Chapter 3

Improving Phishing Countermeasures: An Analysis of Expert Interviews

This chapter is joint work with Alessandro Acquisti, Lorrie Cranor, Jason Hong, and Ponnurangam Kumaraguru. An earlier version of the content in this chapter is published at 2009 eCrime Researchers Summit [126].

3.1 Introduction

As the battle against phishing continues, many questions remain about where stakeholders should place their efforts to achieve effective prevention, speedy detection, and fast action. Do stakeholders have sufficient incentives to act? What should be the top priorities for the anti-phishing community?

To provide insights into these questions we conducted 31 in-depth interviews with anti-phishing experts between May 2008 and May 2009. We selected experts from academia, Computer Emergency Response Team (CERT) centers, the Anti-Phishing Working Group (APWG) officers, law enforcement, and key industry stakeholders. We sought their expertise on the current and future state of phishing attacks, countermeasures that should be implemented to fight phishing more effectively, and incentives that various stakeholders have in their fight against phishing.

The experts we interviewed agreed that phishing is evolving into a more organized effort. It is becoming part of a larger crime eco-system, where it is increasingly blended with malware and used as a gateway for other attacks. Some of the experts suggested that incentives for fighting phishing may be misaligned, in the sense that the stakeholders who are in a position to have the

largest impact do not have much incentive to devote resources to anti-phishing efforts. In terms of countermeasures, experts identified improving law enforcement and shutting down money trails as top priorities. They also identified operating systems vendors, web application providers, browsers, and Internet service providers as stakeholders with key technology influence on phishing. Finally, experts agreed that education is an important factor that is not emphasized enough; however, they did not agree on the extent of the impact that education may have. We present these findings and a set of recommendations to improve countermeasures.

Although previous reports have studied phishing and issued recommendations, to the best of our knowledge this is the first study that synthesizes the opinions of experts from different fields, and examines the incentives of various stakeholders to contribute to anti-phishing efforts.

3.2 Related Work

In response to the growing phishing problem, government agencies, industry groups, and consumer groups have conducted studies and issued recommendations [35, 52, 100, 105].

The Financial Services Technology Consortium's report is the first report that analyzed how phishing works by articulating the life cycle of phishing. It also encouraged financial institutions to assess the costs and risks associated with phishing, develop better intelligence on phishers through improved sharing, and invest and adopt in better mutual authentication. However, the report did not issue recommendations for non-financial institutions who also have high stakes in the phishing problem [35].

The Identity Theft Technology Council report also analyzed different phases of phishing and recommended a set of 21 technical countermeasures citeiitc:phishing-report. We selected a subset of recommendations from this report as a starting point for discussion in our expert interviews. However, we updated the set to address non-technical countermeasures as well as new and evolving threats that were not discussed in the report. In addition to discussing the set of recommendations, we also studied the incentives that stakeholders have to implement them as well as how the incentives can be increased.

Table 3.1 Phishing stakeholders. Primary victims suffer direct losses from phishing. Infrastructure providers have technical capabilities to mitigate the problem. For-Profit protectors sell solutions to primary victims and infrastructure providers. Public protectors include law enforcement officials, computer emergency response teams, and academic researchers.

Categories	Examples of key stakeholders	Roles
Consumers	–	Primary victims
Organizations	Military, Universities, Corporations	
Financial Institutions	Bank of America, Citibank, Paypal	
Merchants	Online merchants (eBay, Amazon), offline merchants	
Registrars and Registries	GoDaddy, Verisign	Infrastructure providers
Internet Service Providers	AT&T, Comcast, AOL, Universities	
Email Providers	Gmail, Yahoo!Mail, Hotmail	
Browsers	Internet Explorer, Firefox, Safari	
Software Vendors	Symantec, RSA, MarkMonitor, Cyveillence	For-profit protectors
Law Enforcement	Federal Bureau of Investigation (FBI), Secret Service state and local enforcement	Public Protectors
Computer Emergency Response Teams	CERT-CC, CSIRTs	
Academia		

In addition to these reports, the Anti-Phishing Working Group (APWG) has issued a set of best practices and recommendations for hacked website owners [8], registrars [6], and ISPs and mailbox service providers [85]. Each of these reports focus narrowly on one particular area. In our analysis, we analyzed the phishing issue holistically and asked our experts to prioritize their recommendations based on their importance and effectiveness.

