Without further ado I would like to introduce to you Kevin Haley and Kurt Garbars.
>> Thank you, this is Kevin Haley, I will kick off the presentation, I get the fun part, at least for me. I will not talk about minimizing the risk, I will talk or about the risk and what it is.
>> Before we get started I would like to ask if anybody knows this person, her name is Rob in -- Robin Sage, sorry to say I'm not a Green Beret. Just a cute girl stopping by to say hello, my life is about in so security all the way.
>> She is a graduate of MIT and a cyber threat analyst.
>> She is 141 twitter followers, 110 Facebook, and 148 link 10 -- 110 Linkedin, she is people following her from NSA, US Marines, House of Representatives, Pentagon, DOD, Lockheed Martin, Northrop Grumman, and Allen Hamilton. She is a well-connected person and someone that would be great to add to your network with all that security experience and the connections she has.
>> The only problem is she does not really exist, she was created by a security researcher, he is wearing the hat on the side. He created her to make a point that people are sometimes branding and -- friending people that they don't really know because social media allows us to create personas that are not necessarily true.
>> This happened back in 2009.
>> He talked about in early 2010 and here is the story. It is good news, this is all over, this sort of thing never happens because we are all too smart. I should point out that if you do want to look, the twitter site is still there, Tom Ryan, the creator is using it to promote himself. Robin has a lot less people following her than she did when he was -- when people thought she was real.
>> The good news is no one falls for this sort of thing anymore.
>> But then of course I read a couple of months ago the this gentleman James DeBord S. -- Stavridis did not have a Facebook account but someone created one for him and people begin to friend him and engage with him when it was not really him.
>> This is his real page now, this is truly a page, if you get a friend request now, I can tell you that this is legitimate, when you look at it looks nice, and professional eerie at
>> --.
>> You might get fooled by this because it looks good, but there is really nothing there that you could not find somewhere on the Internet.
>> I guess I am just trying to say that it is always possible to get fooled, we cannot live our lives being so suspicious of everything that we are first and into not doing anything and we never friend anyone again. But we can try to be sharp and aware, just a little suspicious.
>> Here is a LinkedIn in termination request I got, you can see this picture is kind of fuzzy and when you look at her experience, she is like a good leader college, but all of her experience does not look very deep. The whole thing looks funny, I can tell you that I did not accept this invitation.

>> If it is obvious that it is not a real person you should not be that desperate to build your numbers up a little common sense will protect you quite a bit.
>> It did not protect 141 other people.
>> If you do not know who someone is or something seems wrong, it probably is.
>> All of this is to say that we have reached a really interesting point in the world.
>> The historic method of gathering data for social engineering and finding information about somebody used to be done like this. Dumpster diving.
>> I used to see people go in the trash and find out what you can find on you, today it is social media. That is why we are here today and that is what we are going to talk about. This is just one example of the trouble you can get yourself into.
>> I also want to talk about trouble you can get into that is not necessarily bad guys after you, it is kind of trouble you can get into yourself as we start using social media.
>> This is a link from Chrysler auto that got sent out a year ago. This is the actual treat -- tweaked -- tweet, I put a red bar over one of the words, but this is one of the things that it they do not want to have people see, your guests and my guess is this is not something they intended to send out, but in fact they did.
>> Later they sent another tweet saying our apologies  our account was compromised earlier today. We are taking steps to resolve it.
>> This is a mistake somebody made is my guess, later news reports did indicate that they used an advertising agency to send a tweet  out for the agency and someone did that.
>> How could that possibly happen? It seems crazy, the guy has to know he is going to lose his job if he send something like that.
>> This came out from the Secret Service, but this is probably not be in H. that the secret -- in H. -- image the Secret Service wants to pretraining.
>> How did that happen?
>>  If you look at how it was send it was done with twitter for iPAQ -- iPad.
>> Last I heard they were not issuing I pass -- iPads to people in the Secret Service, what I suspect happened is he is very hip on social media, has his own twitter account, since his own tweets out and does it from his personal I tried it and got confused and thought he was sending something out to his personal account, that actually sent it out over the secret service account.
