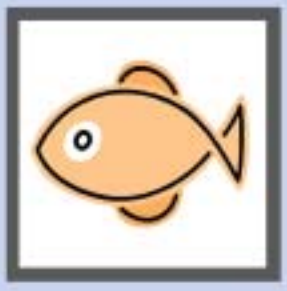
A Call for Action

Report from the National Consumers League Anti-Phishing Retreat

A Publication of the National Consumers League
March 2006



A Call for Action

Report from the National Consumers League Anti-Phishing Retreat

National Consumers League

Washington, DC

March 2006

Contents

Introduction and Executive Summary

This report is a call for action against phishing. For purposes of this report, phishing is defined as using the Internet to fraudulently gather personal data about a consumer. Phishing is also perpetrated by telephone, and some of the recommendations in this report, such as the need for greater consumer education, can be applied to that scenario. However, the focus of this report is how to help stop phishing in the online context. Phishers use the personal information they steal from consumers for gain, such as by hijacking — taking money from — a customer account, and to commit identity theft.

Origins of the Report

The Anti-Phishing Retreat: A major theme of this report is the need for the various "good guys" to work together in the fight against phishing. The report emerges from a unique and fruitful collaboration of the National Consumers League with major sponsors American Express, First Data, and Microsoft, as well as numerous stakeholders in the fight against online fraud against consumers. The National Consumers League convened a 40-person retreat from September 28-30, 2005 at the Harbourtowne Conference Center in St. Michael's, Maryland. Participants are listed in Appendix 2. While a few agencies and organizations could not be included in the list because of legal constraints, all participants were fully engaged in the process and contributed to the outcome. Listing here is not an endorsement by each person or their organization of the specific content of the report.

Participants: The retreat brought together experienced persons from many perspectives relevant to the fight against phishing. Participants included persons from: consumer groups; academia; financial services firms; Internet service providers (ISPs); online retailers; computer security firms; software companies; consumer protection agencies; law enforcement agencies; and existing coalitions such as the Anti-Phishing Working Group, the National Crime Prevention Council, and the National Cyber Security Alliance.

Format of the Retreat and Goals: The retreat was professionally facilitated under the leadership of Dr. Phyllis P. McDonald, Director of Research for the Division of Public Safety Leadership at Johns Hopkins University, with assistance from consultants John Dentico and Joanne DeSimone. It began with a debate which contributed some important ideas and provided context for the discussions to follow. After presentations about how phishing works, how to think strategically about threats, what challenges phishing presents to different sectors, and how other challenges have been creatively addressed, participants were split into working groups. They met intensively to discuss the problem

and generate recommendations for action. The groups then came together to share and discuss recommendations. The goal was to produce solutions that are workable on a technical, economic, and legal basis. The reporter for this project has been Professor Peter P. Swire of the Ohio State University.

Outline of the Report

Understanding the Phishing Problem

Part I: The Internet Fraud Battlefield

Part I looks at phishing by examining **The Internet Fraud Battlefield**. A white paper and diagram of the Internet fraud battlefield, attached as Appendix 4, helps the reader understand the different methods of attack that have developed.

Part II: The Large and Growing Problem of Phishing

Part II documents **The Large and Growing Problem of Phishing**. In addition to direct losses due to fraud, the much larger costs are loss of consumer confidence in the Internet. Recent surveys show that some consumers have already cut back their use of the Internet due to worries about fraud. More generally, there is fear that the growth of the online sector, and thus of the U.S. economy, will slow unless online activities become safer and are seen as safer by consumers.

Part III: The Lifecycle of the Phisher

In order to develop anti-phishing strategies, Part III looks at **The Lifecycle of the Phisher**. For the fraud to be effective, the criminals must go through six phases: plan; launch attack; gather personal data; research how to use data; attempt crime; and launder the proceeds. Analysis of this lifecycle gives the defenders — the various stakeholders fighting fraud — ideas of how to interrupt the criminal enterprise.

Part IV: Recommendations for Action

The report offers **seven principal recommendations for action**. The first four recommendations are to **support key, known responses**. The next three are to **develop promising new approaches** that were generated during the retreat. Some of these recommendations are already being implemented in some settings. In summary, the recommendations are as follows:

1. ***Support greater consumer education.*** There was widespread agreement among retreat participants of the need for greatly enhanced consumer education and awareness about phishing and for a clear and consistent message. Resources will be needed to fund traditional public-service announcements as well as PSAs on the Internet and new tutorials that teach consumers "in context," as users do potentially risky activities on their home computers. There may be other points where educational information could be provided, such as when someone buys a computer or enrolls with an Internet service provider, at which educational information about phishing could be provided.

2. ***The consumer experience must be "secure by design."*** A major way to combat phishing is to create an ecosystem that is "secure by design." This means that, wherever possible, strong security should be the default setting. Consumers should not have to become professional programmers simply to use their home computers. In the face of new attacks by the fraudsters, it is especially important for security measures to be updated regularly.

3. ***There must be better user and site authentication.*** Phishers fake being the consumer when they hijack an account and fake being a trusted organization when they send the phishing email or create a spoof Web site. The answer for fake identity is better authentication, which means better ways to establish someone's true identity. Most retreat participants believe that users will increasingly need to identify themselves with something stronger than name and password. In the fight against phishing, it is perhaps even more important to develop new ways to authenticate Web sites, so that ordinary users can tell a real site from a fake. The report suggests way to improve both user and site authentication, or what is sometimes called "strong mutual authentication."

4. ***There must be better tools for effective investigation and enforcement.*** Investigators in law enforcement agencies and the private sector often lag behind cyber criminals in terms of their understanding of technology and the equipment at their disposal. In order to take advantage of strategic opportunities to disrupt phishing and bring enforcement action against those involved, government and the private sector must commit more resources for personnel, training, and equipment. Better information sharing and cooperation between law enforcement agencies in the U.S. and abroad, and between law enforcement agencies and the private sector, is also essential in the fight against phishing.

5. ***Learn from the lifecycle of the phisher.*** Analysis of the lifecycle of the phisher highlights the moments that are riskiest from the perspective of the phishers themselves. Sting operations and other investigative and enforcement measures can disrupt the early stages of an attack. Supplying false information to phishers, such as fake Social Security numbers, can create an evidence trail back to criminals who attempt to use the false information. In addition, anti-phishing efforts can learn from the "follow the money" experience that the anti-money laundering community has created for other crimes.

6. ***ISPs and domain name owners can cooperate on white lists***. One idea generated at the retreat would have Internet service providers cooperate more closely with the major organizations whose names are most often used in phishing attacks. The major organizations could provide ISPs with a "white list" of the organization's legitimate sites, updated regularly. The ISPs can then establish a method so that spoofs of that organization are flagged for special action. Creation of this white list may be surprisingly easy for the many organizations that already keep track of their legitimate sites in the course of policing their corporate trademarks.

7. ***Use black lists to create a "phishing recall" approach.*** One interesting statistic raised at the retreat is that the average email is not opened until about 12 hours after the ISP first makes the e-mail available to the consumer. This 12-hour latency provides a window of time for an updated black list to be distributed. The email could then be flagged for special action as a potential phishing email. Perhaps the email could even be "recalled" — filtered out — so that the consumer never sees the phishing email or sees it only in a quarantined way. This new approach would take advantage of the fact that it is much easier to detect a phishing site after the bait is sent than before.

Summary

In summary, intensive discussions at the retreat support a call to action against phishing. There are key measures that are already known but which deserve renewed support, such as consumer education, "secure by design," improved authentication, and better tools for investigation and law enforcement. There are also promising new approaches. The lifecycle of the phisher offers as-yet-untapped opportunities to disrupt criminal activity. New collaboration on white list and black list approaches also would likely achieve more than any one type of stakeholder could achieve on its own.

Retreat participants agreed that it is imperative to work together in a systematic approach to the phishing problem. The recommendations in this report form a comprehensive action plan for combating phishing more effectively. Some of the strategies recommended in this report, such as improving authentication and building security into design, have already been embraced by many. The goal of this report is to encourage wide adoption of these anti-phishing strategies.

Understanding the Phishing Problem
Part One: The Internet Fraud Battlefield

An initial task is to understand the various kinds of phishing attacks. Retreat participants used the diagram of the Internet Fraud Battlefield,[1] shown in Appendix 4, to envision the main sorts of attacks and potential defenses. In the diagram, the consumer is squarely in the middle, in the blue box. Attacks start in the red boxes on the left, and move through email providers and other "good guys" on the way to consumers. When the attack succeeds against the consumer, then there are red boxes on the right side that show how the criminals try to reap the benefits. At the far right of the diagram is enforcement against the criminals once they are caught.

The classic phishing attack. In the diagram, the classic phishing attack goes from left to right beginning with "phisher sends spam with bait." Most often, the bait is an email claiming to be from a trusted organization, such as a bank or an online retailer. The email often claims that the consumer must urgently take action, or else a bad thing will occur such as closure of the account. A collection of bait emails has been posted by the Anti-Phishing Working Group, at *http://www.antiphishing.org/phishing_archive.html*.

In the diagram, once the "phisher sends spam with bait" the next step is that the email "provider delivers bait to consumer." Next, the "user reads bait." A user might respond directly to the email, shown as "user enters info." More often, the "user clicks on spoofed link."

The link is typically to a Web site controlled by the phisher. The Web site is designed to seem like the site of the trusted company. The consumer then enters personal information, such as account number, password, or Social Security number. When the "user enters info on spoofed site" the phishing attack has succeeded at its first goal, to gather personal information fraudulently. Next the personal information is used to harm the consumer, when the "bad guy selects victims and attempts fraud." Important examples of fraud are if the phisher commits bank fraud, such as by hijacking the consumer's account, or credit card fraud, by using the personal information to purchase goods fraudulently. Finally, if investigative and enforcement efforts are successful, the result is to "fine and jail bad guys."

In short, the classic phishing attack urges the consumer to provide personal information in response to the bait email. Once the personal information is harvested, then the phishers seek to profit from it.

Usually the phisher sends out millions of emails, most of which end up in the inboxes of people who do not have a relationship with the entity that is being spoofed, and so are unlikely to take the bait. However, in a new approach called spear-phishing, the phisher seeks to improve the odds of success by targeting a relatively small group, and often by leveraging institutional affinities. For example, the phisher may comb the public Web site of a university or government agency for the names and email addresses of employees, then send those individuals emails that purport to be from the credit union which serves them. This target-marketing is evidence that phishers are becoming more sophisticated and efficient in their operations.