3.3 Stakeholders

Phishing involves many stakeholders, including consumers, financial institutions, online merchants, Internet Service Providers (ISPs), mail client and web browser vendors, and law enforcement. In this paper, we have classified stakeholders into the following categories: *primary victims,*

infrastructure providers, for-profit protectors, and public protectors. Table 1 describes these stakeholders and their roles. We used it to select experts and structure our interviews.

3.3.1 Primary victims:

In most cases, consumers, organizations, financial institutions, and merchants are direct targets of phishing attacks. Each of them is negatively affected by phishing in a different way.

Consumers who fall for phishing can potentially become victims of identity theft: they not only suffer monetary loss, but also psychological costs (e.g. fear, anxiety). Generally speaking, consumers fall for phishing because they have incorrect mental models about what constitutes trustworthy emails and websites [23] and they are susceptible to manipulation and social engineering. Organizations such as the military and corporations worry that phishing may lead to further compromise of credentials that can be used to steal key intellectual property or conduct corporate espionage.

Financial institutions lose money from fraud conducted with credentials acquired through phishing. They may also suffer indirect losses such as increased customer service cost, damage to reputation, etc. Some argued that indirect losses are much greater than the direct losses, although this claim has not been independently verified. Merchants lose money because these financial institutions eventually charge them for the fraudulent transactions.

In general, these entities are most impacted by phishing, and have the strongest incentive to protect against phishing. However, as shown later in the result section, some of them have limited capabilities to counter phishing attacks.

3.3.2 Infrastructure providers:

Internet service providers, email providers, browsers, domain name registrars, and registries are infrastructure providers. In most cases, phishers do not go after these providers for their money; instead, they seek to gain access to the entities' infrastructures so that phishers may launch their attacks. For example, phishers register fake domain names with registrars. Phishers use compromised machines from Internet Service Providers as part of a botnet to launch phishing campaigns,

sending emails to end user mailboxes or compromising mail provider accounts to send phishing emails. These stakeholders are important to study, as they are in a better position than most victims to protect against phishing. However some infrastructure providers do not lose money from phishing, so they may not have sufficient incentives to devote resources to combating phishing. In our interview study, we asked experts what these stakeholders can do and examined whether or not they have incentives to do so.

3.3.3 For-profit protectors:

Certain organizations actually benefit from phishing because it is an opportunity to develop and sell products to other stakeholders. These include companies that sell spam filters and anti-virus software, as well as companies that take down phishing websites. As they are the front-line defenders against phishing, we selected a few of our experts from these companies. Table X also However, as they make money from combating phishing, it could somewhat bias their recommendations. We discuss these potential biases in detail in the methodology section.

3.3.4 Public protectors:

In contrast to anti-virus vendors and spam filter companies who are for-profit protectors, law enforcement, computer emergency response teams (CERT), and academics are public protectors.

There are some para-organizations such as the Anti-Phishing Working Group (APWG) and the Message Anti-Abuse Working Group (MAAWG) that aim to bring different stakeholders together to fight more effectively against phishing. Some of the experts we interviewed hold positions in these organizations. However, we did not consider these organizations as separate stakeholders in our analysis.

3.4 Methodology

During May 2008 and May 2009, we conducted in-depth interviews with 31 experts involved in phishing countermeasures. In this section, we discuss how we selected the experts, the interview process, and the steps taken to analyze the data.

Table 3.2 Anti-phishing experts interviewed. For confidentiality purposes, all partipants are anonymized.

