Internet Fraud Battlefield

Jeffrey Friedberg
Chief Privacy Architect
Microsoft Corporation

Introduction

Consumers embracing the online digital lifestyle are under attack. The "Bad Guys" are trying to steal their identities and hijack their systems. The potential harms are serious and range from bank fraud to cyber-terrorism.

The Bad Guys use a variety of methods. Typical ploys include sending spoofed email (Phishing) or downloading Spyware. But the stakes continue to go up. Pharming covertly redirects users to spoofed sites and puts the integrity of the Internet into question. Remotely controlled "Bot Nets" (large collections of compromised systems) give Bad Guys the power to take down a service or send spam under the radar. Rootkits can circumvent detection and execute with impunity.

In order to establish effective strategies and tactics to mitigate these problems it's critical to see the big picture. A high level map of the "battlefield" would:

- Help demystify what is happening
- Provide insight for setting strategy
- Help assess the efficacy of tactics
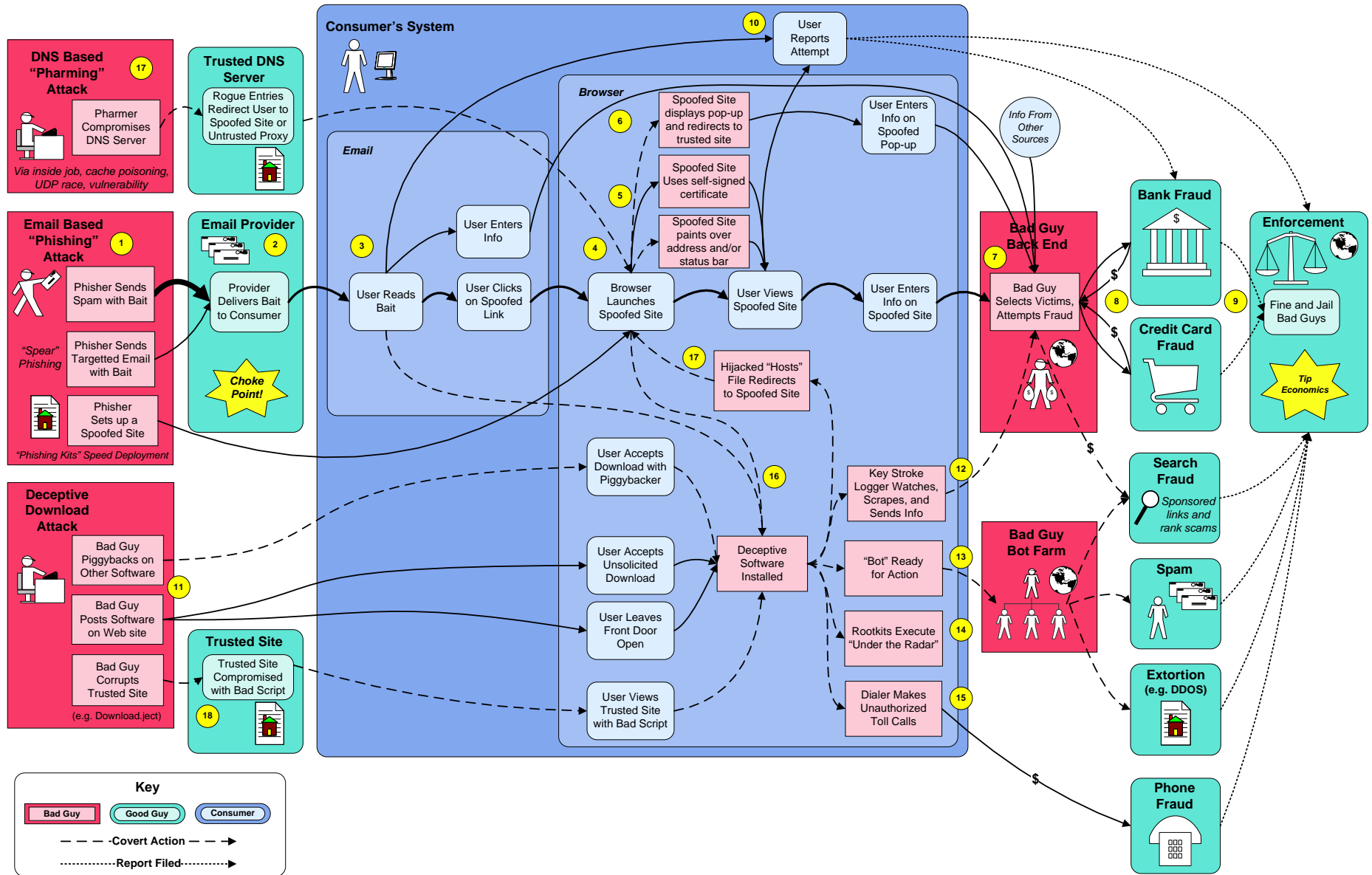- Provide a common reference

