The Current State of Phishing Attacks

Jason Hong
Carnegie Mellon University
5000 Forbes Ave

jasonh@cs.cmu.edu

1. INTRODUCTION

Phishing is a kind of social engineering attack in which criminals use spoofed emails to trick people into sharing sensitive information or installing malware on their computers. Victims perceive these emails as associated with a trusted brand, while in reality they are the work of con artists. Rather than directly targeting the systems people use, phishing attacks target the people using those systems. Phishing cleverly circumvents the vast majority of an organization's security measures. It doesn't matter how many firewalls, encryption software, certificates, and two-factor authentication mechanisms an organization has if the person behind the keyboard falls for a phish.

On the surface, phishing attacks may seem to be a variant of spam. However, phishing attacks have already led to damaging losses, in terms of identity theft [14,25], loss of sensitive intellectual property and customer information by companies, and loss of national security secrets.

Phishing attacks are also becoming increasingly pervasive and sophisticated. Phishing has spread beyond email to now include VOIP, SMS, instant messaging, social networking sites, and even massively multiplayer games [4,6,35]. Criminals are also shifting from sending out mass emails in the hopes of tricking anyone, to more selective "spear-phishing" attacks that use relevant contextual information to trick specific victims.

Academic and commercial work in phishing is a dynamic area that combines elements of social psychology, economics, distributed systems, machine learning, human computer interaction, and public policy. In 2006, Jakobsson and Myers [20] provided an overview of how phishing works and what countermeasures were available at that time. This article serves as an introduction as well as an overview on the current state of phishing. We start by examining how phishing attacks work. We then discuss why people fall for phishing attacks. We follow with the debate over the actual damage caused by phishing attacks. Afterward, we close with a survey of countermeasures against phishing.

2. ANATOMY OF A PHISHING ATTACK

Phishing attacks have three major phases. The first is potential victims receiving a phish. The second step is the victim taking the suggested action in the message, which is usually to go to a fake web site, but can also include installing malware or replying with sensitive information. The third step is the criminal monetizing stolen information.

2.1 Fake Phishing Emails

Most phishing emails use social techniques rather than technical tricks to fool end-users. For instance, conveying urgency is a well-known method used by criminals to misdirect people's attention [34]. One example is pretending to be a system administrator warning people about a new attack and urging them to install the attached patch. Another example is notifying people that there have been multiple failed logins for their account and that they need to verify their account now or risk the consequences.

Appealing to people's sense of greed is an old technique that has been adapted to the digital world. One phish the author of this article almost fell for was filling out a survey for a bank in return for a small amount of money. The survey seemed innocuous until it asked for a bank account number to deposit funds into. So-called Nigerian 419 scams, which offer "free" money in exchange for helping the sender move large sums of money, also fall into this category. However, these kinds of obvious get-rich-quick scams have been morphing into ones appealing to other emotions. Nowadays, phishers might pose as a relief agency asking for help with a recent natural disaster, or be a random person appealing to prurient interests ("see Britney Spears naked").

More sophisticated *spear-phishing* attacks use specific knowledge about individuals and their organizations. For example, an attack on military personnel might contain an invitation for a general's retirement party, and ask people to click on a link to confirm that they can attend. People who would not normally fall for phish might in this case, because of the context of the situation. Jagatic et al [19] experimented with using social network information, and showed that people were 4.5 times more likely to fall for phish sent from an existing contact over standard phishing attacks. Criminals have been heavily targeting online social networking sites partly for this reason.

Spear-phishing has also been used against high-level targets, in an attack known as *whaling*. For example, in 2008, several CEOs were sent a fake subpoena, along with an attachment that would install malware when viewed [26]. A CACM blog entry outlines several successful spear-phishing attacks in late 2010 and early 2011, with victim including HBGary Federal, the Australian Prime Minister's office, the Canadian government, RSA SecurID, the Epsilon mailing list service, and Oak Ridge National Laboratory [16].

2.2 Setting Up Fake Web Sites

Most phishing attacks try to convince people to go to a fake site where personal information can be collected. To host a fake site, scammers use free web space, use a compromised machine, or register a new domain [27].

When registering new domains, criminals try to get names similar to the site they are impersonating. For example, if impersonating eBay, scammers might register ebay-login.com. Criminals also use *homograph attacks* that exploit the visual similarity of characters. For example, bankofthevvest.com [8] uses two v's to look like a w. Internationalized domain names facilitate this kind of attack, since characters in different language sets may appear identical.