Affiliation	No. of Experts
CERT	4
Academic researchers	5
APWG officers	3
Law enforcement	5
Registrars, Registries	3
Financial institutions	4
Internet service providers	3
Browser vendors	1
Other experts	3
Total	31

3.4.1 Recruitment and Participants

We recruited experts in several ways. First, we compiled a list of frequent speakers from 2004 through 2007 APWG member conferences and generated a list of well-known experts in academia and industry. To recruit law enforcement officers, we attended the 2008 Digital PhishNet conference. To recruit experts in Internet service providers, registrars, and technology vendors, we solicited recommendations from APWG's Internet Policy Committee (IPC), which is composed of 90 members from various stakeholders. Finally, we recruited additional interviewees through our own network of contacts. In order to obtain a variety of views, we tried to select candidates from different organizations who worked at different levels of company hierarchy.

We recruited a total of 31 experts responsible for, or knowledgeable of, operational or policy decisions with regard to phishing and malware prevention in their organizations. Most of the interviewees chose to remain anonymous. Table 2 shows the organizational profiles of these experts. 67% of the experts interviewed had a technical background, 20% had a policy or business background, and the remainder had a background in law or law enforcement.

In addition to the 31 experts interviewed, we also had a short interview with a legal expert on the question of liability for false positives.

The sample size of 31 balances the resource-intensive demands of in-depth interviews and analysis against the marginal return of new insights from additional participants. We had multiple participants who shared similar views on most of the topics we discussed in our interviews, suggesting that theoretical saturation was likely achieved, even with our small sample.

3.4.2 Interview Protocol

We used a semi-structured interview protocol. The protocol allowed us to ask structured questions that enabled comparable responses across participants, while providing the interviewer flexibility in drilling down on areas of particular relevance to each participant [115].

Each interview typically lasted 60 minutes (min =25, max = 90) and was recorded for transcription. Some interviews were conducted in-person, while others were conducted over the phone. We began each interview by asking each expert to describe his or her background and responsibilities. We then asked a set of open-ended questions about how phishing impacts their organizations, amount of losses, current and future state of phishing, and the effectiveness of current countermeasures. We then asked them specifically to comment on a set of 31 recommendations broken into six categories that we compiled through our research. Experts prioritized the recommendations in each category and provided feedback on them. Finally, at the end of each interview, we asked experts to provide additional recommendations, and if they did, we summarized and added them to our list of recommendations and asked experts about them in subsequent interviews.

3.4.3 Analysis

After completing each interview, we transcribed the audio recordings and recorded the answers to each question in a spreadsheet. We then analyzed the interview results and synthesized a series of findings and accompanying recommendations.

In our analysis, we synthesized experts' opinions by selecting themes that recurred most frequently across all interviews. We also report some of the comments that were discussed by only one or two experts, but that we found particularly useful in thinking about phishing countermeasures.

3.4.4 Limitations

Before turning to the empirical findings, it is important to note the scope and limitations of this study.

Most of the experts interviewed were from the US, but we also had some from Japan, Hong Kong, Italy and Britain. Thus, while there is some international representation, for the most part these interviews represent a US-centric view.

It is also reasonable to assume that this set of interviewees was influenced by some degree of self-selection. Registries, for example, are more likely to respond favorably to an interview request about their phishing countermeasures if they have policies in place that are at least on par with other registries, if not better. With that said, some of the organizations we interviewed are *not* known for having outstanding records with regard to phishing.

Our findings reflect how stakeholders themselves describe what they are doing and why. In other words, we report on the perceptions of the interviewees, not the independent assessment of their actions and the factors driving them. Whenever possible, we did crosscheck information provided to us against the information from other interviews and against publicly available data, such as reports, surveys and research publications.