The Internet Fraud Battlefield diagram presented on the next page offers a high level end to end view of the problem space. It illustrates some of the ways users get tricked, how their systems get compromised, how the Bad Guys commit fraud, and where the Good Guys (e.g., email service providers, banks, merchants, and law enforcement) come into play. It also shows how "blended attacks" can occur.

Seeing multiple attack vectors at the same time helps identity opportunities for leverage. Addressing a big attack vector "upstream", like spam, could become an effective choke point for reducing threats throughout the ecosystem.

Creating mitigations can be costly. Before investing heavily in a tactic, it's important to assess its efficacy. The battlefield can help facilitate that analysis (e.g. what good is blocking one method of attack if the Bad Guys can just go around the mitigation).

Finally, there are many players that need to come together to address these problems (e.g. technologists, financial institutions, consumer groups, policy makers, and law enforcement). Having a common framework helps these parties discuss the problem, understand their role, discover meaningful mitigations, and work collaboratively to protect consumers.

Internet Fraud "Battlefield" – The Big Picture

Consumer's System

DNS Based "Pharming" Attack 17
Pharmer Compromises DNS Server
Via inside job, cache poisoning, UDP race, vulnerability

Trusted DNS Server
Rogue Entries Redirect User to Spoofed Site or Untrusted Proxy

10 User Reports Attempt

Spoofed Site displays pop-up and redirects to trusted site 6

User Enters Info on Spoofed Pop-up

Info From Other Sources

Email Based "Phishing" Attack 1
Phisher Sends Spam with Bait
"Spear" Phishing
Phisher Sends Targetted Email with Bait
Phisher Sets up a Spoofed Site
"Phishing Kits" Speed Deployment

Email Provider 2
Provider Delivers Bait to Consumer
Choke Point!

Email
3 User Reads Bait
User Enters Info
User Clicks on Spoofed Link

5 Spoofed Site Uses self-signed certificate
Spoofed Site paints over address and/or status bar

4 Browser Launches Spoofed Site
User Views Spoofed Site
User Enters Info on Spoofed Site

Browser

Bank Fraud

Bad Guy Back End 7
Bad Guy Selects Victims, Attempts Fraud
8 $
9 $

Credit Card Fraud

Enforcement
Fine and Jail Bad Guys
Tip Economics

17 Hijacked "Hosts" File Redirects to Spoofed Site

Deceptive Download Attack
Bad Guy Piggybacks on Other Software
11 Bad Guy Posts Software on Web site
Bad Guy Corrupts Trusted Site
(e.g. Download.ject)

User Accepts Download with Piggybacker

User Accepts Unsolicited Download

16 Deceptive Software Installed

12 Key Stroke Logger Watches, Scrapes, and Sends Info

Search Fraud
Sponsored links and rank scams

13 "Bot" Ready for Action

Bad Guy Bot Farm

Spam

User Leaves Front Door Open

14 Rootkits Execute "Under the Radar"

Trusted Site
Trusted Site Compromised with Bad Script 18

User Views Trusted Site with Bad Script

15 Dialer Makes Unauthorized Toll Calls

Extortion (e.g. DDOS)

$

Phone Fraud

Key
Bad Guy
Good Guy
Consumer
— — -Covert Action — — ▶
·········Report Filed··········▶

Battlefield_Overview.doc
2
© 2006 Microsoft Corporation

Understanding the Battlefield

The large blue box in the center of the battlefield represents the consumer's system. It is surrounded by both Good Guys (colored green) and Bad Guys (colored red).   When a Bad Guy compromises the consumer's system (e.g., with a key stroke logger), the corresponding box is colored red. Arrows that are dashed indicate an action was covert (i.e. not exposed to the consumer in the User Interface). Numbers in the small yellow circles correspond to the notes below.