However, in practice, criminals have opted for simpler approaches. One common technique is to put the domain name at the front, for example paypal.com.phishsite.com. Surprisingly, many attacks make no attempt to disguise the destination site, relying on people's lack of understanding of URLs. These simple tactics unfortunately still fool a great number of people.

When phishing attacks were just starting, scammers would create web pages by hand. These web pages tended to be poor in quality, often having misspellings and hotlinks to images on the original site. Nowadays, the majority of phishing sites are created with toolkits. A toolkit might let a phisher specify what legitimate page to copy and where to direct stolen data, and then generate all of the needed content. In 2008, Cova et al [7] identified over 500 working kits. One surprising finding was that over a third of these toolkits would send phished information to a location different than the one specified by the phisher. These kits targeted inexperienced criminals, who would do the work (and bear the risk) in breaking into sites.

When phishing attacks started, law enforcement, industry, and academia were not organized in preventing and responding to these attacks. However, as countermeasures such as blacklisting and takedowns were deployed (these are discussed in more detail in Section 5.1), criminals began introducing new techniques, thus starting an arms race that continues today. The most innovative approach so far is *fast flux*, which uses a large pool of proxies and domain names to hide the true location of a phish. Fast flux makes it harder to blacklist sites since there are many URLs that need to be manually checked. Finding and taking down offending sites is also difficult, since it takes more work to find the actual server. While an average phishing site lasts an average of 62 hours before being taken down, sites using fast flux tended to last an average of 196 [27].

2.3 Monetizing Stolen Information

The last phase of phishing is to monetize stolen information. In some cases, the path is direct, such as when stealing banking credentials. In other cases, the path is convoluted, such as stealing credentials for online games or social networking sites. Criminals have shown high levels of ingenuity here. For online games, criminals might transfer all of a victim's virtual gold to an accomplice and then sell the stolen gold to other players for real money. These attacks are common enough that Blizzard Entertainment, the creator of the popular online game World of Warcraft, sells special authenticators and offers in-game gifts for using them [5].

Phishing on social networks is also somewhat indirect in terms of monetization. One attack is notifying the victim's friends that that person is in trouble and needs money fast. Another attack is to use compromised accounts to spread malware. For example, the Koobface worm sends messages to a victim's friends urging them to go to a site that contains malware. Another attack is to steal the victim's password and break into his email and bank account, which unfortunately works all too well since many people reuse passwords and because existing password reset mechanisms send responses to one's email address.

We've also seen the growth of marketplaces for criminal activities. Previously, phishers might use stolen credentials directly. Nowadays, many phishers sell these credentials through underground networks to other criminals. These purchasers in turn might recruit unsuspecting people as "mules" to launder money and goods, to reduce the risk that the criminals face and to circumvent existing countermeasures. As an example, some "work at home" jobs involve receiving money transfers into the mule's bank account, with the funds actually coming from a hacked bank account. The mule then wires that money to a different account in another country, keeping a small commission. These kinds of activities are illegal, and many people have already been indicted around the world [22].

This evolution in how stolen credentials are monetized is due to specialization and perceived risk. A person who is good at creating phishing sites may not necessarily be good at stealing money from those accounts, especially given greater vigilance by banks and law enforcement. Thus, rather than risk being traced, a phisher might opt to sell stolen information to others who are less risk averse.

Many researchers have examined how criminals trade stolen information on open IRC channels. Interestingly, Herley and Florencio [15] found that criminals often sold credentials for pennies on the dollar, explaining the situation as a classic case of a marketplace for lemons. Given the anonymity of IRC, it is easy for sellers to swindle purchasers by offering fake credentials or selling the same ones multiple times. It is also easy for law enforcement and banks to offer honeypot credentials. As such, it is difficult for buyers to assess the quality of stolen data before buying. This asymmetric information about sellers and their goods leads buyers to dramatically lower what they are willing to pay.

3. WHY DO PEOPLE FALL FOR PHISHING ATTACKS?

We now turn to the question of why people fall for phishing attacks. An unfortunate response by technically savvy individuals is to dismiss end-users as stupid and gullible. This view overlooks the fact that phishers deliberately exploit the poor usability of many interfaces, which offer few cues to assess the legitimacy of emails and web sites. Also, a deeper understanding of end-users' motivations, beliefs, and mental models is essential if we are to build effective countermeasures.