In addition, the interviewees are not experts in all areas, and they have biases of their own. For example, take-down vendors are more likely than others to recommend that more efforts should be focused on take-downs. We address this in a few ways. During our interviews, we let interviewees select the two to three areas in which they are most experienced to comment on. Whenever possible, we asked them to provide evidence to support their positions and recommendations, and in some instances, we tried to probe experts further by presenting a counter-argument for experts to respond to.

Despite these limitations, our approach is an important complement to purely technical analysis of phishing (e.g. [52]). First, our interview approach synthesizes the opinions of experts from many different fields. It would be difficult to obtain this information through other methods. Second, our interviews examine the incentives of various stakeholders to contribute to anti-phishing

efforts, an important consideration in producing workable solutions. For example, past qualitative research in information security investments has proven to be a valuable complement to the knowledge generated through quantitative modeling or analysis (e.g. [119], [117]).

In the next sections we present the findings from our interviews. We classified our findings into four topical categories: the evolving threat, stakeholder incentives, what stakeholders should do, and law enforcement and education. We also provide a set of recommendations based on these findings. Table 3.3 presents the high-level findings from the interviews.

Finally, this paper does not discuss some relevant technologies such as email authentication (SPF, DKIM), extended validation certificates. These technologies were rarely mentioned by the experts we interviewed and we found no consensus on the effectiveness of these technologies.

3.5 Results

3.5.1 Evolving threat

Table 3.3 High-level findings.

Categories	**Findings**
Evolving threat	A. Phishing is evolving to be more organized and targeted. It is becoming part of a large crime eco-system. B. Phishing and malware are increasingly blended together.
Stakeholder incentives	A. Stakeholders have varying incentives to fight phishing. B. Sometimes stakeholder incentives are misaligned.
What stakeholders should do	A. Operating systems vendors, web application providers, browser vendors, and Internet service providers are stakeholders with key technology influence over phishing. B. Organizations are conservative about filtering and warning about phish because they are worried about false positives. C. Registries and registrars can play an important role in fighting against phishing.
Law enforcement and education	A. Law enforcement should be emphasized; but law enforcement lacks the necessary tools, personnel, and resources to catch phishers. B. Shutting down money trails is very important to defeat phishers. C. Education and awareness are important factors that are not emphasized enough. However, not all experts agree on the effects of education.

Phishing is evolving to be more organized and targeted. It is increasingly used as a gateway to other attacks.

We asked experts to describe the phishing attack trends they have observed and predict how phishing attacks will continue to evolve. Experts observed that phishing attacks are becoming more organized. One technical expert in law enforcement explained:

> These are criminal organizations that exist that perpetrate these types of fraud. It is not likely your teenage hacker like in the old days. They are criminal organizations with business plans and contingency plans. They are typically involved in other crimes besides phishing. It could be malware, it could be hosting other content, possibly child pornography, and it could be the old 419 scams and mule schemes. What we see is that these types of folks don't just do one thing. They either do other things or work with groups that do other things.

One example of an organized group mentioned frequently by experts is the rock phish group, which is believed by many experts to originate from a group of phishers in Eastern Europe. One academic researcher said 88% of the one million URLs his research group processed in October 2008 had rock phish characteristics. Published studies have also analyzed the frequency of fast flux phishing attacks. For example, Moore et al. found that 68% of the phishing emails in their study sample were sent using fast flux techniques [95].

Another trend that experts observed is that phishing is increasingly used as a gateway to other attacks. One expert from a major browser vendor said:

> We are seeing a lot of blended attacks, where a piece of the infrastructure is a phishing attack, but that's not necessarily the end goal. . . . It is malware, it's affiliate advertising, it's spam as form of advertising, scams, and ring tones, there is a number of ways to monetize. But the goal is to look for not only the traditional stuff but ways to monetize groups of users. And you know, stealing a password is a pretty good way to tag into real people, real networks, so we see the social network site is being targeted very heavily, and it's the result of that.

One of the experts from a major US bank agreed, and added that his institution had been seeing an increasing amount of cross channel fraud, where credentials harvested through traditional phishing attacks were being used to commit fraud in other channels such as telephone banking.