>> If you are a Tweeter for your company or agency or business, you need to make sure you know which account you are using. There is software that helps you keep that straight.
>> There's also something that builds approval processes before you send something out.
>> You need to be careful about what you tweaked -- tweet . And separate work from personal.
>> In the beginning of last year this tweet when out from  NBC news, it was in September of 2011, breaking news about a flight crash, if you remember September in 2011, nothing like this ever happened.
>> Somebody went into the account and said we hacked this. It is not a joke, it was but it was not a good joke at all.
>> They went out and said the account to secure and we apologize for the scare, we value your request -- trust.
>> I'm sure they do but they lost a lot of trust right there.
>> Final insult to injury, this is the final tweaked -- tweet that they sent out .
>> This is not someone mistaking the sending a personal tweet  Hackers did get in there.
>> The temptation is to think that these genius hackers broke in and did this. Now they are sending tweet  out whenever theywantt.
>> The reality is that the way this happens is a lot simpler and easier to fall for.

>> Unfortunately you do not have to be a genius to pull this off.
>> Let me give you an example.
>> Here is a tweet that came through.
>>  In is a common, on, someone posted pictures of you all over twitter.
>> Of course I want to see what that is all about, I am going to think -- click on this link, it happens to be short, useful and twitter, doesn't tell me what I'm going to, but when I get there I see it's the login page, I guess I have to log back

into twitter, maybe I was using another interface or I got locked out, these things happen.
>> So I am going to login again. Does anyone notice the problem?
>> If you look way up in the corner it is not twitter, it is Al twitter -- Ltwitter this is a unique pack -- hack, there is that l that is hard to see, and you might miss it eerie at
>> Now somebody else can login as you and cause a lot of damage.
>> This is bad news that is easy to do, it will get easier. I imagine you are doing twitter on your phone, you can't even see the URL to know if it's a bad site.
>> Which one is the real log in for Netflix?
>> If you guessed the one on the left you are correct.
>> There is more data on there, it looks more official, but you have to admit that they look pretty much the same. There is not a lot of information on either one to give it away.
>> Mobile phones present a problem and they make phishing is here if we are not taking steps to protect ourselves.
>> Let me go to one last thing on twitter.
>> This is my page.
>> You can see my thoughts on security, social media, and cyber crime.
>> This is my personal account. I am talking about things that are related to the work I do.
>> What I need to do is say that I work at Symantec, but these opinions are my own.
>> If you see something coming out for me that could in various my company, they did not say that, I did, I am not speaking for Symantec when I tweet here.
>> Is that is at -- if that is at -- if I'm going to tweet about things related to work I better make it clear to protect myself and the company that these things are my own .
>> Let's move on. What I would like to move onto is game shows.
>> Many of you are familiar with family feud.
>> I think it is still on the air.
>> I would like to play little family feud right now.
>> We surveyed 100 malware creators and asked them what Facebook users are desperate for.
>> I would like to explain that we did not really survey, but we did spend a lot of time looking at what they are doing, I will show you the top three social engineering tricks that they use to catch you specifically on Facebook.
>> Let's assume that you did not get any answers right, there are three things that they no Facebook users are desperate for.
>> They are desperate to watch own I got videos, to see who viewed their profile, and to have a dislike button.
>> How do bad guys use that?
>> There is something about the phrase or acronym all my God -- oh my God. For some reason it makes people click, they know it, they measure what works and what does not.
>> Here are examples of different videos that went through Facebook, if you clicked on them you are actually infecting yourself with malware.
>> My friends share videos but they never say oh my God, they say this is interesting or I enjoyed this.
>> If you got something like this, even from your friend, you should be very suspicious, that is why this stuff really works on social media because you feel you are surrounded by your friends, but they have tricked your friend into putting it on their wall, and you are more likely to click on this, even if your antenna goes up and something seems off.
>> The first thing is when you click on this they will download malware and post it on your wall so that everyone thinks you are saying that.
>> If you see that, prepare yourselves.