Dhamija et al [8] conducted one of the earliest studies investigating why people fall for phishing scams, asking participants to identify various web sites as legitimate or fake. They found that good phishing sites fooled 90% of participants and that most browser cues were ineffective. Many participants incorrectly judged sites based on its content and how professional it appeared, not realizing that web pages can be easily copied. Dhamija et al also found that even experienced participants had trouble with picture-in-picture attacks, which show screenshots of a web browser at a given site (see Figure 1). Picture-in-picture attacks point to a bigger challenge, which is that many people cannot differentiate between the browser chrome, which can mostly be trusted, and the browser content, where attackers can show anything they want.

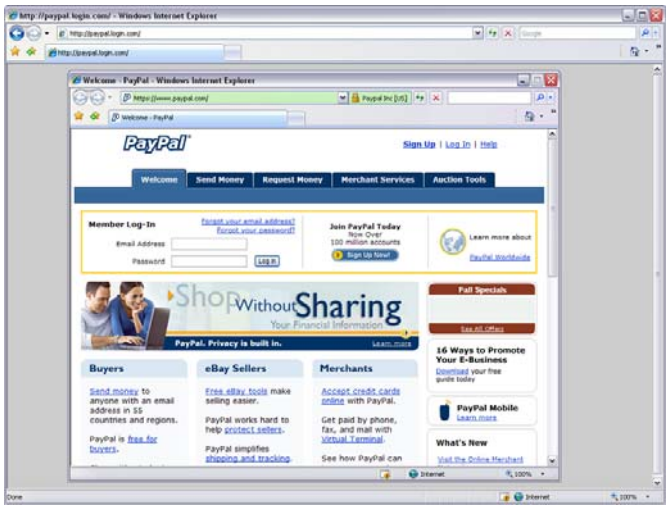

Figure 1. Picture-in-picture phishing attacks show an image of a web browser in the content area of a web browser. These attacks are effective in fooling even experienced users. Figure adapted from [18].

Downs et al [9] conducted a complementary study examining phishing emails. Again, people used basic and often incorrect heuristics in deciding how to respond to emails. For example, some participants reasoned that since the business already had their information, it would be safe to give it again.

Sheng et al [30] conducted a follow-up study, a large scale survey to examine demographics and phishing susceptibility. Surprisingly, they found that women were more vulnerable to phishing than men, primarily due to women having less exposure to technical knowledge. They also found that younger participants between the ages of 18 and 25 performed worse than all other age groups, possibly due to fewer years of experience on the Internet, less exposure to training materials, and less aversion to risk.

4. HOW BAD IS PHISHING?

The Anti-Phishing Working Group is an international consortium of law enforcement, industry, and academics devoted to combating Internet scams and online fraud. In the 4th quarter of 2009, the APWG found over 90,000 unique phishing emails and over 130,000 unique phishing sites, just slightly below the all time high [3].

However, there is a wide variance in the estimates of damage caused by phishing, ranging from $61m [14] to $3b per year [25] of direct losses to victims in the USA. The main problem is a lack of data from banks and other institutions that suffer losses. As such, these estimates are heavily dependent on the methods used and assumptions made.

While there is not yet full agreement regarding the direct damages, there is increasing agreement that the indirect costs of phishing are substantial. One bank our team has spoken to said it cost them about $1 million per attack, in terms of call center costs, recovery costs, and actual money that could not be recovered (which turned out to be relatively small). A more difficult metric to measure is the damage to one's reputation. In presentations on the economics of computer security, Cormac Herley captured this problem succinctly: what is the first thing you think of when you hear the words "Nigerian businessman"?

Estimates of direct costs to the public also don't capture the damage from specialized spear-phishing attacks. In 2011, there were a number of successful high-profile phishing attacks, with victims including RSA, Lockheed-Martin, the Epsilon mailing list service, Gmail, the Australian and Canadian government, and the Oak Ridge National Laboratories [16].

In 2009, the Operation Aurora attacks used spear-phishing and malware to target a number of organizations. In many cases, the attackers successfully stole source code and other intellectual property. However, there are no good estimates as to the damage caused by spear-phishing, due to victims' unwillingness to share information and the difficulty in assessing damages.