Finally, experts agreed that phishing attacks are evolving into be more targeted attacks, which are very effective and harder for spam filters to detect. Recent phishing attempts to defraud top executives are examples of these targeted attacks. Past research has demonstrated the effectiveness of spear phishing attacks. For example in a study at Indiana University, 16% of participants fell for regular phishing emails, but 72% fell for spear-phishing emails [53].

Phishers kept moving to new targets as traditional targets of phishing attacks have devised response plans. Some experts thought that small and medium brands would become the next victims. Others speculated that credit unions, social network sites, and Xbox live accounts would be increasingly targeted.

Phishing and malware are increasingly blended together.

Experts mentioned that malware attacks that use phishing emails are on the rise and pose a serious threat. One academic researcher framed phishing and malware as different expressions of the same problem. He said:

> You will see social engineering aspects of malware and high automation aspects of phishing. At some point, it might be hard to tell them apart . . . To the attackers, it doesn't matter what they use. They know social engineering has an effect on the end user, they know script and code and have some effect on the user's machine. It is just a matter of putting what they know and what they have.

Some of the experts we interviewed believe that malware now poses a bigger threat than phishing. Their reasoning is that due to vulnerabilities in operating systems and web applications it is easy for computers to get infected with malware, and that even security-conscious users may have difficulty avoiding infection.

3.5.2 Stakeholder incentives

Stakeholders have varying incentives to fight phishing.

We asked experts how phishing impacts their organizations. Their responses provided insights into their organizations' incentives to fight phishing.

In general, we found that the primary victims have incentives to invest resources to protect against phishing as they suffer direct losses from phishing. Nonetheless, there is evidence that not all potential primary victims have made this investment. One expert from academia said that many midsize and smaller banks he talked to did not have a strategy for phishing, as they had never been targets: "There is low chance that those banks are targeted, but if they are targeted, they could lose a lot of money."

The stakeholders who do invest in anti-phishing protection sometimes feel that they are carrying a disproportionate share of the burden. One expert said:

> After speaking to many service providers such as financial institutions, there is one thing that stands out very clearly, a sense of "injustice," that they are often carrying the cost for something they have no ability control or even measure. For example, financial service providers, they are not able to determine if their clients, the end users, have appropriate anti-virus software or not. So one way to align the incentives is for service providers be able to audit the security posture of user clients.

Our interviews revealed information on the incentives of several types of stakeholders, described below.

Financial institutions. Financial institutions are among the primary victims of phishing as they lose money from fraud committed with compromised accounts. Currently, over 79% of phishing attacks target financial institutions [131]. A major US bank told us that over the past 12 months, their loss due to phishing and malware was $4.5 million, accounting for 25% of their fraud loss through online channels.

Financial loss and regulatory oversight are both drivers for adopting anti-phishing technologies. One electronic fraud risk manager from a major bank in Asia mentioned that their loss to phishing

and electronic crime is less than 1% of their overall fraud loss. However, they still invest a lot of money in anti-phishing efforts because regional regulators demand two-factor authentication and require comprehensive analysis for electronic crime incidents. Thus, stakeholder incentives may vary depending on local regulations.

Finally, reputation was also mentioned by some as a factor. This same risk manager mentioned that another major reason his bank was spending a lot of money in this area was that bank management wanted to position their electronic banking service as the safest in the region.

It is worth noting the inherent difficulty of obtaining accurate phishing loss figures for financial institutions. It is difficult to separate phishing from other electronic fraud, such as malware. Furthermore, such losses impact a variety of different parts of a company, such as customer service, and thus may not be fully accounted for by the fraud department. Finally, it is difficult to quantify indirect loss such as damage to one's reputation.

Even if financial institutions have accurate phishing loss estimates, they often do not have incentives or regulatory requirements to disclose them. They may prefer not to disclose these losses due to fear of brand erosion due to negative publicity. This leads to a wide range of loss estimates that differ by an order of magnitude (e.g. [92] vs. [43]).