Pharming and deceptive downloads. On the far left of the diagram, the top box is for a DNS Based "Pharming" Attack. In plain language, that refers to attacks on the domain name system, such as if a consumer typed in a legitimate site such as *www.whitehouse.gov* and got diverted to a spoofed site without realizing it. In this kind of attack, the problem is that the routing system of the Internet is compromised. The main defense is to harden the domain name system against attack.[2]

The bottom box on the far left of the diagram is for a Deceptive Download Attack. In this type of attack, the problem is that the consumer's computer is infected with spyware or other deceptive software. This software can get onto the user's computer in a number of ways. For instance, it might be "piggybacked" onto legitimate software, the user might accept it not knowing what it does, or the user might use low security settings that accept it.

When this software seizes consumer information, it is part of the larger identity theft and fraud problem. "Keystroke loggers" record actions typed into the consumer's keyboard. "Screen scrapers" are able to capture images of what the user sees, giving the criminals access to the information on the screen. When keystroke loggers or screen scrapers are on a consumer's machine, then there is usually additional software to "phone home" to the criminals, so that they can receive what the spyware has learned.

Another way that consumers are tricked is when software covertly directs them to spoof Web sites operated by the criminals. This kind of hijacking is similar to pharming. The user types in a legitimate Web address, but gets sent to a spoof site that fraudulently gathers data.

Other threats. Other kinds of deceptive download attacks can pose serious threats to individual consumers or to the security of the Internet more generally. The diagram, for instance, shows how home computers can get turned into "bots" that can launch attacks to other computers.

Experts at the retreat also warned of phishing virus "applications" that were capable of automated learning, sensing when and where they were being detected, then adapting to evade removal and continue to operate. As phishing evolves, it is necessary to anticipate new threats and how to counter them.

At each step, various counter-measures could reduce the likelihood of the consumer being harmed by the phishing attack. Before examining the counter-measures, this report will first look at the rise of phishing as a threat to consumers.

Notes to this section

1 The Internet Battlefield was created by Jeffrey Friedberg at Microsoft.

2 For an excellent discussion of pharming, see Ollman [2005].

Understanding the Phishing Problem

Part Two: The Large and Growing Problem of Phishing

The Anti-Phishing Working Group (APWG), an industry association focused on eliminating the identity theft and fraud that result from phishing and email spoofing, reports that the term "phishing" comes from the analogy that Internet scammers are using email lures to "fish" for passwords and financial data from the sea of Internet users.[1] The term was used by the mid 1990's to describe tricking Internet users to reveal their passwords for dial-up service.

Beginning in 2003, the number and variety of phishing attacks climbed sharply. Although reporting methodology has shifted somewhat over time, regular reports from the APWG give a clear picture of the rise in attacks:

- The APWG defines a unique phishing attack by the base URL of the phishing Web site. The number of unique phishing attacks in January 2004 was 176. By October 2004, that climbed to 1,142. By October 2005, that number was up to 4,367.

- The APWG defines a unique phishing report as a unique email sent to multiple users, directing them to a specific phishing Web site. The count for October 2004 was 6,957. A year later, the number of unique phishing reports was up to 15,820.

- There were only 28 brands attacked in November 2003. The count was 44 brands in October 2004. In October 2005, 96 brands were attacked.

- The APWG reported in October 2005 that the average time online for a spoof site was 5.5 days. This short time suggests the challenge in identifying and responding to spoof sites before the phishers remove them from the Web. [2]

A May 2005 consumer survey by First Data confirmed the widespread nature of the problem. It found that 43 percent of respondents had received a phishing contact, and of those, 5 percent (approximately 4.5 million people) provided the requested personal information. Nearly half of the phishing victims, 45 percent, reported that their information was used to make an unauthorized transaction, open an account, or commit another type of identity theft. [3]

Behind these raw numbers, the consumer experience of the Internet is being profoundly affected by phishing, identity theft, and other types of fraud. The Ponemon Institute

conducted a survey in the summer of 2004, at a time when phishing attacks were running at less than half the rate of October 2005. This survey had the following major findings:

- Most people are vulnerable to spoofing. Over 60 percent of online users had inadvertently visited a fake or spoofed site.

- Many people are tricked into providing sensitive personal information such as checking account information or Social Security numbers. Over 15 percent of respondents admitted to having provided personal data to a spoofed site.

- Most people expect organizations to do a better job in addressing phishing problems. A full 96 percent agreed with the statement that "the organization should install technology that allows customers to know the differences between authentic emails and Web sites from fake emails and spoofed Web sites."

- Economic loss from spoofing had touched only about 2 percent of respondents, with an average reported cost of $115. Extrapolated to the full U.S. population, the result would be direct monetary loss from phishing fraud of approximately $480 million.[4]

A *Consumer Reports* survey conducted in late 2005 found signs of decline in trust in the Internet compared to its 2002 survey. It summarized its findings as follows:

- Nine out of 10 U.S. Internet users over 18 have made changes to their behavior due to fear of identity theft.

- Of those changes, 30 percent say they have reduced their overall use of the Internet.

- 25 percent say they stopped buying things online.

- Among those who shop online, 29 percent say they have cut back on how often they buy things.[5]

One additional survey from the fall of 2005, by Entrust, shows the upside that would come with an increase in trust. That survey found:

- Of users who connect to the Internet but do not currently use online banking, 72 percent would likely do to so if online identity security was improved.

- Of users who do currently bank online, 90 percent would take advantage of additional, higher value services if their online identities were better protected.

- The security of online identities would influence 65 percent of users when selecting

which bank to do business with. In fact 22 percent indicated that they would be very likely to switch banks to obtain better protection of their online identity.[6]

The Ponemon and *Consumer Reports* findings are based on survey results, and not on measures of actual participation in ecommerce. They nonetheless give evidence of lack of trust — many people are being targeted by phishers, the number of persons being victimized is growing rapidly, and many consumers report they are reducing their participation in online commerce because of fear of identity theft. The Entrust survey, by contrast, shows the gains to organizations that provide trusted transactions to consumers. Taken together, these surveys indicate that the direct financial losses due to fraud are only a small fraction of what is at stake in the fight against phishing. The much greater effect from phishing and other fraudulent activity is a reduction in trust in the Internet. Trust in major brands is eroded as brand names are used in phishing schemes. Many positive transactions, and much economic growth, will be lost if trust is not restored and maintained.

Notes to this section

1 *Http://www.antiphishing.org/word_phish.html*

2 *Http://www.antiphishing.org/resources.html#consumer.*

3 *Http://news.firstdata.com/media/ReleaseDetail.cfm?ReleaseID=163659.*

4 Ponemon [2004].

5 *Consumer Reports WebWatch* [2005].

6 Entrust [2005].

Understanding the Phishing Problem

Part Three: The Lifecycle of a Phisher

In creating tactics to fight phishing, one logical strategy is to study the "lifecycle of a phisher"[1] — the steps the criminal takes to profit from the fraud. By looking at phishing from the criminal perspective, it is easier to notice the moments where the criminal is most at risk. Those moments of maximum risk for the criminal are moments of maximum opportunity for the rest of us. Strategies can be designed to attack the criminal activity at those moments, and a number of those strategies are discussed in the "what to do next" section of this report.

Here are the key stages in the lifecycle of a phisher:[2]

1. Plan Attack

The criminal perspective. The first stage for the criminal is to plan an attack. Criminals often must collaborate with other bad guys, to learn how to operate and to carry out the attack. Criminals need to identify and recruit accomplices. They will identify potential marks and decide what data to gather from what sources. They will decide on the method of attack, which will often be some combination of email phishing, pharming, deceptive downloads, and other available techniques. An entire phishing subculture has arisen, with Web sites offering phishing kits that include samples of messages, instructions for building links, and other assistance in preparing and carrying out attacks.

Counter-measures. A major moment of risk for criminals is when they are collaborating with other persons and recruiting accomplices. Potential phishers have to be public enough to find co-conspirators. This offers an opening for undercover agents, monitoring of Internet forums, and sting operations.

Two factors increase the risk for the criminals. First, "there is no honor among thieves." If one person in a criminal operation is caught, then law enforcement can hope to "turn" that person and catch other perpetrators. Second, hackers and other Internet criminals are prone to bragging about their exploits. What the criminal calls bragging, a prosecutor calls "confession of criminal conduct."

The "what to do next" section discusses counter-measures in greater detail, including more active measures to interrupt the planning of phishing attacks. For now, an important point is that interrupting the criminal activity early in the lifecycle is very desirable, because all the later stages are stopped as well.

2. Launch Attack

The criminal perspective. The next step for the criminal is to send out the bait for a phishing attack or find some other way to attack the consumer. The best-known phishing attack is an email that asks the consumer for personal information. Other attacks are shown in the Internet Fraud Battlefield, in Appendix 4. These include deceptive downloads onto user computers, pharming attacks, and recruiting insiders who can help in harvesting personal information.

Counter-measures. The best defense depends on which method of attack the criminal chooses. One general strategy is to trace criminals when they attack. For instance, locating the Internet service provider that sent a phishing email can lead to identification of the attacker, or at least blocking use of that ISP for attacks in the future. Another general strategy is to filter communications for signs of phishing (*e.g.*, filter out false emails concerning leading banks) or malicious code (use anti-virus software and other tools). The Internet Fraud Battlefield shows possible counter-measures in greater detail.

3. Gather Data

The criminal perspective. The definition of phishing used in this report is use of the Internet to fraudulently gather personal data about a consumer. Once the attack is launched, the criminal needs a way to actually harvest that personal data. Major ways to harvest include: user entry of data, such as on a spoofed Web site or in an email; and software capture of data, such as by logging the consumer keystrokes, scraping data from the user's screen, or sniffing traffic in the network.

Counter-measures. The major risk to the criminal is that defenders can "follow the data." If the data can be accurately routed back to the criminals, then there may be a chance to trace that route. Rapid tracing of the route is essential, because criminals don't tend to hang around a long time in one place. One counter-measure, discussed below, is to send deliberately false personal information to criminal phishing sites. In that way, later use of that false information is linked to the phishing site.

A next-best approach is to block the sending of the data. Software tools might successfully prevent the data from getting to the criminals, and we propose below a "phishing recall"

system and greater use of white and black lists Where these blocking tools are easy for consumers to operate they can reduce the success of phishing greatly. Barriers to sending data are incomplete, however. They do not help catch the criminal, but instead reduce the profit from a given attack.

4. Research How to Use Data

The criminal perspective. Once the criminals have gathered personal data, they have to decide how to use it. For attacks against a financial institution or online merchant, they have to learn the modus operandi — what information is needed for authorization, what dollar limits set off alarms, and what kinds of transactions get more scrutiny. The criminals also need to select the "best" customers to attack — who has the large assets, the good credit score, or other traits that make them a profitable target.