5. PHISHING COUNTERMEASURES

Given the risks of phishing, what can individuals and organizations do to protect themselves? From the end-user's perspective, there are three strategies: (1) make it invisible, so that users do not have to do anything different; (2) provide better user interfaces that either make things more obvious to users or offer additional protection; and (3) train end-users to recognize and avoid phishing attacks. All three of these approaches are needed to offer the strongest possible protection against phishing attacks.

5.1 Make it Invisible

The first line of defense is to prevent phishing attacks from reaching end-users. The solutions in this space include filtering phishing emails, blocking fake sites, and taking down fake sites.

5.1.1 Filtering Phishing Emails

There is a large body of research on detecting spam. However, research on detecting phishing emails is sparse, in part because phishing is a relatively new phenomenon, but also because phishing emails look legitimate. Fette et al [11] developed the first email phishing filter, identifying several features that are highly indicative of phishing, for example, having URLs that use different domain names. Researchers have since then explored additional features and machine learning techniques.

An alternative to heuristics is to rely on authentication and verification technologies. Sender Policy Framework (SPF) uses Simple Mail Transfer Protocol (SMTP) to reject forged email addresses. DomainKeys Identified Mail (DKIM) verifies the DNS domain of a sender and the message integrity. However, these technologies have proven difficult to deploy on a large scale and do not provide protection against several kinds of phishing attacks [13]. For example, these technologies focus on preventing email spoofing, but attackers can easily create alternative fake addresses.

5.1.2 Blocking Phishing Sites

Currently, there are two ways of detecting phishing web sites. The first is to use heuristics that examine the URL, HTML, and server characteristics to classify sites. The second is to use manually-verified blacklists.

For heuristics, researchers have investigated a large number of ideas using machine learning. Some examples include looking for patterns in URLs [12], words in the web page [2], and using search engines [39]. Researchers have also looked at linguistic characteristics of web pages, identifying the brand name that a web page claims to be [37]. The effectiveness of these techniques

are reasonable, with true positive rates (correctly identifying a phishing site) of 90% or better, and false positive rates (incorrectly labeling a legitimate site as phish) approaching 1% or less.

There are also several anti-phishing blacklists, the best known of which are operated by Microsoft, Google, and PhishTank.com. These blacklists contain URLs manually verified as phish. Microsoft's blacklist is integrated with Internet Explorer, and Google's blacklist is integrated with FireFox and Chrome, making it so that end-users do not have to take special action to protect themselves. PhishTank's blacklist uses a wisdom-of-crowds approach to identify phish. PhishTank lets people submit potential phish. Once enough other people vote that a submission is a phish, then it is added to their blacklist. Since October 2006, PhishTank has had close to four million votes from volunteers, labeling over half a million phishing sites [28].

There are also several commercial browser addons for blocking phish. Since these tools can be installed in web browsers, it is possible to evaluate their effectiveness. In 2009, Sheng et al [33] examined major blacklists and browser tools and showed that zero-hour protection offered by blacklists had a false positive rate of 0% but a true positive of less than 20%. Even after 12 hours, the best blacklist identified only 83% of phish. They also found that deployed heuristics were somewhat effective in identifying phish, but these heuristics were only used to warn people in the web browser rather than block likely phishing sites.

Sheng et al's work identified a gap between research and industry in terms of true positives. Academic research has focused on heuristics and machine learning techniques which have very good true positives though somewhat high false positives. These heuristics are good at identifying phishing sites that have not been seen before. On the other hand, industry relies primarily on blacklists, which have middling true positives but no false positives. However, these blacklists do not generalize well to future unseen cases, can be slow to respond to zero-hour attacks, and can be easily overwhelmed by automatically generated URLs, a tactic that phishers have already adopted.

In follow-up work, Sheng et al [31] probed this issue by interviewing people in industry, law enforcement, and academia. They found that concern over liability for false positives was the major barrier to deploying more aggressive heuristics. However, the first few hours of an attack are critical, as a substantial fraction of users will have read their email by the time blacklists are updated. Jagatic et al found that during regular work hours, the majority of users who would fall for a phishing attack did so within 8 hours after the start of the attack [19].

Sheng et al identified several ways to ameliorate the situation [31]. One is to clarify the legal issues surrounding false positives. Another is to have a central clearinghouse for phish, rather than piecemeal efforts that take longer to identify phish because of duplicated effort. A third is for researchers to develop better heuristics that minimize false positives. An early example of such heuristics was developed by Xiang et al [38], who observed that many phish are near or exact duplicates of each other because they are generated by toolkits. Thus, once a phish appears on a blacklist, other copies of it can be quickly identified and blocked with virtually no risk of false positives. By using probabilistic matching methods, the obvious countermeasure of adding noise can also be mitigated.