>> They often do this as well, before you download this video you need to upgrade the viewer, anything they can think of to trick you into thinking you need to upgrade it before you can use it.
>> Here is another trick, they might say before I show you this I need you to prove that you are human.
>> There is nothing to make them prove that they are human, but they want you to.
>> They want you to click on the red and blue, the first one will download malware,

the second click will post this on your wall so all your friends can see it.
>> How about viewing the profile.
>> Let's pretend it was me, I want to see who viewed my profile, I though this application and then it posts this on my wall.
>> The application does not work and it will not tell you who viewed your profile, it will infect you with malware, and now it sends  and sets a trap for all your friends.
>> You will see that there are a lot of zeros used for the letter a -- o, Facebook is looking for these sort of things, but they have different techniques to avoid detection.
>> They might not get you with malware, they might just get you to fill out a survey,  they say you will get a $200 giftcardd.
>> I will give them where I live, my first a last name, my text, my phone number, my date of birth. You ever get a text message and you wonder how they got your phone number?
>>  You may have fallen for one of these.
>> Someone stole your mobile number, you will never get the gift card, and you might give them a lot of information that you normally would not give to anyone. Be careful of those surveys.
>> Some people are so desperate for a dislike that in -- button that they will cut and paste pieces into their browser just to get the dislike button.
>> They probably do not know that they are infecting themselves, but they are JavaScript, they are cutting and pasting.
>> This is a lazy malware operator, he didn't code anything, he has you do all the work .
>> I want to finish this up I saying that all end-user education is the best practice.
>> This is why I do webinars like this and encourage people in positions to affect user education that they really need to do this.
>> Most threats or social engineering, it means we are fooling someone, we are not attacking the computer, we are attacking the person.
>> We need to educate ourselves and other people. We need to make it harder, it is too easy right now.
>> This reminds me of things that happened during World War II where they create posters to educate people of the dangers.
>> If I was doing it I would make a poster like this, someone tweeted, or this one that was in England I changed it to be thoughtful, wary, skeptical, especially on social networks. If you just do that and have good software then you will be skeptical and go along way towards protecting yourselves.
>> I'm going to turn this over to Kurt to give you some real world help on protecting yourself.
>> That may change the presenter and I will hand it over to you.
>> Thank you, that was helpful. We just want to remind everyone that we are taking questions at the end of the call. If you want to go ahead and start typing questions into the top box, go ahead and feel free to do so.
>> There is a lot of engaging content and we want to make sure we can get through as many questions as possible.
>> Thank you for completely scaring the audience, I think I have my work cut out for me now.
>> I'm going to try to talk them off the ledge.
>> I am down to only three followers on twitter, even my mother dropped me in the last 30 minutes.
>> Thank you very much for that.
>> I will be presenting what I see a GSA, how to reduce threats.
>> One thing I do want to say is that the idea is really to minimize the risk, we will not be able to a limiting -- eliminate.
>> I'm going to go over three cases, the one that Kevin talks about is public social media.
>> Things like Facebook, twitter, things like that.
>> I will also be talking about big government social media sites, the things that we put out for the public to use.
>> Finally GSA is using salesforce chatterer and we will talk about some challenges in those areas.

>> We will look in depth at a defense strategy that we will get into a little bit later.
>> The malicious links and malicious files we need to be careful about, we need a our users and things like our PII, things like vacation times, embarrassing photos or post, I have been trying to teach my teenage children about this.
>> They're posting pictures of people out into a military location.
>> There is also different plans for things like that.
>> Are best practice is threefold. You use computer security and network security. That is how we try to tackle and reduce the risk.
>> You need to be careful that you don't click on the unknown links or requests to download software. That is a huge one, especially the video file.
>> Be careful what you post, not only from the standpoint of hurting your agency, but even yourself.
>> This is another big one, I have learned this with my children, assume all of your information is public even if you think only your friends can see it.
>> Privacy settings can change mysteriously, this is a helpful hint, my wife friends our children and I do not, and we can see what the different postings are based on what goes out to the public. That is very important to see, it is amazing how basic security and privacy settings can change.