Counter-measures. To the extent the defenders can figure out the patterns of attack, there are potential counter-measures. Sometimes police are lucky enough to identify a potential criminal who is "casing" a system. More likely, financial institutions and online merchants can continually monitor attempted and successful attacks. Better self-awareness within the institution, and better information sharing across institutions, will let defenders respond more nimbly to new generations of attacks.

5. Attempt Crime

The criminal perspective. Next the criminals seek to take advantage of the data they have gathered. Most often the crime is financial fraud, such as by making an unauthorized purchase, opening a credit card account under an assumed name, or hijacking a bank account and stealing funds from it. The crime may occur on a wholesale basis, such as by selling an entire inventory of credit card numbers. As part of the phishing eco-system, there are Web sites that help phishers fence the personal information of their victims. This fragmentation of the crime presents a challenge to investigation and enforcement. The crime may be extortion, such as threatening to reveal information or cause other harm unless payment is made. In some instances, the activity may involve terrorism or support for a political agenda, where the gains would be political rather than financial.

Counter-measures. The moment of actually trying to steal money is the time of maximum risk for many phishers. Before this stage of the lifecycle, the phishers are likely subject to prosecution for conspiracy or computer hacking. Once stealing money occurs, the crime is obvious.

More care may need to be taken by financial institutions, merchants, and others before turning over money or goods. There are numerous counter-measures that can be adopted to prevent theft by insider employees and outside thieves. One important theme is that there should be accurate authentication of individuals before they can actually take money or goods, and improved authentication is one of this report's recommendations.

To reduce the overall level of phishing, one challenge is to arrest the criminal ringleaders who pose the largest risks over time. In some phishing attacks, the actual use of the personal data is done by "mules" who receive modest payments from the ringleaders. Strategies for deterring, detecting, and arresting those ringleaders are also needed.

6. Launder Proceeds

The criminal perspective. When the criminals succeed in stealing money and goods, they next face the challenge of laundering their ill-gotten gains. Goods must be converted into cash, and cash must eventually be placed into legitimate accounts in legitimate institutions.

One expert at the retreat said that the characteristics of the Internet and the new cyber-based payment mechanisms facilitate money laundering because they provide relative anonymity, lack regulation or third party oversight, and provide the ability to move easily across borders without detection or interception. Furthermore, money is represented by digital bits and other value propositions, thus making it difficult to track and trace. In his view, the exponential growth of these models, particularly those that are nonbank and peer-to-peer, may perpetuate the money-laundering problem by providing technical capabilities to more people and enabling them to operate from the comfort of their homes. He also warned that online casinos and new forms of online financial service providers may be used to launder fraudulently obtained funds.[3]

Counter-measures. For criminals, it is risky to try to shift assets into legitimate financial accounts. The international system of anti-money laundering (AML) laws has expanded greatly in recent decades, with a new boost after 2001 in the fight against terrorism. One component of AML efforts is to identify patterns of criminal activity. As phishing grows, it should be a greater priority to ensure that AML systems are used to detect fraud and that phishing patterns of criminal activity are included in the AML system.

Notes to this section

1 The phishing lifecycle was originally conceived by Chuck Wade of the Financial Services Technology Consortium. His paper that includes that work is at *www.fstc.org/projects/counter-phishing-hase1/FSTC_Counter-Phishing-Solutions_Survey_Summary.pdf.*

2 A detailed chart of the lifecycle adapted for the retreat by Jeffrey Friedberg is in Appendix 5.

3 See Kellerman, "Phishing in Digital Streams" at *http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTFINANCIALSECTOR/0,,contentMDK:20383269~menuPK:282890~pagePK:148956~piPK:216618~theSitePK:282885,00.html* and "Money Laundering in Cyberspace" at *http://www.cybrinth.com/uploads/Money%20Laundering%20in%20Cyberspace.pdf*

Understanding the Phishing Problem
Part Four: Recommendations for Action

Participants at the retreat strongly favored supporting, and putting greater resources into, four key, known responses to the phishing problem: support greater consumer education; the consumer experience must be "secure by design;" there must be better user and site authentication; and there must be better tools for effective investigation and enforcement.

Participants also favored developing promising new approaches, summarized here as: learn from the lifecycle of the phisher; ISPs and domain name owners can cooperate on white lists; and use black lists to create a "phishing recall" approach.

In considering recommendations for action, retreat participants were aided by a diagram on tactics, an updated version of which is included in the Internet Battlefield paper at Appendix 4.

1. Support Greater Consumer Education

There was widespread agreement among retreat participants of the need for greatly enhanced consumer education and awareness about phishing.

The case for much greater consumer education. The need for greater consumer education results from the large and growing nature of the phishing problem. The number of phishing attacks has risen rapidly in the past two years. The nature of such attacks also keeps shifting. Bait emails have become far more convincing in appearance. The bad grammar and English usage of earlier attacks — helpful hints to consumers that something was amiss — are less common. Pharming and other sneak-attack methods of phishing are difficult for consumers to detect. In short, ordinary consumers face more and more dangerous phishing attacks, posing obvious hazards for the consumers themselves.

These attacks create a large and growing hazard for many other stakeholders as well. One hazard to businesses is direct loss, such as when merchants or financial institutions are the victims of fraud. The much greater hazard to business, however, is risk of loss of consumer confidence in online commerce. Suppose, for instance, that 10 percent of consumers become increasingly nervous about doing business online. In terms of effects on online merchants or financial institutions, the drop in business would dwarf the direct losses due to fraud. That sort of drop-off in consumer confidence would also impact ISPs, software providers, and all other companies whose business is based on the growth of online activity generally.

Some sectors of online business are likely to be hit harder than others. Some online activities are less risky for consumers, such as simply going to a Web site and surfing. News and other content sites, therefore, quite possibly will be less affected by reduction in consumer trust. By contrast, consumers are likely to treat some online activities as posing greater risks. Online banking, for instance, could be greatly affected if consumers are concerned that malicious software is on their computers or they cannot tell the difference between legitimate banking sites and spoof sites. Companies that are the most constant targets of phishing attacks, including auction sites and banks, likewise face heightened risks from loss of consumer confidence.

The case for consumer education, then, is based initially on the concerns of consumers themselves. It rests next on the business stakeholders whose success depends on consumer trust, both online merchants and financial institutions, but also ISPs and other infrastructure providers. Even more broadly, the dynamism and competitive advantage of the U.S. economy depend on consumer trust in online activity. If American consumers better understand the risks and how to face them, that will contribute to economic growth in the online sector and the U.S. economy generally.

It should be noted that better consumer education is one of several components that are each vital to a comprehensive action plan against phishing. As phishing evolves from exploiting social engineering tactics to using technology to take over consumers' computers without their knowledge, solutions must also focus on the business side of the equation, such as by implementing "secure by design," black lists, and other recommendations in this report.

Recommended Actions

Develop consistent, clear messages. The retreat participants with the most experience in consumer education emphasized the following — *the central need for consistent, clear messages to consumers, leading to learnable actions.*

At the retreat, there were various candidates for what the clear messages should be. For example, the messages could include:

- Don't enter personal information on Web sites;
- Don't click on URLs in email messages; or
- Check through other channels, such as a phone call or a visit to the official Web site, before trusting any suspicious-seeming communication.

Each of these candidate messages may appear overly simplistic. After all, some Web sites properly need to gather personal information to complete a transaction. Sophisticated users often click on a URL in an email when it comes from a trusted source. And constant checking of online transactions by telephone would erode the competitive advantages of online commerce. In response to concerns about phishing, some businesses have opted to put consumer safety first and stopped sending emails to customers asking them to click on links to take advantage of promotions or update their account information.

However, the downsides of this approach to the problem — the loss of cost efficiency and consumer convenience — make it unlikely that it would be universally embraced.

It is also important not to give consumers the false impression that there is a "silver bullet" — a single action that they can take that will protect them from phishing. For instance, encouraging consumers to type in a known URL rather than clicking on a link in an email might protect them from the classic phishing attack but not from pharming.

With that said it remains crucial for those experienced in consumer education to select one or a few clear messages to address the large and growing phishing risk. To address concerns that warnings about phishing could make consumers leery about email and engaging in online commerce at all, educational messages can be positive *i.e.*,"Here are things you can do to use email and the Internet with more confidence." Retreat participants also felt that effective educational messages should convey that consumers have something at stake — "This affects you in this way."

Teach people in context. A second theme from retreat participants was to find ways to teach consumers "in context," at the moment that the risk of phishing appeared. For instance, there may be ways for ISPs or software providers to incorporate a pop-up tutorial or piece of advice when a consumer does a risky action. One example would be if the tutorial became available when a consumer clicked on a URL in an email: "Did you know clicking on this sort of link can be risky? For some helpful pointers on phishing attacks click here." Similarly, consumers may benefit from an anti-phishing toolbar[1] or other software measures to assist consumers.

It was also noted that there are other points at which educational information about phishing could be provided to the consumer. For instance, there could be a brochure in the box when someone buys a new computer. Another idea is for Internet service providers to give consumers advice about phishing when they enroll.

Educate others about phishing. Along with educating consumers, retreat participants also stressed the need to educate other key actors about phishing. Law enforcement and consumer protection experts need to understand the issue better. Technical persons need to understand the broader legal and policy implications. At each stage of the "lifecycle of the phisher" there can be greater education from those who can intervene to reduce the profitability of phishing attacks.

Commit more resources to education. Overall, there was consensus at the retreat of the need for greatly enhanced consumer education about phishing and related risks, such as downloads of spyware and other deceptive software. This will require substantial resources, for traditional public-service announcements on television, for Internet-based PSAs, and for new tutorials that teach "in context."

Educational efforts to address phishing should be part of a larger strategy to have a safer Internet experience and reinforce consumer trust in online activities. To move forward, there must be clear, consistent messages and consensus to use them, innovative ways of

delivering the educational information in context, and funding to enable third-parties to help communicate those messages to consumers.

2. The Consumer Experience Must Be "Secure by Design"

A major way to combat phishing is to be "secure by design." This means that, wherever possible, strong security should be set as the default. Consumers should not have to become professional programmers simply to use their home computers securely.

Security challenges on the Internet. Security on the Internet is inherently challenging. The Internet was designed as an open system, where everyone can connect with everyone else. This openness is a major reason that the Internet has grown so enormously since commercial activity on the 'Net began in 1993. Internet users have increased by more than a billion in just these 13 years. Openness, however, also means that attacks can come from innumerable sources, launched as easily from distant countries as by a nearby neighbor.