5.1.3 Taking Down Phishing Sites

There are several companies that identify and take down phishing sites. There are also private mailing lists used for sharing information about fake sites as well as finding contact information for specific ISPs and web sites.

Typically, when phishing sites are taken down, end-users who click on a phish are shown a "page not found" error. One innovation developed by APWG and Carnegie Mellon University is to have ISPs and takedown providers replace the phishing page with a training message, thus teaching people who click on phishing emails about these kinds of attacks. The APWG landing page [1] has been in use since Sept 2008 and is available in several languages. As of April 2010, it has been displayed in place of 1285 phishing pages and viewed about 200,000 times [17]. While it is hard to measure the effect of the landing page, it is a step in the right direction in offering multiple ways of protecting people.

5.2 Better Interfaces

The second major strategy for protecting people is to offer better interfaces. Here, we discuss innovations in warnings, support for properly identifying web sites, and authentication.

A general problem with security warnings is that users close them the instant they appear. This is perfectly rational behavior: many warnings are so obtuse that people don't understand what the problem is or what to do. Other warnings annoyingly interrupt what people are trying to accomplish. Warning notifications can also be too subtle, with people not even seeing them.

A *passive indicator* warns of potential dangers without interrupting the user's task. In contrast, *active indicators* force users to notice the warnings by interrupting them. Studies by Wu et al [36] and Egelman et al [10] demonstrated that passive warnings are ineffective in protecting people from phishing scams, as they are easily missed.

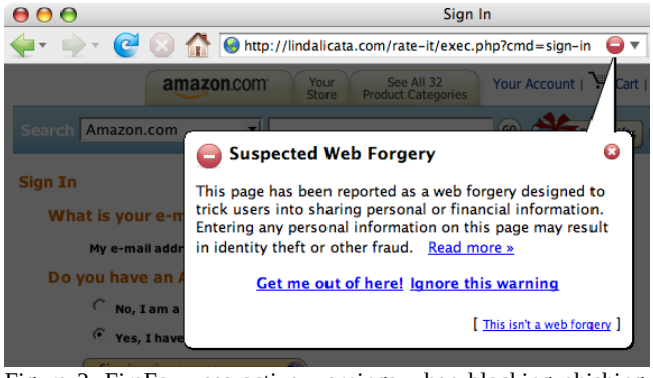

Figure 2. FireFox uses active warnings when blocking phishing pages, which are more effective than passive warnings.

Egelman et al [10] also examined the effectiveness of active anti-phishing warnings in FireFox and Internet Explorer 7. Figure 2 shows an example of FireFox's active warning. Using simulated phishing attacks, they found that no participants fell for phishing attacks when they saw FireFox' warning, but surprisingly, half of the participants using IE did. Egelman et al analyzed the results

using a model from the warning sciences, which describes a flow by which people see, understand, believe, and act on warnings in the physical world. Using this framework, it turned out that most people simply did not "see" the warning in IE, since it looked like a standard "page not found" warning. A few people also did not believe the warning, thinking that Microsoft would not put them at risk, and went on to give sensitive personal information. In response to this work, Microsoft re-designed their anti-phishing warnings in IE8.

There have also been some techniques developed for helping people identify what site they are on. However, it is unclear how much they help in practice. For example, Extended Validation certificates are a special kind of certificate with specific guidelines for verifying that the company purchasing the certificate is legitimate. When a site with an EV certificate is loaded, the browser's URL bar is changed to show the brand name of the site (see Figure 3). However, a study by Jackson et al [18] found that EV certificates were not effective in protecting people from phishing attacks.

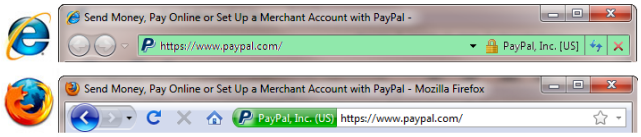

Figure 3. Extended Validation certificates as shown in Microsoft's Internet Explorer and Mozilla FireFox.