Phishing for Personal Information (centerline through the picture)

1) The "phisher" creates an email with some bait and sets up a spoofed web site. To speed deployment, they can start from a "Phishing Kit" that has the code and artwork needed to launch an attack against well known targets like Ebay or Citigroup. The phisher gives the email to a spammer for distribution. The spammer distributes the email, sometimes via a "Bot Net" (i.e. systems covertly taken over).   Better results are possible with "Spear Phishing" where bad guys target a specific victim (by name) or a group (e.g., employees that have just completed open enrollment for a 401K).

2) The Email Provider receives email with the bait and forwards it to the user. This is an opportunity for a "choke point" (e.g. Microsoft Smart Screen blocks 3 billion messages per day). Even with aggressive filtering, some email with the bait still gets through.

3) The user reads the email that contains a spoofed link (i.e. the text of the link looks OK but it's really to a spoofed site). The user is tricked and clicks on the spoofed link and launches the browser. Note launching a web site to collect the user's personal information is not necessary. The Bad Guy could have simply asked the victim to reply to the email with the information or they could have asked them in the email to fill out an HTML form that was embedded in the message. Some users are overly trusting and will comply (not unlike victims of telephone scams).

4) The browser displays the spoofed site. The spoofed site asks the user for personal information. The user is tricked and enters their personal information.

5) Embellishments can make the spoofed web site more convincing. Bad Guys were previously able to display a phony lock symbol or draw over the spoofed address with the expected address (known visual exploits like these have been fixed in IE). Unfortunately, seeing a real lock symbol is still not sufficient for trust; a bad guy can setup an interloping proxy or use a self-signed certificate to cause the symbol to be displayed. Also, the bar to get a certificate is inconsistent and in some cases too low (e.g., a mail room clerk could request a certificate and spoof the company's web site).

6) Another clever trick is to use a phony pop-up rather than a spoofed web site. When the user first clicks on the spoofed link, the user is presented with the spoofed pop-up that requests their personal information. The Bad Guy then immediately redirects the browser to the trusted site.   The user sees the spoofed pop-up over the trusted site, assumes it's real (since they see a valid lock symbol and address on the trusted site), and they enter their personal information in the pop-up (see Figure 1). By design, pop-ups do not need to show a lock symbol or address bar which could help users spot this scam (this is a compelling reason to never enter such data in a pop-up and to use a pop-up blocker).
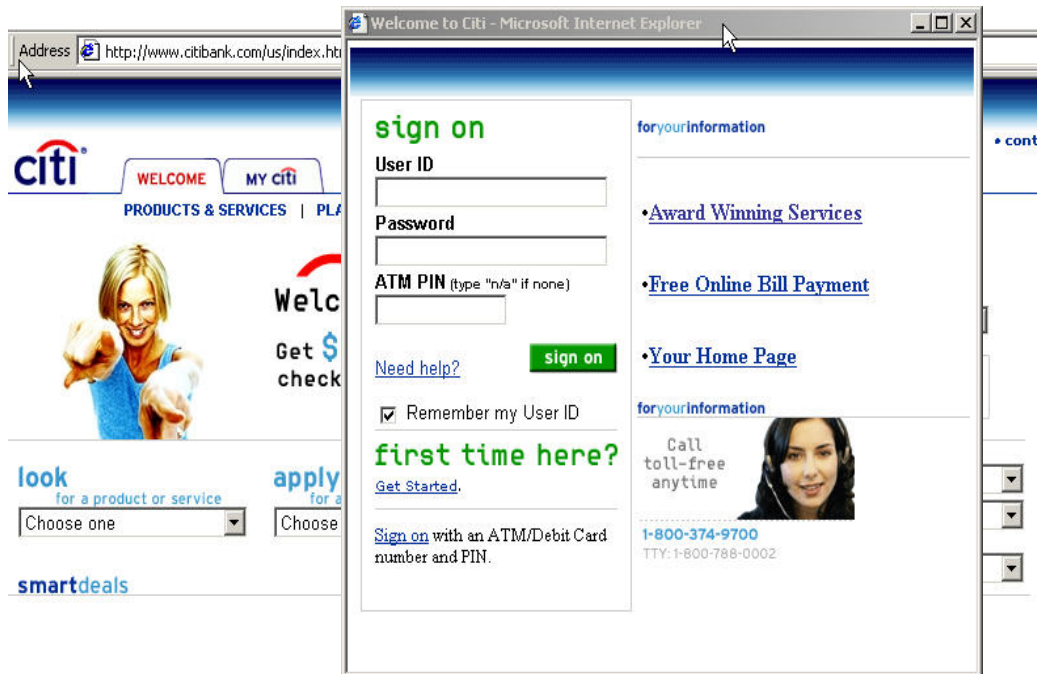
Figure 1: Spoofed pop-up with phony login visually on top of a real site.