To fight the attacks, it makes sense for the experts who design software and systems to design them in a secure fashion. As recently as the late 1990s, security was an afterthought at best for most Web companies.[2] Today, by contrast, gaining and keeping consumer trust is essential.

There have been numerous improvements in the past five years that illustrate security by design. Today, many email programs automatically quarantine or take other action against potentially malicious code that is attached to emails, such as .exe files. Today, many users are protected by anti-virus and anti-spyware software, either on their desktop or through their Internet service provider. Firewalls are now a standard part of the major operating systems, and the software arrives with the firewall already turned on.

Recommended Actions

Emphasize the need to update. Security measures, though, must constantly be updated. Defenders face a cat-and-mouse game, or an arms race, with attackers. For example, attackers by 2004 were pasting a picture over the address line in the browser. The picture showed a reassuring site name, such as *www.realbank.com*. Underneath the picture, however, the browser was actually running a spoof site, such as *www.fakebank.com*. Users who looked at the URL — the address line — were lulled into a false sense of security. They then would provide their personal information, transfer funds, or otherwise fall for the fraud.

The creators of browsers then responded. Internet Explorer, for example, is now designed so that attackers cannot paste a picture over the address line. That part of what the user sees is now "hardened" — the browser software is written to prevent this sort of attack. Ordinary users never learn about the change, but "security by design" is achieved.

This example illustrates a broader point, the need for updates. Consumers who use the

Internet are linked to a billion other people who are potential attackers. New attacks are being created constantly. In this environment, *it is imperative for consumers to update their protections often*. For anti-virus, anti-spyware, and software more generally, consumers will be exposed to known and dangerous attacks unless they update. A key ingredient of "security by design" is having "updates by design."

Implement "secure by design." Discussions at the retreat revealed that businesses and consumers may have different perspectives on how to pay for computer security. Consumer advocates stressed the need to have good security included by default and for free. Only in this way will ordinary consumers be safe, and feel safe, on the Internet. Some business representatives, by contrast, compared the family computer to the family car. Families are used to paying for customer service during the life of the car, and it is reasonable for them to pay for updates, upgrades, and other security features during the life of the computer.

In practice, there will undoubtedly be variety in the ways that different industries and different consumers approach computer security. There are at least three arguments, however, for having much of the burden of computer security fall on the professionals.

First, there are spillover effects ("externalities") from bad security at the individual level. Home computers can be infected by viruses and then spread the problem. Similarly, home computers with bad security often become "zombies," taken over by hackers and used to launch attacks against others.

Second, widespread good security will shift the risk/reward calculation of the attackers. If effective anti-phishing measures are used on most home computers, then the profitability and prevalence of phishing attacks will fall. This is similar to having inoculations for most people in a population — even the few people who lack inoculations are less likely to be exposed to the dangerous disease.

Third, it makes sense for security measures to be designed and operated, where possible, by the actual experts. Computer security professionals will do a better job at designing and operating defensive measures than will home users. The burden should not be on home users to know what to ask for in a complicated marketplace.

There was widespread consensus at the retreat that "security by design" is an important principle that should be implemented across-the-board. As new attacks occur, the defenders must create new defenses, and make the defenses into the new default.

3. There Must Be Better User and Site Authentication

Phishing attacks depend on fake identity. In the classic phishing email, the fraudster fakes being the trusted brand, such as the bank or online merchant. The user then goes to a fake web site, which pretends to be the legitimate site of the trusted brand. Next, the fraudster uses the harvested personal information to fake being the actual consumer, such as by purchasing goods online or hijacking the consumer's account. Similarly, for

deceptive downloads, the malicious software often fakes being from a trusted source.

The answer for fake identity is better authentication, that is, better ways to establish someone's true identity. Participants at the retreat agreed that better authentication is an essential element in the fight against phishing. Better authentication is needed on the user side, so that it is harder for the fraudster to pretend to be the consumer. Better authentication is also needed on the business side, so that it is harder for the fraudster to pretend to be the trusted brand in an email or Web site.

Recommended Actions

Implement better user authentication. Most retreat participants believe that users will increasingly need to identity themselves with something stronger than "single-factor authentication" such as name and password. The FDIC and other federal banking agencies have taken the lead in requiring stronger authentication. The FDIC has issued two detailed studies of how to authenticate users in order to prevent account hijacking.[3] In October, 2005 the federal banking agencies together required more than name and password for transactions involving access to customer information or the movement of funds to other parties:

> *"Financial institutions should conduct a risk assessment to identify the types and levels of risk associated with their Internet banking applications. Where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks. The agencies consider single-factor authentication, as the only control mechanism, to be inadequate in the case of high-risk transactions involving access to customer information or the movement of funds to other parties."*[4]

Financial institutions are expected to come into compliance with this guidance by the end of 2006.

The federal agencies, while calling for stronger authentication, did not state exactly what new measures should be used. In 2006, financial institutions will likely experiment with a number of new approaches for authenticating their customers. These experiments, in turn, will provide useful examples that can spread to other online sites.

Retreat participants expressed support for various approaches. From the consumer perspective, it will be important that new measures be easy to learn and use, with good customer support as users get accustomed to the new systems. Technical experts at the retreat stressed the importance of not using symmetric keys to authenticate (*i.e.*, a common secret that the consumer must share with a Web site and a bad guy might intercept), but instead moving to asymmetric keys (*e.g.*, Public Key Cryptography) where a private key is securely maintained by the consumer and the Web site uses an openly distributed public key to authenticate that person.

There was considerable discussion at the retreat about one-time passwords that can be used to authenticate consumers. There are various types available, from high tech devices that display time-based unique PINs, to low tech solutions such as a wallet-size card, apparently used in Brazil but not widespread in the United States, that is similar to a lottery rub-off card. When logging in to their account, users give their name and password, and then rub off the next number of the card and enter that number as a one-time extra password. In this way, phishing Web sites and spyware might learn a one-time password, but if it is after the consumer has used it, the password would be worthless. New access to the account would require another password that had never previously been sent over the Internet.

However, it should be noted that two-factor authentication by itself does not address the full range of phishing problems. For example, one-time passwords may still be compromised by man-in-the-middle attacks in which consumers are tricked into providing them to phishers before they have been used. The phishers can then immediately use those passwords to gain access to consumers' accounts.

Implement better site authentication. Many phishing attacks would be foiled if it were easier for ordinary users to tell a real Web site from a fake site. This report recommends a number of measures to improve site authentication. These include: improved transparency of URLs, discussed in the previous "secure by design" recommendation; cooperation on white lists of safe sites, discussed in Recommendation 5; and the phishing recall approach, discussed in Recommendation 7.

One intriguing suggestion at the retreat was that companies may be able to design their URLs better and more simply. Phishers take advantage of the complexity of Web addresses to fool consumers. For instance, the URL for the National Consumers League's Web site, *http://www.nclnet.org*, could be represented in other formats full of odd characters and seemingly random numbers:

Equivalent URL	Format
1. *http://216.147.26.113*	Internet Protocol address (dotted-decimal)
2. *http://3633519217*	D-word (decimal)
3. *http://11011000100100110001101001110001*	Binary
4. *http://%77%77%77%2e%6e%63%6c%6e%65%%74%2e%6f%%72%%74*	Hexadecimal
5. *http://!$^&*()+'+{}[]:;@www.nclnet.org*	Alphanumeric

URLs # 1 through 4 represent simple mathematical translations which are machine readable. In the case of URL # 5, only the portion after the @ sign is used to determine the location of the Web site. Each of these addresses is legitimate and if copied and pasted into a Web browser, would take one to the National Consumers League's Web site.

When consumers see URLs such as these, it is very difficult for them to know to whom they belong and whether trusted organizations are being spoofed. To illustrate this dilemma, assume that phishers have registered the domain name *http://www.phishinginc.com*, whose Internet Protocol address is 10.10.10.10., and that they are targeting an online bank called First Real Bank, *www.firstrealbank.com*, whose Internet Protocol address is 217.147.26.113.

To trick consumers, the phishers might create obfuscated URLs that look like they come from First Real Bank:

1. *http://www.firstrealbank.com%40%77%77%77.phishinginc%2e%63%6f%6d/*
Translation: *http://www.firstrealbank.com@www.phishinginc.com/*

This bogus URL, which includes a combination of hexadecimal and alphanumeric characters, will take the customer to *www.phishinginc.com*, not to *www.firstrealbank.com*.

2. *http://ebanking/login@10.10.10.10/firstrealbank/*
Translation: *http://ebanking/login@phishinginc.com/firstrealbank/*

This bogus URL takes advantage of the fact the bank's customers will assume they are being sent to an ebanking login screen at firstrealbank.com.

3. *http://%77%77%77%20/%2020427512177/217.147.26.113/useraccount/@*
01101110000010100000101000001010
Translation: *http://www/phishinginc.com/firstrealbank.com/useraccount@phishinginc.com*

This bogus URL uses a combination of techniques to obfuscate the URL and in the process redirect the bank's customers to the spoofed Web site.

Technically savvy consumers can use tools like the one found at *http://www.netdemon.net/decode.html* to determine if a suspicious URL is legitimate or not before clicking on it. However, most consumers would find that procedure onerous. Moreover, most consumers are unlikely to question what appears in their browser's address bar when they click on links in emails purporting to be from trusted sources or when they type in the URLs for their intended destinations. Using software that automates this type of checking can be helpful and is available from a variety of vendors. Examples include ScamBlocker from Earthlink, SpoofStick from CoreStreet, AccountGuard from eBay, and the Phishing Filter that will soon be released by Microsoft.

To limit the potential for confusion and the corresponding opportunities for phishers, legitimate companies and organizations can educate their technical staff about the advantages of easy-to-understand URLs. A related best practice would be to encourage the use of standard forms for significant URLs and educate consumers to look for them. It may be useful, for instance, to obtain consensus on a standard format for consumer affairs, such as *www.mycompany.com/consumer*. Having this standard approach for site names would be consumer-friendly. The ability to easily contact the organization's consumer relations personnel could also enhance trust in the site and in online commerce more generally.