Merchants. Merchants lose money because financial institutions eventually charge them back for fraudulent transactions. When a phisher makes a purchase using a stolen credit card, the credit card company usually charges the merchant for the loss. With online and telephone transactions known as "card-not-present" transactions, merchants assume this liability directly if cardholders dispute a charge. The Merchant Risk Council estimates that merchants who manage their risk well still lose about 1% of their revenue to credit card fraud [84].

Internet Service Providers: The ISPs we interviewed all considered phishing as part of the spam problem, which is their number one concern. Since phishing usually represents less than 1% of the spam they receive, their typical response is to filter out phish with spam. For example, one University ISP expert said, "We filter as much as we could and we would like [our users] not be sending their credit card and social security numbers online, but we don't see that as our

responsibilities to protect those numbers, it is their personal data to protect." Other experts from academia echoed this sentiment as well.

ISPs do have an incentive when phishing targets their own mail systems. These phishing attacks typically seek to compromise users' webmail accounts hosted by these ISPs and use them to send out more spams. ISPs have the incentive to ensure mail flows properly and avoid having their mail servers being blocked by blacklists.

When it comes to fixing compromised machines that are often used as part of a botnet to send out phishing emails, ISPs currently do little. These compromised machines sometimes form a fast flux network, in which a domain name that phishers use has multiple IP (Internet Protocol) addresses assigned to it. The phishers switch those domains quickly between the addresses (often compromised machines) so that it is not as easy to find or shut down the phishing sites. One expert from a major US ISP recognized that compromised PCs cause major problems, and told us that close to 10% of their customers' machines were infected with malware. However, when asked why his company does not remove these computers from the network he said, "Well, they are paying [a monthly fee] . . . for Internet access."

Experts from other ISPs made similar comments and noted that fixing infected computers can be costly. Infected computers may need to have their operating systems reinstalled. One expert from an ISP mentioned that customer service is the largest cost for the ISP. However, most experts who did not work for ISPs identified infected machines on ISP networks as a major problem that needs to be fixed.

Domain Registrars: Registrars have been generally regarded as lagging in terms of phishing countermeasures. One expert claimed that registrars actually have a disincentive to fight phishing as criminals still pay them for registering phishing domains. However, another expert familiar with the registrars disagreed, saying, "Registrars would get charge back eventually because phishers are usually using fake credit cards to register these domains." Some other experts suggested that registrars lacked the capability to detect and shutdown phishing fraud, as they work on small profit margins.

Stakeholder Capabilities and Incentives are Often Misaligned.

Economists have suggested that liability should be assigned to the party that can do the best job of managing risk [136]. However, throughout the interviews, we found that the party that can do the best job is not always managing the risk.

For example, in Asia, if banks can prove that a customer acted with negligence, the bank is not liable for a phishing loss. The difficulty is to prove that customers acted with negligence. One participant from a major bank in Asia said that when his bank was first attacked by phishers, the bank reimbursed victims. However, he said, "We've then since done a lot of education and we have joined the association of banks for a series of community bank education programs. After that, if customers do not pay attention to the education, we consider that to be negligent, so we try not to reimburse them. Of course, if the customer starts to yell and complain to the regulators, then it is entered into a fueled debate."

As another example, experts mentioned that merchants are held liable when phishers use fake credit card credentials to buy goods from them. When banks find out about the fraudulent charges, they will charge the merchant for it and sometimes also charge fines. This liability can be shifted if merchants implement the "Verified by Visa" program, but many merchants do not because of usability concerns. Furthermore, one expert argued that it is very difficult for merchants to notice that a credit card is stolen, noting that banks are at a much better position to make that judgment because they possess more information about the given credit card and a history of the transactions that make it easier for them to spot fraudulent charges.