SiteKey is a technique used by many financial organizations. Users first select a secret picture. When logging in, users can see if the picture is displayed to verify that they are on the right site. However, Schecter et al [29] found that SiteKey suffers from the same problem as passive indicators, in that the absence (or presence) of an indicator is easily missed or even rationalized away.

An alternative to indicators is to improve the way we sign into sites. Two-factor authentication (2FA) strengthens authentication by requiring two separate ways to prove one's identity. One of the most common forms of 2FA is key fobs that have a periodically changing number that is synchronized with the remote server. Users login by using both their password and this number. While 2FA does increase the cost of conducting phishing attacks, phishers have also developed workarounds, for example switching to real-time man-in-the-middle attacks using malware such as the Zeus Trojan horse.

5.3 Train the Users

The third way of protecting people from phishing scams is to train them. Training is an essential part of computer security but arguably the least popular approach, given the inherent challenges in motivating people to be secure, as well as the fact that training does not guarantee complete protection (though in reality, neither do other solutions today).

Many web sites offer advice on how to identify phishing sites. Past studies by Kumaraguru et al [24] have shown that this kind of information is useful in helping people identify fake web sites, but only if you can get people to read the material. In a different study [23], Kumaraguru et al found that simply emailing anti-phishing material was not effective, because people were habituated to receiving these kinds of warnings and thought that they already knew how to protect themselves.

There have been two lines of research to address these problems. The first is micro games that teach people about phish. Micro games are a popular format for games that can be played for short periods of time. Sheng et al developed a micro game for computer security called Anti-Phishing Phil [32] (see Figure 4). Phil teaches people about browser address bars, domain names, and phishing pages, and then tests them on what they learned. Phil incorporates many ideas from learning science, a body of empirical research that seeks to understand the best methods for learning and retention of knowledge. An example principle is conceptual-procedural, which states that high-level concepts should be interleaved with concrete procedures on how to achieve given tasks. An evaluation of Phil with over 4500 people demonstrated that it improved novices' ability to identify phish by 61% while also dramatically lowering false positives.

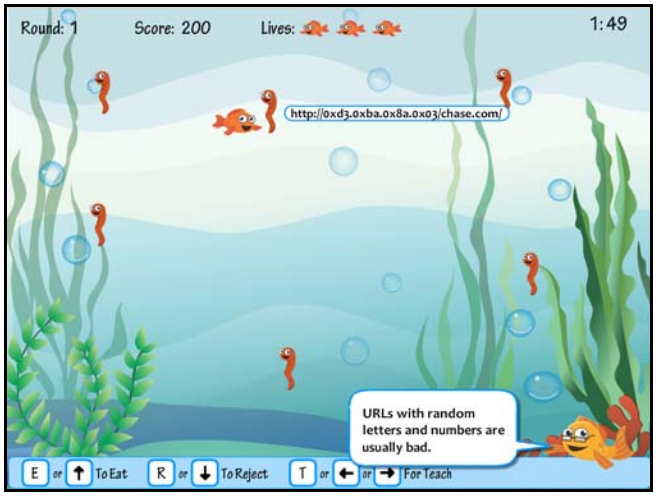

Figure 4. Anti-Phishing Phil is a micro game that teaches people how to identify phishing scams.

The second approach to training is embedded training, which teaches people in the specific context of use in which they would normally be attacked. Embedded training is in contrast to other forms of security training, which might take place in a classroom and give people few opportunities to test what they learned. Kumaraguru et al [24] developed an embedded training system named PhishGuru, which sends simulated phishing emails to people. If participants fall for one, they see an intervention that teaches them about phishing and how to protect themselves. In a study with over five hundred participants, Kumaraguru et al found that this approach led to a 45% reduction in falling for phish even a month after being trained. This finding helped lead to the creation of the APWG landing page [1], as described earlier.

6. Conclusions

Throughout this article, we have emphasized the tenacity and creativity of criminals. Unfortunately, this inventiveness is a trend that will only continue. It is also likely we will see an increase in spear-phishing and whaling attacks, as phishers continue to look for vulnerable targets with valuable information.

Phishing also causes new problems for organizations, as they blur traditional security perimeters. One's lawyers and accountants

may be attacked to surreptitiously gain access to documents. Facebook and other social media provide more contextual details that can be used for spear-phishing attacks. An employee falling for a phish in one context may cause a headache for your organization because of reused passwords. Finally, instant messaging, VOIP, SMS, and other new ways of communicating offer criminals new vectors for sending attacks.