There are also longer-term efforts underway to improve site authentication. For example, Microsoft has launched its "Infocard" project that would address many aspects of online identity.[5] The Liberty Alliance is supported by 150 global organizations in a federated approach to improving authentication for online commerce.[6]

Email authentication can also help consumers avoid phishing attempts. Many consumers are not sure whether to trust emails sent by their banks, retailers, auction sites, or others. Efforts to improve email sender authentication include DomainKeys[7] and Sender ID.[8] Another related effort is the Electronic Authentication Partnership.[9]

4. There Must be Better Tools for Effective Investigation and Enforcement

Lack of resources. Investigators in law enforcement agencies, consumer protection offices, and the private sector often lag behind cyber criminals in terms of their understanding of technology and the equipment at their disposal. As phishing methods evolve, it is crucial for investigators to keep up-to-date. Yet sufficient funding is often lacking in both the public and the private sector for the ongoing training, hardware and software, and other tools necessary to keep up with the phishers.

Fragmented nature of phishing. Another challenge for investigators is the fragmented nature of phishing. Different people may be responsible for various aspects of phishing, such as providing "how-to" instructions, helping to set up spoofed sites and sending emails, and laundering the proceeds.

Furthermore, many of the perpetrators targeting consumers in the U.S. operate from foreign countries. Differences in language, laws, and legal procedures make it very difficult to conduct searches, seize assets, and bring enforcement actions. In addition, travel for investigators, lawyers, and witnesses can be costly.

Constraints on information sharing. These problems are exacerbated by the fact that some U.S. law enforcement agencies are prohibited by law from sharing investigative information with their foreign counterparts. Information sharing is also an issue between government and the private sector. For example, the Consumer Sentinel Database, maintained by the Federal Trade Commission, contains information from consumers about identity theft and other types of fraud, but is only accessible to government investigators. Law enforcement agencies, Internet service providers, and entities that have been spoofed may each have vital information about a phishing incident, but there

is no central repository that specifically contains information about phishing and that is accessible to both government and the private sector.

Recommended Actions

Commit more resources for personnel, training and equipment. In order to take advantage of strategic opportunities to disrupt phishing and bring action against the perpetrators, government and the private sector must commit more resources for training, hardware and software. Peer-to-peer training, in which personnel from one government agency or company would train personnel from other agencies or companies, is one model to consider. Another is cross-training, where personnel from the government would provide training for fraud investigators from the private sector (or vice versa). Training must be constant to keep investigators up-to-date. Equipment and software must also be regularly updated if investigators are to keep up with the evolving tactics of phishers. In addition, funding is necessary to ensure that there are sufficient numbers of investigators and other personnel to handle the phishing problem, and that expenses related to phishing investigations and enforcement, such as travel, are covered.

Improve information sharing and cooperation. Legislation may be needed to enable law enforcement agencies in the U.S. to share investigative information with their counterparts in other countries and to make it easier to bring cross-border actions against phishers. Legislation may also be needed to facilitate information sharing between government and the private sector.

It would also be helpful to create a database for phishing information that would be accessible to government and the private sector. In considering such a project, initial issues might include:

- *Cost of design and management.* Designing and managing such an extensive database would probably require significant time and money.
- *Access to the database.* Obviously, it is essential to keep investigative information confidential. A system would have to be devised for vetting those who would contribute to and obtain information from the database, and good security would be needed so that only they would be able to gain access.
- *Liability for information in the database.* The entity that maintains the database might need to be shielded from liability for information in the database that is provided by others.

5. Learn from the Lifecycle of the Phisher

Our examination of the lifecycle of the phisher highlights moments of maximum risk from the perspective of the phishers themselves. Those concerned with phishing have tended to look at the problem from the side of consumers and others who are trying to prevent the attacks. By focusing on the criminals' perspective, it is possible to create additional ways to deter, detect, and catch the criminals.

Recommended Actions

Disrupt the early stages of an attack. There appear to be significant opportunities to disrupt the planning and other early stages of a phishing attack. Phishers need to learn about opportunities to attack, and likely need to assemble a group in order to send the bait, operate the spoof Web site, convert the information into money, and then launder the money.

There are familiar enforcement strategies to disrupt these types of criminal activity. Investigators can lurk in chatrooms and other places where potential phishers communicate with each other. Undercover agents can infiltrate the criminal groups. Sting operations can create the evidence needed for successful prosecutions. These sorts of measures, for instance, are currently being used on an international scale against child pornography. These measures, taken together, can significantly increase the risk to potential phishers. They won't know who to trust as they create the phishing attacks. The goal is to "tip" the calculus of the criminals, so that the risk outweighs the benefits of phishing.

At our retreat, some participants emphasized the investigative and enforcement challenges in this area. Phishing attacks are often international, creating obstacles to enforcement. Prosecutors and police have not made phishing a priority, in part because it is not a violent crime and the theft of information may seem less serious than direct financial fraud. In addition, many corporate fraud departments and law enforcement offices lack the resources or expertise to bring cases involving cutting-edge technology.

In response, there are strong arguments for industry to work especially closely with law enforcement in the fight against phishing. There have been recent examples of how industry support increases the effectiveness of law enforcement. As part of the CAN-SPAM Act, Internet service providers have a private right of action. ISPs have used this power to go after large-scale spammers, and have developed evidence used by government enforcement agencies. For trademark law, the owner of the trademark has a direct financial stake in fighting against counterfeiting. Trademark holders have long worked closely with law enforcement on these efforts, in some cases supplying additional investigators or attorneys for law enforcement. Similarly, the music and movie industries work closely with government agencies in fighting against copyright piracy.

As the scale of phishing attacks continues to grow, law enforcement and the affected industries should learn from these precedents. Together, there are likely cost-effective ways to increase the risk to individuals who are considering becoming part of the phisher underground.

Use disinformation when the criminal gathers personal data. Defenders can cause trouble for phishers by feeding false personal data to the spoof sites. This approach may reduce the economic value of phishing. For instance, it is apparently common today for phishers to sell each individual's personal data for a certain price per account. The fraudsters who buy the accounts then attempt to hijack the account or otherwise use the personal information for profit. In this setting, suppose that half of all accounts were

actually fake data, provided on purpose by defenders in order to fool the phishers. If many accounts are actually fake data, then the price per account will plummet. The economics of phishing thus becomes less favorable for the phishers.

Feeding false data to the phishers has another key advantage. The defenders can deliberately "seed" a false name, Social Security number, bank account, etc. to a spoof site. If that false name or number is then used, that is strong evidence that the person using the data is linked to criminal phishing activity. This sort of seeding is already used in the information industry as a way to guard against unauthorized use of a mailing list or other corporate information.

The use of disinformation, therefore, can reduce the value of personal information on the black market and create evidence that links the criminal to illegal phishing activity. The hope is that phishers may actually become scared to use personal data, once they realize the personal data may be "bait" to catch the phishers themselves.

Follow the money in the later stages of the attack. It obviously makes a great deal of sense to disrupt criminal acts as early in the lifecycle as possible, before the harm to individuals takes place. The lifecycle analysis, however, suggests there may be useful measures as well that target later stages of the lifecycle.

The best hope may be to "follow the money." One stage is where a "mule" — a low-level operative — tries to convert the stolen personal information into money. Antifraud programs may identify likely fraudulent purchase and phishing attacks. Law enforcement can follow up on these fraudulent purchases, perhaps seeing where the mule sends the money or perhaps catching the mule and seeking to "turn" the mule into an informant.

A variation is to work more closely with the anti-money laundering community. It is not clear that phishing has been brought clearly to the attention of that community. Once it is, there may be opportunities to detect phishing transactions, or to trace and then enforce against persons involved in known phishing operations. More generally, those engaged in fighting phishing may learn valuable lessons from AML experts who have faced similar issues for different crimes.

6. ISPs and Domain Name Owners Can Cooperate on White Lists

For the classic phishing attack, the bait almost by definition pretends to be from a trusted company, agency, or organization that owns the domain name. Examples include well-known financial firms, auction sites, online merchants, charities, and federal government agencies. Because phishing attacks concentrate on these well-known domain name owners, there is an opportunity for them to fight back.

The idea is these entities — the most likely victims of phishing attacks — can cooperate with Internet service providers. Each of them can provide a "white list" of the actual URLs that they use. The ISPs then can establish some mechanism so that spoofs of that

entity are filtered out or flagged with a warning.

There are various technical ways that such cooperation might be implemented. To give one example, American Express might provide ISPs with its "white list" of corporate sites, updated regularly. If a suspicious site is detected, a warning might appear on the user's screen, saying: "The link has the name 'American Express' in its title. That organization has informed us that the site you have clicked on is not a Web site of 'American Express.'" In this approach, the user would be given a very useful warning if the site is a spoof site. On the other hand, the words "American Express" might be in the title because of news or commentary about the company. In those instances, the user may wish to click through to the site.

Participants in the retreat suggested that domain name owners might find it easier to create a white list than one would suspect. The reason is that they already have a strong incentive to police their URLs (their Web site addresses) for trademark or other legal reasons. Companies engaged in online commerce have strong incentives to monitor dilution of their trademarks. Government agencies and nonprofit organizations such as charities also have grave concerns about the integrity of their names. For Web sites that have confusingly similar names, domain name owners can bring enforcement actions under national laws or the Uniform Dispute Resolution Procedure, administered as part of the international domain name system.

Recommended Actions

Create a white list system. If creating the white list of sites is indeed manageable on the domain owner side, then the next step is to set up cooperative relationships between it and the ISPs. One useful model here might be the "clearinghouses" that developed historically for payments among multiple banks. Those domain name owners and ISPs that wish to cooperate in a clearinghouse can do so immediately, without waiting for legislation or for universal agreement on procedures. If major domain name owners and ISPs can get such a clearinghouse started, then protection against phishing could begin promptly for millions of consumers.

It is not the role of this report to recommend the technical details of how such a clearinghouse arrangement might work. Initial issues might include:

- *How to check the white list*. This might be done at the ISP level, on email entering the system or on web sites clicked that are the destination of a user. It might be done instead at the client level, on the user's desktop.
- *Updating*. There may be challenging technical details about how to distribute the updated white lists. The updating process itself would have to be designed to resist hacker attacks.
- *Cost sharing*. The costs of participating in the clearinghouse would have to be worked out, with the roles of Web site owners and ISPs determined. Because white lists would probably be quite long, quickly filtering URL requests would be challenging and may have significant impact on response time and hardware

demand.

- *Complaint procedure*. The clearinghouse would likely need to develop some procedure for handling complaints from Web sites that believe they are being treated unlawfully or unfairly by the system.
- *Liability issues*. The stronger the blocking action taken within the system, the greater the risk of liability. In the American Express example, above, there was simply a warning to users that they might be going to a spoof site. If the approach instead is to block access for users to certain sites, then there may be greater liability concerns, such as on defamation or antitrust ground.[10]
- *Other security concerns*. Technical experts should examine the proposed system to discover and address any possible security problems that might arise from dissemination of white lists of sites.
- *Authentication:* The clearinghouse would need to be able to prove that additions/subtractions are made by authorized company representatives.
- *Accreditation:* The clearinghouse would necessarily exclude certain businesses and organizations (the spammers for example). The clearing house would need to establish clear and consistent membership rules to steer clear of unfair business practice claims.