>> From the standpoint of the technical side, as much is you can educate and train things are getting more and more sophisticated each and every day. I have found that it is a lot easier to load malware  if you have admin rights.
>> I think it is very important for home as well.
>> They have regular and user accounts, I think that is a lot of now where -- malware  Job, Adobe flash, and Adobe reader are used for patching attacks, it is important to keep those updated.
>> Not using something old, that would be what your IT people would be using to secure your browser.
>> We are just starting this with Windows 7, we are using this to only allow certain types of programs to run.
>> It has been very helpful in all of this. Another thing that has been critical is -- [Indiscernable-low volume].
>> They're working with the motherboard and things that really help.
>> You can also post firewalls, that would be like your Symantec software.
>> As many of you know, those of you that no semantics, when a file comes down it will say hundreds of thousands of people have downloaded this, you were tricked into downloading a file, and you may not want to go any further.
>> From a network standpoint, this is where they come into play.
>> We work with navigate a and it shows connections to bad Internet addresses.
>> You can be able to look at that and have your network equipment monitor that.
>> Your main server entries and URLs, you can get a list of that ones, when you first click on that bad one your network software can block that.
>> The intrusion protection system and intrusion protection system you can look at that logs data and bad traffic.
>> You may not be able to stop that first person from going there and infecting themselves, but we can then look at that data input in blocks and in our case there are 20,000 other people going out there.
>> Application firewalls are very important, we is something called Palo Alto.
>> In the last year or so we have implemented security into an event management system, it correlates different events going on in the network and if people are tricked into downloading malware you can see that across the board to see if there is correlation .
>> Also working closely with US CERT, they gather threat data from all of the agencies to report into them.
>> From Emmanuel standpoint as well as technical, they get logs and things like that and they share that across the government.
>> The next area I would like to get into is on public sites.
>> Your site has been compromised with now where -- malware , this is the integrity of your own site, as Kevin indicated with things like the Secret Service or anything like that, people are putting up down files on your site and you are serving those out to the public at large. This is a huge reputation problem as well as inspecting the regular normal users.
>> They like to post malicious or derogatory post.

>> We also need to be careful about what we post up there.
>> Here are the best practices, one of the keys for preventing is to put software up on your file to monitor for bad uploaded files and it will do antivirus checking. You can put an application Web filter so that people that would normally put JavaScript things out will not be allowed to do that because you are protecting your site from bad uploads and former ability.
>> You can hard in your website in accordance with security.
>> You can also scan.
>> If you have a hard and website they will not be able to upload.
>> We also have 10 testers that think like hackers and they go to see how your site is honorable.
>> It is important from a government standpoint to keep your site secure.
>> In inappropriate posting, there are companies out there that will run scans of different types of posts and keywords and things like that.
>> If you feel it is a really important site and you don't want people up there loading anything, we have a website facilitator to review all the postings.
>> It slows down the communication, but in some cases it is really important.
>> You need to train employees on what can and cannot be posted. They need to understand what can be shared.
>> Finally there is a government intern all site.
>> They can share with to many people or the wrong people, or external people. You are creating some groups and the idea is to work in small teams to collaborate. It is not a public site, there might be some more data on it, because it is generally internal to your own security boundary.
>> This is really key for training, we have set up some policies and procedures for sharing information. The group owner is, they have some things they need to go through.
>> We need to request authentication and two factor authentication.
>> We monitor postings, it's a combination of manual and technical controls.
>> Though most of it is intern all, these are not publicly accessible sites, but we still need to be careful.
>> In Austin oh is key to train on what can and cannot be posted -- again it is important to train on what can and can not be posted.
>> That is really what we try to do to minimize the risk in the three prong defensive depth.
>> User training, network security, and putting those controls in helps to balance the risk and the return for increased collaboration among people from a work stand point.
>> Thank you, I will turn it over to the facilitators.
>> Inc. you, this was very informative, especially with Kevin starting off with what to look out for a new wrapping up. -- You wrapping up.
>> The first question that we have is with everyone using the URL shorthairs -- shortened hours -- shorteners have you seen it escalate with malware  being downloadeditt -- downloaded onto government computers because they think it is a trusted site like a.gov.