On the positive side, law enforcement, industry, and academics are becoming better organized, in terms of reporting phishing attacks, sharing information, analyzing data to identify trends, and focusing resources. There are more organizations now devoted to combating online fraud, including the APWG, the National Cyber-Forensics and Training Alliance (NCFTA), and the Internet Crime Complaint Center (IC3). There are also initiatives for educating people about phishing scams, for example StaySafeOnline.com. Law enforcement has been stepping up efforts in gathering evidence and cooperating with international partners in shutting down phishing sites and phishing gangs. Legislators have also been passing new laws to explicitly spell out what phishing is and what the penalties are for committing this crime, such as California's Anti-Phishing Act of 2005 [21], though these laws face many of the same challenges that anti-spam laws do, in terms of attackers being outside of one's jurisdiction, the sheer quantity of attacks, and limited resources from law enforcement.

Phishing will continue to be an arms race. Since any communication medium can be used for phishing, it is also a problem that can never truly be solved. Moving forward, the best we can hope for is to blunt the worst parts of phishing and continue to work on better ways of preventing, detecting, and responding to this new form of a very old crime.

7. ACKNOWLEDGMENTS

Special thanks to the Supporting Trust Decisions group and members of Wombat Security Technologies for their contributions and comments.

8. REFERENCES

1. APWG. APWG & CMU's Phishing Education Landing Page. 2008. http://education.apwg.org/r/en/.

2. Abu-Nimeh, S., Nappa, D., Wang, X., and Nair, S. A comparison of machine learning techniques for phishing detection. *The Anti-Phishing Working Group's 2nd Annual eCrime Researchers Summit (ECRS 2007)*, (2007), 60.

3. Anti-Phishing Working Group. *Phishing Activity Trends Report: 4th Quarter Report*. .

4. Arthur, C. Facebook hit by phishing attack. *The Guardian*, 2009. http://www.guardian.co.uk/technology/2009/apr/30/facebook-phishing-scam.

5. Blizzard. Battle.net Authenticator FAQ. http://us.blizzard.com/support/article.xml?locale=en_US&articleId=24660.

6. Cavalli, E. World of Warcraft Phishing Attempts on the Rise. *Wired Magazine*, 2009. http://www.wired.com/gamelife/2009/04/world-of-warcraft-phishing-attempts-on-the-rise/.

7. Cova, M., Kruegel, C., and Vigna, G. There is no free phish: an analysis of "free" and live phishing kits. *Proceedings of the 2nd conference on USENIX Workshop on offensive technologies (WOOT 2008)*, (2008).

8. Dhamija, R., Tygar, J.D., and Hearst, M.A. Why phishing works. *Conference on Human Factors in Computing Systems (CHI 2006)*, (2006), 581.

9. Downs, J.S., Holbrook, M.B., and Cranor, L.F. Decision strategies and susceptibility to phishing. *Symposium on Usable Privacy and Security (SOUPS 2006)*, (2006).

10. Egelman, S., Cranor, L.F., and Hong, J.I. You've been warned: an empirical study of the effectiveness of web browser phishing warnings. *Conference on Human Factors in Computing Systems (CHI)*, (2008), 1065-1074.

11. Fette, I., Sadeh, N., and Tomasic, A. Learning to Detect Phishing Emails. *Proceedings of the 16th International World Wide Web Conference (WWW2007)*, (2007).

12. Garera, S., Provos, N., Chew, M., and Rubin, A.D. A framework for detection and measurement of phishing attacks. *Workshop On Rapid Malcode*, (2007), 1.

13. Görling, S. An overview of the Sender Policy Framework (SPF) as an anti-phishing mechanism. *Internet Research 17*, 2 (2007), 169 - 179.

14. Herley, C. and Florencio, D. A Profitless Endeavor: Phishing as a Tragedy of the Commons. *New Security Paradigms Workshop (NSPW 2008)*, (2008).

15. Herley, C. and Florencio, D. Nobody Sells Gold for the Price of Silver: Dishonesty, Uncertainty and the Underground Economy. *Workshop on the Economics of Information Security (WEIS 2009)*, (2009).

16. Hong, J.I. Why Have There Been So Many Security Breaches Recently? *Blog@CACM*, 2011.

http://cacm.acm.org/blogs/blog-cacm/107800-why-have-there-been-so-many-security-breaches-recently/fulltext.