There was considerable interest among a number of retreat participants about the possibility of setting up improved systems of cooperation among ISPs and online companies. Participation in such a clearinghouse might grow quickly if it becomes a competitive edge for members. Participating companies and ISPs could tell their customers about the anti-phishing advantages for consumers of being part of the "Anti Phishing Clearinghouse," or whatever the cooperating group might be called.

7. Use Black Lists to Create a "Phishing Recall" Approach

Along with "white lists" of legitimate sites there can be 'black lists" of known or suspected phishing sites. In this report, we are proposing a new approach to black lists that might greatly reduce the number of phishing emails opened by consumers.

One interesting statistic raised at the retreat is that the average email is not opened until about 12 hours after the ISP first makes the email available to the consumer. This latency provides a window of time for an updated black list to be distributed. The email could then be flagged as a potential phishing email. There are various choices about what to do with such emails — they might be deleted entirely, placed in a special "warning" mailbox, or be opened along with a warning message. The insight is that this window of time provides a major opportunity for those fighting against phishing. We are calling this the "phishing recall" approach, because of its goal of recalling (or limiting the effect of) phishing emails even after they first go to the consumer. (Some people at the retreat called it the "alert/recall" approach, because of the recall of emails once there was an alert about the spoof site.)

The goal is to squeeze the amount of time that a spoof Web site can operate. Criminal

spoof sites want to stay open long enough to get consumers to respond, but close before law enforcement can catch up with the site operators. Other parts of this report have discussed the potential of greater industry and law enforcement cooperation in detecting and bringing enforcement actions against spoof sites. Greater enforcement efforts thus limit how long the spoof site can profitably stay open. The APWG reports that the average spoof site now stays up for about 5.5 days.

Recommended Actions

Create phishing recall systems. The phishing recall approach takes advantage of the fact that spoof sites have to stay open long enough for consumers to respond to the bait. Suppose that all the bait emails get sent at the same time. Some consumers might take the bait immediately, and our proposal would not help them. The average email, however, sits for 12 hours before being opened. If the defenders can spot the spoof site within that time, then the updated black list can be distributed. In our example, consumers who open email after 12 hours would have the new protection.

One advantage of the phishing recall approach is that it is much easier to detect a phishing site after the bait is sent than before. Various stakeholders might set up "honeypots" to attract the bait. These would be email addresses that look like ordinary accounts and seem attractive targets to phishers. As soon as a new bait email is distributed, the honeypots can identify the new attack and the associated spoof site. The black list can be updated immediately.

Participants at the retreat suggested various mechanisms for implementing the phishing recall approach. One approach is for ISPs to take a central role, perhaps actually "recalling" emails that have been addressed to consumers but not yet opened. Variations are for those emails to be placed in a special mailbox as a potential phishing attack, or for a warning to pop up as the email is being opened. If black lists can be spread quickly, then another alternative might be to have the warning or other action done at the client level, on the consumer's own computer. Another approach might be to have the warning or other action kick in at the moment that the user clicks on a Web site address that appears to be that of a spoof site. Some Internet service providers are already using information about phishing sites to protect customers; for example, AOL blocks known phishing sites so that customers who click on their addresses cannot reach them.

The technical details of the phishing recall approach, therefore, are open to the creativity of ISPs, consumers, and software companies that work with emails or browsers. One question for industry discussion is what set of stakeholders should sit down together to decide how to detect likely phishing attacks and then get solutions to the consumer desktop before the spoof sites are accessed. A related question is who should pay the costs of establishing honeypots and otherwise detecting apparent phishing sites. In all of these discussions, one underlying theme should be how to scale the pro-consumer actions so that they are effective against global and numerous attacks.

Advantages of the phishing recall approach. As with the white list approach discussed above, a positive aspect of the phishing recall approach is that it can begin incrementally, with the organizations who decide to start it. There is no need to wait for legislation or universal agreement on standards. Instead, various ISPs and other anti-phishing organizations can seek to implement mechanisms immediately to protect consumers as soon as a site appears to be a phishing site.

One especially favorable aspect of this approach is that it may offer particular help to consumers who are otherwise most vulnerable to phishing attacks. As an empirical estimate, the consumers who check their email most frequently are the heavy users who are likely to be relatively sophisticated about phishing attacks. These constant users of email may also be protected more often by corporate firewalls or other measures that reduce the risk of phishing. By contrast, persons who less feverishly check their email seem likely as well to be less sophisticated on average. With the phisher recall approach, these less sophisticated users would be more fully protected, because more of their emails would be "recalled" before they were opened by the consumer.

The phishing recall approach also has a positive interaction with consumer education about phishing. The most effective consumer education is when it happens in context, at a "teachable moment." Suppose that a consumer tutorial is available at the moment that a phishing email is recalled or otherwise flagged by the system. Consumers might see an email that is known to be linked to phishing. At the moment they open it, a tutorial might pop up explaining why it is known to be a phishing email, and providing additional links or information about phishing. This kind of consumer education in context is likely to be especially effective.

The next recommended step is for industry stakeholders and consumer advocates to meet to discuss ways to implement the phishing recall approach. Initial issues might include:

- *Means of creating black lists.* Criteria would need to be developed for creating and sharing black lists.
- *Costs of creating honeypots and other monitoring.* Stakeholders would have to decide on cost-sharing approaches for tracking apparent bait emails.
- *Technical issues on updating.* Ways to get black lists circulated in real time need to be developed, while being resistant to attack by hackers.
- *Creating appropriate responses once black lists are circulated*. Various stakeholders should consider what mix of recall, segregation of emails, warnings, or other measures would be best once a bait e-mail or spoof site is placed on a black list.
- *Legal liability issues.* Black lists that benefit consumers must be consistent with defamation and other legal concerns. Appeals procedures should be created to address the concerns of those whose activities are placed on black lists.
- *Cooperation with law enforcement.* Private-sector participants in the process should consider under what circumstances information on the black list should be immediately shared with law enforcement agencies. A related question is the extent to which the resources of private-sector stakeholders can be used to leverage

law enforcement resources for these efforts.

- *Authentication and accreditation of submitters/information:* The content of the lists needs to be trustable. Bad guys, disgruntled individuals, and business competitors can not be allowed to mischievously enter legitimate domains.

As with the white list approach discussed above, there appears to be a way forward for industry leaders who wish to protect their consumers against phishing. Reducing the volume of phishing emails that are opened by consumers can shift the economics of phishing, benefiting even those who do not participate in the initial efforts.

Notes to this section

1 One such toolbar is available at *http://www.microsoft.com/mscorp/safety/technologies/antiphishing/at_glance.mspx*.

2 For a discussion of how recently security awareness has come to the Internet, see Swire [2005].

3 See FDIC [2004], [2005].

4 Federal Financial Institutions Examination Council [2005].

5 For background on Infocard, see Microsoft [2005]. For an analysis of Infocard and how it differs from Microsoft's Passport authentication approach, see Swire [2006].

6 See *www.projectliberty.org*.

7 See *antispam.yahoo.com/domainkeys*.

8 See *www.microsoft.com/senderid*.

9 See *www.eapartnership.org*.

10 If the liability concerns turn out to be too great, then it is possible that legislatures could consider narrowly-tailored safe harbors for activities done by the clearinghouse.

Conclusions and Next Steps

If the level of phishing attacks continues to rise on the Internet, numerous consumers may stop participating in online transactions or may curb their growth in use compared to a more trusted system. Collaborative efforts among the many stakeholders are needed. The call for action in this report shows multiple ways to move forward, in both the near and long term. This action will be good for consumers, for industry, and for all who value an environment where trust, not fraud, flourishes.

The recommendations that arose from the retreat form a comprehensive action plan against phishing:

- Support greater consumer education;
- The consumer experience must be "secure by design;"
- There must be better user and site authentication;
- There must be better tools for effective investigation and enforcement;
- Learn from the lifecycle of the phisher;
- ISPs and domain name owners can cooperate on white lists;
- Use black lists to create a "phishing recall" approach.

The National Consumers League plans to organize working groups to carry forward recommendations from the Anti-Phishing Retreat. Participation in the working groups will not be limited to the people who attended the retreat; others who are interested are welcome to join in this effort, whether they are from the same agencies, institutions and organizations or from different ones.

Please contact Susan Grant at NCL, 202-835-3323 x 124, for more information.

Appendix 1

NCL Anti-Phishing Retreat Acknowledgements

The National Consumers League

The National Consumers League (NCL) was the convening organization for the Anti-Phishing Retreat and this report. A nonprofit organization founded in 1899, NCL's mission is to protect and promote social and economic justice for consumers and workers in the United States and abroad. Among its programs is the National Fraud Information Center/Internet Fraud Watch (NFIC/IFW), a hotline and Web site that provides tips to consumers about telemarketing and Internet fraud and transmits information from consumers about suspected fraud to law enforcement agencies. Tips on phishing and other Internet-related frauds can be found on the NFIC/IFW Web site, *www.fraud.org*. NCL also operates the *www.phishinginfo.org* Web site, which provides advice about phishing and materials for consumer education. NCL's main Web site is *www.nclnet.org*.

American Express Company

The American Express Company is one of the principal sponsors of the retreat and this report. American Express Company (NYSE: AXP) is a diversified worldwide travel, financial and network services company, founded in 1850. It is a world leader in charge and credit cards, Travellers Cheques, travel, and business services. Since 1996 American Express has been aggressively pursuing a strategy of opening its merchant network and card product portfolio to third party issuers around the world. By leveraging its global infrastructure and the powerful appeal of the brand, American Express aims to gain even broader reach for its network worldwide. American Express has now established 93 card-issuing partnership arrangements in more than 100 countries.

First Data Corporation

First Data Corporation is one of the principal sponsors of the retreat and this report. First Data Corp. (NYSE: FDC) is a leading provider of electronic commerce and payment solutions for businesses and consumers worldwide. Serving 4.6 million merchant locations, 1,500 financial institutions and millions of consumers, First Data powers the global economy by making it easy, fast and secure for people and businesses around the world to buy goods and services using virtually any form of payment. The company's portfolio of services and solutions includes credit, debit, private-label, gift and other prepaid card issuing and merchant transaction processing services; money transfer services; money orders; fraud protection and authentication solutions; check guarantee and verification services through TeleCheck; as well as Internet commerce and mobile solutions. Western Union, together with Orlandi Valuta and Vigo, make up one of the world's largest money transfer networks with more than 271,000 Agent locations in more than 200 countries

and territories. The company's STAR Network offers PIN-secured debit acceptance at 1.9 million ATM and retail locations. The company's STAR Network offers PIN-secured debit acceptance at approximately 1.9 million ATM and retail locations.