7) The Bad guy captures personal information from user. They will often combine it with data from other sources (e.g., public sources like genealogy sites, court records, or information stolen from private sources like data custodians). The Bad Guy mines data looking for "good" victims. They consider factors like financial institution, credit score, and when the next account statement will be delivered (to maximize time before detection). The Bad Guy gets everything ready and attempts fraud.

8) Where account to account transfers are common (e.g. Australia), the Bad Guy transfers funds (just under the reporting limit) from the user's account to a phony account. The Bad Guy then sends in "mules" to withdraw the cash. For new account fraud, the Bad Guy establishes credit in the user's name, draws from the line, and defaults.

9) Effective law enforcement is an opportunity to "tip the economics" through big fines and jail time (i.e. create a deterrent). Financial institutions report fraud to Law Enforcement. Law Enforcement utilizes traditional tactics (e.g. follow-the-money and stings). This is a world-wide issue and requires world-wide cooperation. The Bad Guys will often use a "spread the pain" strategy to avoid law enforcement action (i.e. they distribute hits across jurisdictions and keep hits small). Need to aggregate crimes to make it harder to hide.

10) Through consumer education, users may spot spoofs and report them. Key points for detecting a spoof are reading email and browsing. Reports can help tune filters and give Law Enforcement new leads.

Deceptive downloads: getting more than you bargained for

11) One way unwanted software gets on your system is through covert piggy backing. The rogue software is included with software you want, like a P2P file sharing program, but it's not obvious. Another is posting software on a page and triggering a forced download (blocked by XP SP2). Some users leave their security settings below medium (the default) which allows "drive by" downloads.

12) Deceptive downloads can include key stroke loggers that send your key strokes to the Bad Guys for analysis. They may include "screen scrapers" which send images of your desktop. This software can directly compromise your personal information and expose you to bank fraud, credit card fraud, and identity theft.

13) Deceptive downloads could turn your system into a "zombie" where the Bad Guy is able to remotely control your system resources. You become part of a Bot Farm for hire. When not looking for new recruits, Bot Farms can send Spam and launch Distributed Denial of Service attacks (DDOS). Spam perpetuates Phishing attacks. Threat of DDOS has been used to extort money from commercial sites. The Bad Guys also try to get search engines to promote their spoofed links by paying for sponsored links or using the Bot Nets to cheat the rank algorithm.

14) The most insidious form of deceptive software is a "rootkit" which installs at or below the level of the operating system to avoid detection.

15) "Dialers" make authorized toll calls resulting in phone fraud. Ireland took extreme step of blocking direct dialed international calls (Sept 2004).