17. Hong, J.I. Statistical Analysis of Phished Email Users, Intercepted by the APWG/CMU Phishing Education Landing Page. *APWG CeCOS*, 2010. http://www.antiphishing.org/events/2010_opSummit.html.

18. Jackson, C., Simon, D.R., Tan, D.S., and Barth, A. An Evaluation of Extended Validation and Picture-in-Picture Phishing Attacks. *The 11th International Conference on Financial Cryptography (FC2007)*, (2007).

19. Jagatic, T.N., Johnson, N.A., Jakobsson, M., and Menczer, F. Social phishing. *Communications of the ACM 50*, 10 (2007), 94.

20. Jakobsson, M. and Myers, S. *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*. Wiley-Interscience, 2006.

21. Keizer, G. California Enacts Tough Anti-Phishing Law. *Information Week*, 2005. http://informationweek.com/news/171202672.

22. Krastev, N. U.S. Indicts Dozens From Eastern Europe In Internet Theft Scheme. *Radio Free Europe*, 2010. http://www.rferl.org/content/US_Indicts_Dozens_From_Eastern_Europe_In_Internet_Theft_Scheme/2173545.html.

23. Kumaraguru, P., Rhee, Y., Sheng, S., et al. Getting users to pay attention to anti-phishing education: evaluation of retention and transfer. *The Anti-Phishing Working Group's 2nd Annual eCrime Researchers Summit (ECRS 2007)*, (2007), 70.

24. Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L.F., and Hong, J.I. Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology (TOIT) 10*, 2 (2010).

25. Litan, A. *Phishing Attack Victims Likely Targets for Identity Theft*. 2004.

26. Markoff, J. Larger Prey Are Targets of Phishing. *New York Times*, 2008. http://www.nytimes.com/2008/04/16/technology/16whale.html.

27. Moore, T. and Clayton, R. Examining the impact of website take-down on phishing. *The Anti-Phishing Working Group's 2nd Annual eCrime Researchers Summit (ECRS 2007)*, (2007).

28. PhishTank. PhishTank Stats. 2011. http://www.phishtank.com/stats.php.

29. Schechter, S.E., Dhamija, R., Ozment, A., and Fischer, I. The Emperor's New Security Indicators: An evaluation of website authentication and the effect of role playing on usability studies. *IEEE Symposium on Security and Privacy*, (2007).

30. Sheng, S., Holbrook, M.B., Kumaraguru, P., Cranor, L.F., and Downs, J.S. Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions. *Conference on Human Factors in Computing Systems (CHI 2010)*, (2010), 373-382.

31. Sheng, S., Kumaraguru, P., Acquisti, A., Cranor, L.F., and Hong, J.I. Improving phishing countermeasures: An analysis of expert interviews. *The 4th APWG eCrime Researchers Summit (2009)*, (2009).

32. Sheng, S., Magnien, B., Kumaraguru, P., et al. Anti-Phishing Phil: the design and evaluation of a game that teaches people not to fall for phish. *The 3rd Symposium on Usable Privacy and Security (SOUPS 2007)*, (2007), 88.

33. Sheng, S., Wardman, B., Warner, G., Cranor, L.F., Hong, J.I., and Zhang, C. An Empirical Analysis of Phishing Blacklists. *Conference on Email and Spam (CEAS 2009)*, (2009).

34. Stajano, F. and Wilson, P. *Understanding scam victims: Seven principles for systems security*. 2009.

35. Verisign. *Fraud Alert: Phishing — The Latest Tactics and Potential Business Impact*. 2009.

36. Wu, M., Miller, R.C., and Garfinkel, S. Do Security Toolbars Actually Prevent Phishing Attacks? *Human Factors in Computing Systems (CHI 2006)*, 601–610.

37. Xiang, G. and Hong, J.I. A hybrid phish detection approach by identity discovery and keywords retrieval. *International World Wide Web Conference*, (2009), 571-580.

38. Xiang, G., Rose, C., Hong, J.I., and Pendleton, B. A Hierarchical Adaptive Probabilistic Approach for Zero Hour Phish Detection. *15th European*

Symposium on Research in Computer Security (ESORICS 2010), (2010).

39. Zhang, Y., Hong, J.I., and Cranor, L.F. Cantina: a content-based approach to detecting phishing web sites. *International World Wide Web Conference*, (2007), 639.