Microsoft Corporation

Microsoft is a leading software company that works to enable people and business around the world reach their full potential.

The Reporter

The Reporter for this project is Peter Swire, C. William O'Neill Professor of Law at the Moritz College of Law of Ohio State University and a Visiting Senior Fellow at the Center for American Progress. From 1999 until early 2001, Professor Swire served as Chief Counselor for Privacy in the U.S. Office of Management and Budget, where he was also active on the White House E-Commerce Working Group. His research and writings have covered many of the topics relevant to phishing, including the uses of personal information, financial privacy, cybersecurity, trust in online transactions, and the international aspects of the law of cyberspace. The writings are available at *www.peterswire.net*. Thanks to Margaret Betzel for her research assistance on this report.

Appendix 2

Retreat Participants

Bill Ashworth
Yahoo! Inc.
Jacqueline Beauchere
Microsoft Corporation
Margaret Betzel
Ohio State University
Paula J. Bruening
Center for Democracy & Technology
Peter Cassidy
Anti-Phishing Working Group
Gregory Crabb
U.S. Postal Inspection Service
John Dentico
LeadSimm
Joan DeSimone
Facilitator
Danielle Domenica
American Express Company
Shannon L. Feldpush
Facilitator
Anna Flores
American Express Company
Jeffrey Friedberg
Microsoft Corporation
Stephen Diaz Gavin
Patton Boggs LLP
Susan Grant
National Consumers League
William Gruhn
Maryland Attorney General's Office
Kathleen Hamilton
Identity Theft Resource Center
Stephen D. Hannan
Howard County Office of Consumer Affairs
Doug Johnson
American Bankers Association
Franck Journoud
RSA Security
Laurel Kamen
American Express Company
Tom Kellermann
Cybrinth LLC
Daniel Larkin
FBI, Internet Crime Complaint Center
Ron Layton
U.S. Secret Service
Miles Libbey
Yahoo! Inc.
Corinne Martin
Facilitator
Phyllis P. McDonald
Facilitator
Leonard Michaels
American Express Company
Steve Mott
BetterBuyDesign
Judie Mulholland
FSU/Florida Cybersecurity Institute
Linda Sherry
Consumer Action
Barbara Span
First Data Corporation
Gina Strayer
One Economy Corporation
Peter Swire
Ohio State University
Ron Teixeira
National Cyber Security Alliance
Frank Torres
Microsoft Corporation
Dee Walker
Montgomery County, Maryland Department of Police
Neal Walters
AARP Public Policy Institute
James A. Wright
National Crime Prevention Council

Appendix 2

Retreat Agenda and Speakers

Opening Debate: *What's the Problem Here?*

Introduction: Barbara Span, First Data Corporation
Moderator: Steve Mott, BetterBuyDesign
Debaters: Tom Kellerman, Cybrinth LLC
Peter Cassidy, Anti-Phishing Working Group
Jeffrey Friedberg, Microsoft Corporation

Presentation: *How does Threat-based Strategic Thinking and Planning Work?*
Introduction: Dr. Phyllis McDonald, Ed. D., Consultant
Speaker: Dr. John Dentico, Consultant

Tutorial: *Exactly how does Phishing Work?*
Introduction: Frank Torres, Microsoft Corporation
Speaker: Jeffrey Friedberg, Microsoft Corporation

Panel Discussion: *What Challenges does Phishing Present to Different Sectors?*
Moderator: Dr. Phyllis McDonald, Ed. D., Consultant
Panelists: Daniel Larkin, FBI
Franck Journoud, RSA Security
Barbara Span, First Data Corporation
Susan Grant, National Consumers League

Presentation: *How Have other Challenges Been Creatively Addressed?*
Introduction: Laurel Kamen, American Express Company
Speaker: Leonard Michaels, American Express Company

Breakout Groups: *Threat Assessment Activity*
Strengths and Weakness Analysis
Channel Interrupt Analysis
Facilitators: Dr. Phyllis McDonald
John Dentico
Joan DeSimone

Group Reports: *Review and Discussion*
Conclusion: *Discussion and Recommendations*

Appendix 4

Internet Fraud Battlefield

Courtesy of Jeffrey Friedberg, Director of Windows Privacy, 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

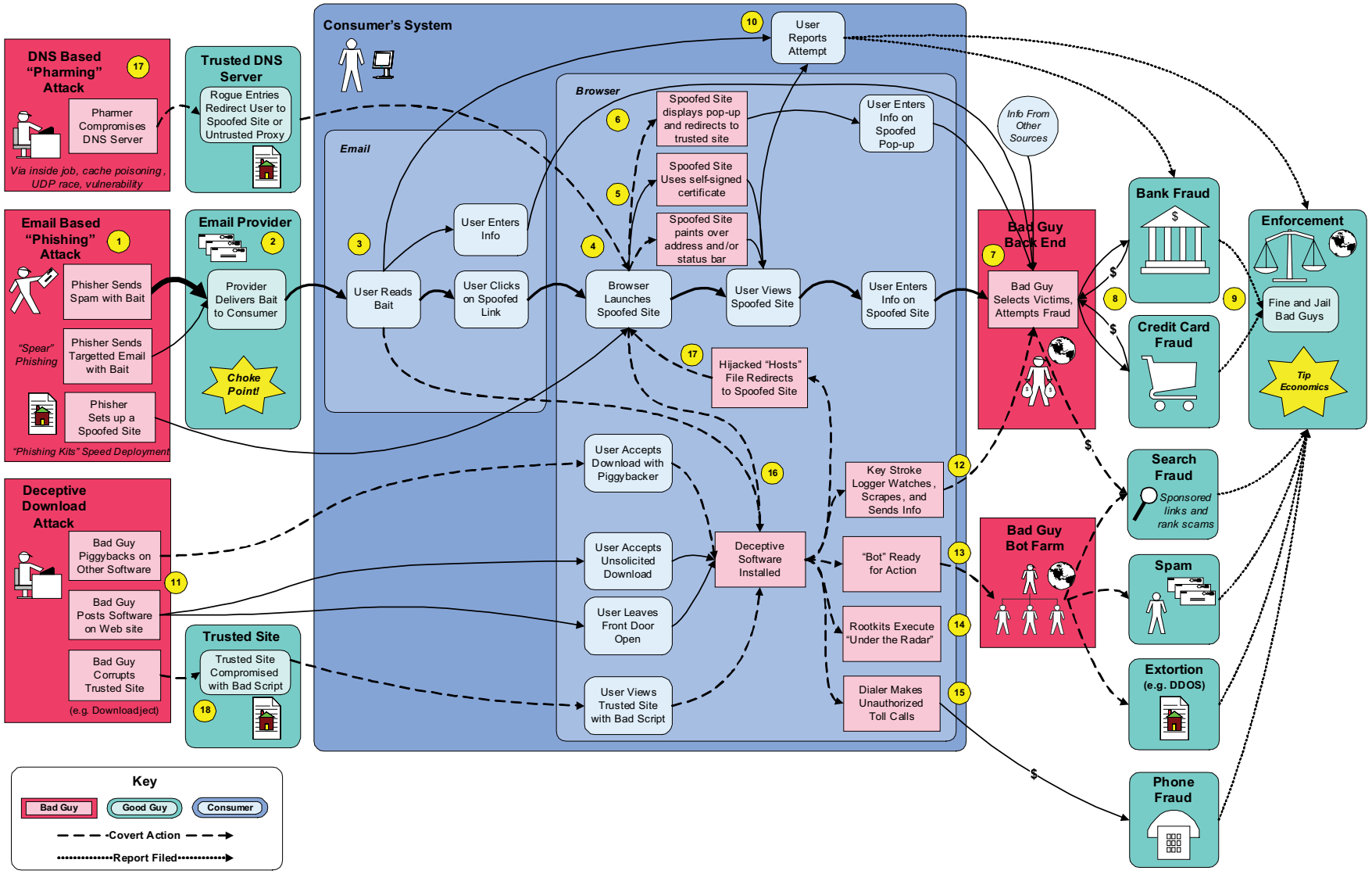
The Internet Fraud Battlefield diagram presented on the next page offers a high level end to end view of the problem space. It illustrates some of the ways users get tricked, how their systems get compromised, how the Bad Guys commit fraud, and where the Good Guys (*e.g.*, email service providers, banks, 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



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).

Figure 1: Spoofed pop-up with phony login visually on top of a real 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).

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.