16) The Bad guys also exploit "unpatched vulnerabilities" in the email and browser client to inject rogue software.   Like Phishing, Bad Guys will impersonate a trusted sender to get you to open compromised emails (i.e. one that will try to install malicious software on your system). Microsoft addresses vulnerabilities in two ways: reactive (e.g. quick fixes) and proactive (e.g. hardening as part of Secure Development Lifecycle and Engineering Excellence). Users should upgrade to the latest version of the software (e.g., XP SP2 which includes many security improvements) and regularly apply updates (e.g. via Automatic updates). Deploying the latest software can reduce your exposure (e.g., XP SP2 desktops and Windows Server 2003 SP1 makes you 13 to 15 times less likely to get infected by malware).

17) Pharming compromises DNS servers which redirect a user to the Bad Guy site even when the user enters or clicks on a trusted link. Rogue software can edit a local "hosts file" to effect the same action.

Blended threats: mix and match

18) Combinations of attacks are becoming more common. One example in 2005 was the Download.ject attack. A trusted site with weak settings was compromised with an evil script. When users visited the trusted site, the evil script executed, and through an unpatched vulnerability a key stroke logger was injected into their system.

Assessing Tactics

Seeing current and proposed tactics overlaid on the battlefield can help identify strategic holes. The battlefield diagram on the next page illustrates this concept. Tactics are represented by yellow stop signs and are placed over the area they target.

The tactics displayed include these deployed by Microsoft:

- Windows XP SP2 mitigations such as a new download blocker and IE policies for drawing and security.
- Microsoft SmartScreen™ Spam Filter.
- Aggressive shutdown of spoofed sites (in FY05 Microsoft successfully closed over 2300 sites, 90% of them under 24 hours).
- Proactive detection that scours the web looking for unauthorized collateral.
- Domain defense that reduces the risk from look-alike sites.
- Special cleaners like the Malicious Software Removal Tool.
- Fixes for known vulnerabilities
- Reward fund to help find the Bad Guys
- Microsoft AntiSpyware (Beta).
- Microsoft Phishing Filter (Beta) that uses intelligent heuristics and an online web service to flag suspected/reported sites.
- Least privilege by default to reduce risk of compromise (Beta)
- InfoCard identity system that is easy to use, reduces the need for passwords, and helps users know who they are dealing with (Beta)
- Full volume encryption to reduce chance of a breach from a lost laptop (Beta)

And these other tactics deployed by a variety of vendors:

- Online consumer education from a variety of sources including the FTC, SEC, Treasury, banks, credit card companies, consumer advocacy groups, and software vendors.
- Email authentication such as Sender ID and DomainKeys.
- Safe/block lists, visual indicators such as AccountGuard (eBay), ScamBlocker (Earthlink), and SpoofStick (CoreStreet)
- One time passwords like SecurID token (RSA) and Scratch-off PIN cards
- Better tools to detect deceptive software
- Follow-the-money enforcement and joint sting operations like Digital Phishnet.

Sampling of Current and Proposed Tactics

DNS Based "Pharming" Attack
Pharmer Compromises DNS Server

Via inside job, cache poisoning, UDP race, vulnerability

Trusted DNS Server
Rogue Entries Redirect User to Spoofed Site or Untrusted Proxy

DNS SEC

Email Based "Phishing" Attack
Phisher Sends Spam with Bait

"Spear" Phishing
Phisher Sends Targeted Email with Bait

Phisher Sets up a Spoofed Site

"Phishing Kits" Speed Deployment

Legal Spam Deterrents

Email Provider
Provider Delivers Bait to Consumer

Choke Point!

Smart Screen*
Reduce Zombie
Sender ID*
URL Filtering
Comp. Challenges
Proactive Detection*
Domain Defense*

Consumer's System

Email
Client side block?
No HTML?
Consumer Education #1
User Enters Info
User Reads Bait
User Clicks on Spoofed Link
Harden OE/ Outlook*

Browser
Block unregistered domains?
New IE Drawing Policy*
Browser Launches Spoofed Site

Spoofed Site displays pop-up and redirects to trusted site
Spoofed Site Uses self-signed certificate
Spoofed Site paints over address and/or status bar

User Enters Info on Spoofed Pop-up
"Is this for real?" Button

Consumer Education #2
Indicator using URL Safe/Block List
Indicator using URL Heuristics
Info Card
Indicator based on Cert Level?