>> We have seen statistically more links are using shortened you are out -- URLs. They know they are effective so we are seeing more of that.
>> Overall every shortened URL does not leave to -- lead to malware  There is security cheat -- technology and things like that to check those links.
>> We are going to shake out. But this is a saw although -- solvable problem that we are working on.
>> The increased use of social media has gone along with increased use of the short URL.
>> I cannot say it's a cause a lot of facts because more people are using the site in general and over the last couple of years there really still has been a lot of use. I have not seen the huge jump just because of that.
>> I would really advise people to be careful when they see a shortened URL in an e-mail, it especially did something they do not know or someone they do not know, even if it is someone they do know, it is just another piece that should make you suspicious.
>> We will not get away from shortened ones, it is too useful, but again, if something seems wrong, although your suspicion -- follow your suspicion.
>> Speaking of e-mails, if they click on a shortened one, what exactly would happen?

Does it send mass e-mails to the people in their contacts or is there sensitive data going out if there is someone that has that computer harnesses the information? What happens to that?
>> The shortened URL could be used for phishing attack that would take you to a website that would be pretending to be a Facebook or your bank or some site that you would normally connect to in attempt to steal your login and password. It would pretend to be a site you know.
>> The shortened URL disguises the fact that it does not look like Facebook.com, it hides it in the e-mail hoping you will not catch it when you get to the site.
>> It might also take you to a website that would attempt to download malware onto your machine .
>> In those cases that is where your security software needs to come into play.
>> It will be watching for it if you were being sent to a site that is bad.
>> It is better not to click that seems suspicious then to get to that point.
>> Will we normally see is a fake URL but then when you put your cursor over in your browser you can see what the real URL is.
>> Then you go below it in you can see that it's not.
>> We see that before we see a shortened URL in an e-mail.
>> Thank you, if you had one point that you would reiterate to those agencies out there that are still leery of using social media, what would you tell them about this to let them know that it is okay to use it, but these are just a few things you need to look out for because of what we have been seeing a lot of our webinars is the agencies are interested, that things like this keep them from taking that next step and would be engaging.
>> I would have to go back to my presentation, user education is critical.
>> Really working with your IT and security people too hard in the end part, hard in the computers, hard in the mobile devices.
>> With those key pieces and doing a three leg and to all -- dual approach, you can balance the risk and rewards.
>> There is a risk that when you drive a car you can crash or run out of gas, most of us still choose to drive, clearly there a risk that the benefits far outweigh the risks if you are aware of them.
>> Thank you, I have a question coming about you are codes -- QR codes, it is difficult to know if they are legitimate, have you seen anything been downloaded using these codes?
>>  Yes, they are kind of like a shortened link for the bones -- phones, we have some software that will check that before it sends you there.
>> There has not been a lot of malware using it.
>> There is the potential there,  and someone probably will, particularly if you see a QR code printed in the newspaper or on a legitimate website, the risk is very small.
>> If it comes in some unusual plays, it is very difficult for bad guys to hijack the printer of the newspaper and put a bad code there.
>> I think it is a very small risk, there is a little risk their.
>> I would not let it stop me from using those codes though.
>> Thank you.
>> We are coming up to the end of the webinar, if anyone has -- if no one has any more questions or would like to take the time to think Kevin and Kurt for doing this webinar, it was awesome and informative, and funny, I was getting messages that you had people in stitches with some of your jokes, it was very need to get people that had us laughing on here.
>> I thank you for that.
>> I want to let everyone on the call know that we will send out a small survey to get your input and your opinion on today's webinar as well as what you would like to see in the future.
>> Also, if everyone or anyone is interested, we have a couple of great classes coming up, you can see those on how to.gov/training.
>> We will go beyond customer service and then we will have a webinar on public assessment tools.
>> Again I would like to thank you for today's webinar, I want to let everyone know that I want them to have a good day and go out and enjoy the weather and -- have a good holiday.
>> Thank you, goodbye.

>> [Event Concluded]