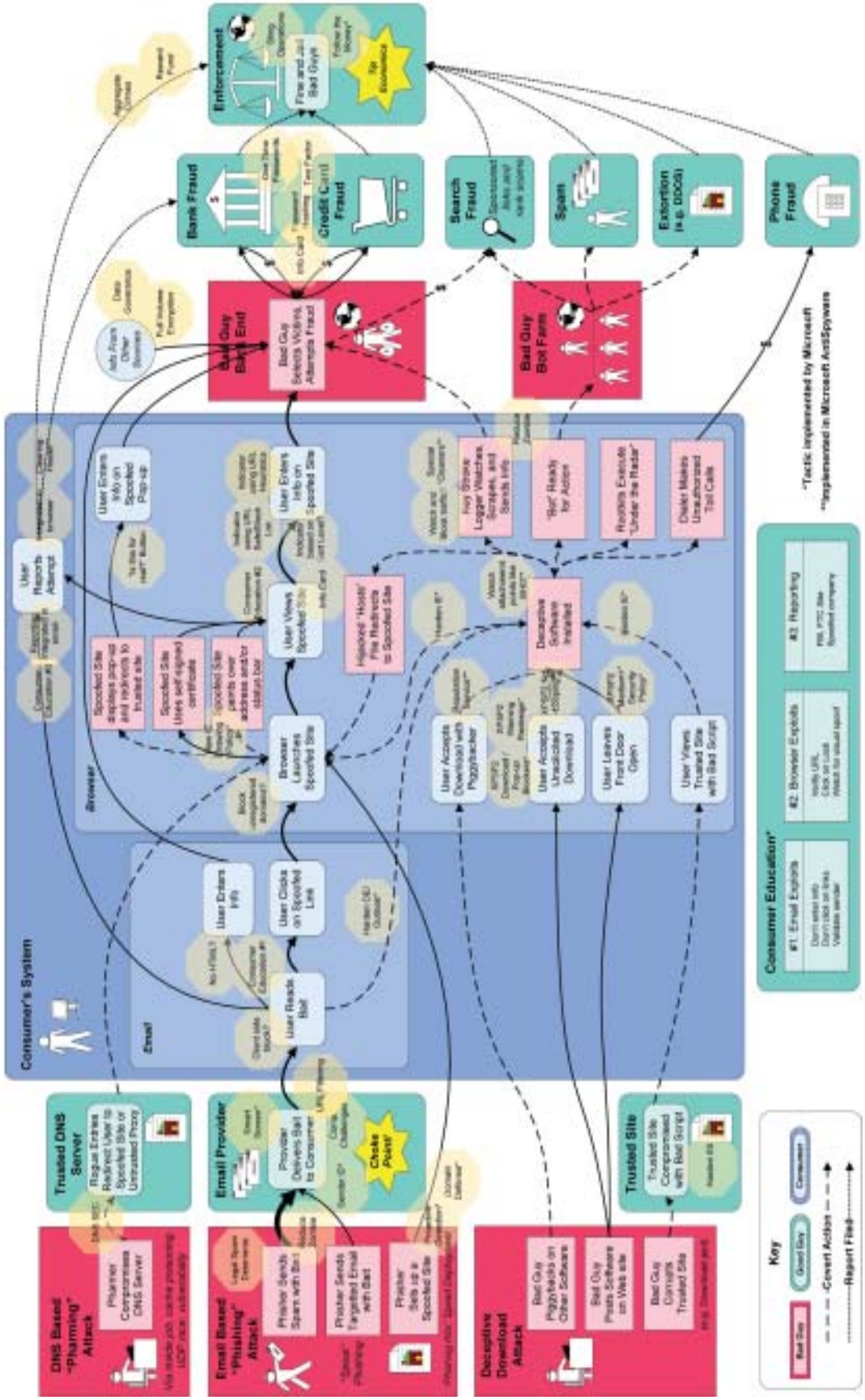
The tactics displayed include these deployed by Microsoft:

- 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.

Tactics – Short and Long Term



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.

Appendix 5

The Lifecycle of the Phisher

1. Plan Attack

Tactic	*Details*	*Notes*
• Collaborate with other bad guys	• Via IRC, Internet Forum • Leverage Barter system	• Bragging rights may come into play • Trust among thieves
• Identify Accomplices	• Other Bad guys and insiders	
• Identify Potential Marks	• Specific Individuals (spear phishing) • Demographics • Products • Merchants • Services • FI's • Channels	
• Decide what data to gather from what sources	• Personal Info from data custodian • PINs from User, …	
• Pick Methods	• Some combination of Phishing, Pharming, Deceptive downloads • Exploit weak security settings • Exploit vulnerabilities in components, systems, and infrastructure (e.g. use XSS, DNS Cache poisoning ...) • Use social engineering tricks: play on fear, greed, naiveté, free, impulse, convenience, reputation, sex	• Spread the pain.

Imagined tactics:

- Pollute software updates
- Mass data compromises
- Breaking encryption
- Corrupting root DNS
- Consumer extortion
- Physical harm or threat
- Become a registrar
- Corrupt credit infrastructure (greed / terror)
- Terrorism
- Stalking

Note: The phishing lifecycle was originally conceived by Chuck Wade of the Financial Services Technology Consortium. His paper that includes that work is at *www.fstc.org/projects/counter-phishing-hase1/FSTC_Counter-Phishing-Solutions_Survey_Summary.pdf.*

2. Launch Attack

Tactic	*Details*	*Notes*
• Send Email with bait	• Via Spammer (botnets)	
• Send IM with bait		
• Deceptive download	• Deceptive pop-up / adware • Unsolicited download • Use UI tricks, associated trust, self-signed certs	• Payload vehicle: executable, rootkit, add-on …
• Navigation hijack	• Hosts file takeover • DNS Server Compromise	• Pharming
• Recruit insiders (or those with access like cleaning staff)	• Flip disgruntled employees or those that need the money	
• Become a rogue client of a data custodian		
• Setup spoofed web sites	• Register cousin domains, disposable domains, and/or rolling domains. • Get certificates to fool user	
• P2P Trojan		
• Send out worms, viruses		
• Piggyback on games		
• Compromise CA		
• Abuse Search Results	• Pay for sponsored links • Rank scam (with botnets)	
• Brute force attacks	• Via botnets.	

Tactic	*Details*	*Notes*
• User enters data on Spoofed Web Site	• With tricks like self signed certs.	
• User enters data in email reply	• HTML form • Clear text reply	
• Man in the middle	• Interloping proxy	
• Steal data from custodian	• Via security or process weakness • Via insider	
• Capture data from user via downloaded keystroke logger, screen scraper	• Detectable or rootkit	
• User provides data over the phone	• Bad guy pretends to be trusted entity (customer service).	
• Get data from user's service providers	• Bad guy pretends to be user, calls customer service.	
• Get user information from public databases	• Court documents, public records	
• "Local" covert collection	• Steal "select" mail from mailbox (leave some to avoid detection) • Break into residence or business • "Skim" credit cards at point of sale. • Over the shoulder camera at ATMs • Insert key stroke logger dongle • Sniff wireless traffic • Via local hardwired network sniffer	• In general "out of scope"; however wireless and network sniffer could be mitigated with encryption and avoiding untrusted proxies
• "Local" overt collection	• Steal wallet (mugging); user knows data is lost.	

4. Research How to Use Data

Tactic	*Details*	*Notes*
• Select best Financial Intuition	• Info need for authorization • Amount of credit it give • Controls for product line, credit card, wire transfer • Fraud detection strategy	

• Select best merchant	• Type of products
	• Method to ship products
	  ○ in/out US
	  ○ non-billable address
	  ○ signature require
	  ○ requires multiple ID's
	• store front authorization method
	• $ threshold at merchant level
	• Automated Number ID (caller ID)
	• Transaction types: online, telephone	

• Select best consumer	• Financial Institutions
	• Next statement date
	• FICO score
	• Credit limit
	• Completeness of personal info
	• Type of access keys
	  ○ SS#
	  ○ Mother's maiden name
	  ○ DOB
	  ○ PINs
	  ○ CC# CVV2
	  ○ Full track CC info
	  ○ User name / passwords
	• Address
		• Build a profile

5. Attempt Crime

Tactic	*Details*	*Notes*
• Financial Fraud (Banks, Credit Cards, Merchants)	• Spread the pain: hit multiple victims across multiple jurisdictions for smaller amounts. Less chance of LE going after them. • Bad guys transfers user's funds to their account at same bank • Bad guy makes unauthorized purchase from merchant • Bad guy makes fraudulent sales using customer reputation • Bad makes counterfeit cards and withdraws money or makes purchases	• Also account hijacking (versus account fraud).

• Extortion	• DDos via Botnet
	• Ransom IP
	  ○ Company secrets
	  ○ Customer data
	• Threaten to hijack domain	

• Terrorism	• Produce counterfeit IDs and docs (e.g. passports) • Take down central services • Erode consumer confidence	

6. Launder Proceeds

Tactic	*Details*	*Notes*
• Convert assets, erase your tracks	• Buy real estate • Foreign bank accounts • Shell companies • Business Bank accounts • Gambling/Porn sites • Inflate inventory / invoices • Recruit unwitting accomplices (job sites) • Re-shippers, bank transfers • Online banks • Digital currency • Jewelry • Insurance polices (cash-in)	

Appendix 6

Bibliography and References

Anti-Phishing Working Group, *http://www.antiphishing.org.*

Consumer Reports Webwatch, "Leap of Faith: Using the Internet Despite the Dangers," Oct., 2005, available at *www.consumerwebwatch.org.*

Elledge, Anthony, "Phishing: An Analysis of a Growing Problem," May, 2004, available at *http://www.sans.org/rr/whitepapers/threats/1417.php.*

Entrust, "Consumer Perspectives of Online Banking Security: Entrust Internet Security Survey" Oct., 2005, available at *http://www.entrust.com/resources/download.cfm/22314.*

Entrust, "Customer Perspectives on Identity Theft and Phishing: Entrust Internet Security Survey," Aug., 2004, available at *http://www.entrust.com/resources/download.cfm/21961.*

Federal Deposit Insurance Corporation, "Putting an End to Account-Hijacking Identity Theft," Dec., 2004, available at *http://www.fdic.gov/consumers/consumer/idtheftstudy/index.html.*

Federal Deposit Insurance Corporation, "Putting an End to Account-Hijacking Identity Theft Study Supplement," June, 2005, available at *http://www.fdic.gov/consumers/consumer/idtheftstudysupp.*

Federal Financial Institutions Examination Council, "Authentication in an Internet Banking Environment," FIL-103-2005, Oct., 2005, available at *http://www.ffiec.gov/pdf/authentication_guidance.pdf.*

Federal Trade Commission, "How Not to Get Hooked by a 'Phishing' Scam," June, 2005, available at *http://www.documation.com/aba/pdfs/016.pdf.*

Honeynet Project & Research Alliance, "Know your Enemy: Phishing; Behind the Scenes of Phishing Attacks," May, 2005, available at *http://www.honeynet.org/papers/phishing.*

Liberty Alliance, "Liberty Alliance Whitepaper: Identity Theft Primer," available at *http://www.projectliberty.org/resources/id_Theft_Primer_Final.pdf.*

Microsoft, Windows Vista Development Center, "Infocard," available at *http://msdn.microsoft.com/windowsvista/building/infocard/default.aspx.*

Ollman, Gunter, Next Generation Security Software Ltd., "The Pharming Guide: Understanding and Preventing DNS-related Attacks by Phishers," July, 2005, available at *http://www.ngssoftware.com/papers/NISR-WP-Phishing.pdf.*

Ollman, Gunter, Next Generation Security Software Ltd., "The Phishing Guide: Understanding and Preventing Phishing Attacks," Sept. 2004, available at *http://www.nextgenss.com/papers/*

To order additional copies of this report, contact the National Consumers League.
Write to 1701 K St, NW, Suite 1200, Washington, DC, 20006.
Phone 202-835-3323, email *pubs@nclnet.org*, or visit *www.nclnet.org*

The National Consumers League, founded in 1899, is America's pioneer consumer organization. Our mission is to protect and promote social and economic justice for consumers and workers in the United States and abroad.

National Consumers League

1701 K Street, NW, Suite 1200 • Washington, DC 20006

phone: 202-835-3323 • fax: 202-835-0747
email: *info@nclnet.org* • Web: *www.nclnet.org*