User Views Spoofed Site
User Enters Info on Spoofed Site

Consumer Education #3
Reporting Integrated in email
User Reports Attempt
Integrated in browser
Clearing- House**

User Accepts Download with Piggybacker
Reputation Service**
Hijacked "Hosts" File Redirects to Spoofed Site
Harden IE*

XPSP2 Download / Pop-up Blockers*
XPSP2 Warning Redesign*
Watch attachment points like BHO**

User Accepts Unsolicited Download
XPSP2 No Looping
Deceptive Software Installed
"Bot" Ready for Action

User Leaves Front Door Open
XPSP2 "Medium+" Security Policy*
Harden IE*
Rootkits Execute "Under the Radar"

User Views Trusted Site with Bad Script
Dialer Makes Unauthorized Toll Calls

Key Stroke Logger Watches, Scrapes, and Sends Info
Watch and Block traffic?
Special "Cleaners"**
Reduce Zombie

Deceptive Download Attack
Bad Guy Piggybacks on Other Software

Bad Guy Posts Software on Web site

Bad Guy Corrupts Trusted Site

(e.g. Download.ject)

Trusted Site
Trusted Site Compromised with Bad Script

Harden IIS

Info From Other Sources
Data Goverance
Full Volume Encryption

Bad Guy Back End
Bad Guy Selects Victims, Attempts Fraud

Bad Guy Bot Farm

Bank Fraud
One Time Passwords
Password Hashing
Two Factor
Info Card

Credit Card Fraud

Search Fraud
Sponsored links and rank scams

Spam

Extortion (e.g. DDOS)

Phone Fraud

Enforcement
Aggregate Crimes
Reward Fund
Sting Operations
Fine and Jail Bad Guys
Follow the Money*

Tip Economics

Key
Bad Guy
Good Guy
Consumer
– – – Covert Action – – –▶
······· Report Filed ·······▶

Consumer Education*

#1: Email Exploits
Don't enter info
Don't click on links
Validate sender

#2: Browser Exploits
Verify URL
Click on Lock
Watch for visual spoof

#3: Reporting
FBI, FTC Site
Spoofed company

*Tactic implemented by Microsoft
**Implemented in Microsoft AntiSpyware

What's Missing?

While the battlefield depicts many of the methods deployed by the Bad Guys, other technologies, like Instant Messaging, Mobile devices, and Internet Telephony, have the potential to be exploited and are not currently mapped.

Data custodians are also under attack both from inside jobs and external campaigns. By design, this battlefield takes a consumer-centric view. A data custodian centric battlefield could be created that illustrates these attacks, as well as potential mitigations (e.g. comprehensive data governance solutions that would reduce the likelihood of a breach).

Conclusion

It's clear from the diagram that there is no silver bullet that will address all issues. The threats are continuously evolving and blended together by the Bad Guys to form new attacks.

That said, if we look more closely at just a subset of the problem we might be able to identify the root cause and make a major impact. In the case of Phishing, lack of strong mutual authentication and the use of shared secrets may be the primary reasons Bad Guys continue to utilize the technique. They can pretend to be your bank or a trusted entity you do business with and unless you're an expert, it's very hard for you to tell the site isn't real. You type in your secrets (your credentials) and the Bad Guys later play them back to the entity and pretend to be you. Adding a "second factor" like a one time password will not help you recognize the site is spoofed and it can still be replayed by the Bad Guy via a classic man-in-the-middle attack.

These issues call for a strategy which makes it easier for users to assess whether they are on the correct site (i.e. stronger mutual authentication) and moves away from using shared secrets to authenticate (e.g. username and password). Using Public Key Cryptography, where the "private key" stays private and only the "public key" is exchanged over the Internet, is one way to take away the prize sought by the Phisher.

Launching a new infrastructure is a large undertaking that will take many players. There will be some costs and it will take time. New technologies will need to be rolled out, incentives and appropriate regulations will need to be identified, and consumers will need to be educated on the new paradigm. To be effective, solutions like these need to become an integral part of our online digital lifestyle and a catalyst for the ecosystem.