As a third example, some experts claimed that ISPs are in the best position to protect their network and clean up compromised machines, but are not willing to take proactive measures because they would incur high costs while generating little benefit. One expert said:

> The ISP is in a good position to inspect and identify some machines that are sending out spam and launching denial of service attacks.... There are quarantine devices that exist.... ISPs have it, but even for the ISPs using them, it is not used much. It is expensive for ISPs. If you put the user on quarantine, you end up having high customer

> cost, the person will call the help desk, and you have to walk them through everything. The benefit to the ISP is very low compared to the cost. This is because the ISP did not bear the cost of compromised machines, putting externalities, hosting spam, it is not infecting the ISPs bottom line, but it is impacting every one else's bottom line.

We asked experts to comment and prioritize on a set of recommendations on the issues of incentives. We discuss the first recommendation with our experts and introduced the second recommendation based on our findings.

Recommendation (R1): Financial institutions should produce more accurate estimates of phishing losses and report these statistics. As we mentioned earlier, accurate estimates of the phishing threat are difficult to come by, but very important. For example, it is difficult for law enforcement to open cases if they do not have a good idea of the amount of loss or the type of damages. Similarly, without quantifying damages, it is hard for corporations to manage the risks.

For a corporation to obtain these figures, experts suggest two possible steps: first, law enforcement should collect and preserve forensics data when the phishing servers or drop accounts (email accounts used to gather stolen credentials) are seized, provide detailed information about the accounts stolen, and collaborate with banks to double check these fraud cases. Second, fraud managers within the organization should look at the organization as a whole when estimating damages, not just the online fraud itself. For example, they could examine how phishing increases customer service costs.

The cost to financial institutions for implementing these policies include researching the damage to the institution holistically, implementing measures to record the losses if no measure is in place. The immediate benefit to the financial institutions is that they will have a clear picture how phishing impacts their organization. The larger benefit, however is given to other stakeholders in that they can make their decisions better with more accurate data.

The obstacles for implmenting this recommendation is that currently many financial institutions do not have incentives to report estimates of phishing losses, and fear of negative publicity serves as a disincentive. One way to address this is mandatory anonymous reporting, such as in the case

of the UK payment association (APACS), which requires its members to report their losses and aggregate them together.

Recommendation (R2): Regulators and academic researchers need to investigate the issue of incentives further. As mentioned in our findings, some stakeholders (such as consumers or merchants) are not really equipped to protect themselves against fraud, so placing the liability or burden of proof on them would do little to help fight against phishing. On the other hand, ISPs who are in a better position to clean the compromised machines do not have incentives to do so. Further research is needed to develop incentive models and determine where incentives are misaligned and ways to realign the incentives.

3.5.3 What stakeholders should do

Experts identified operating system vendors, web application providers, browser vendors and Internet service providers as stakeholders with key technology influence over phishing.

Experts identified operating system vendors, web application providers, browser vendors, and Internet service providers as being best positioned to fight phishing.

Operating systems are crucial because their security or insecurity has far reaching effects. Experts generally praised Microsoft for their efforts in hardening their operating systems, but pointed out more to be done in this area. They gave a few recommendations that we will cover in the later part of this section.

Experts pointed out the insecurity of web applications as a significant hurdle. One technical expert charged web application vendors for the current state of the problem:

> [Phishers] are losing on the email; the majority of the places are running filtering now, spam and antivirus filtering. But if I want to compromise the end-user, I am going to send them a URL and redirect them to some website that hosts malware. The stuff that can become most widespread is SQL injection of some legitimate server, and users will see an iframe that loads a malware onto it.

Experts also commented on the strategic position of the browsers in the fight to protect consumers. First, web browsers can warn users directly and effectively. A recent laboratory study showed that when Firefox 2 presented phishing warnings, none of the users entered sensitive information into phishing websites [29]. This study also recommended changes to Internet Explorer's phishing warnings, and Microsoft has already acted on some of them to improve IE 8's warning mechanism. Second, the browser market is fairly concentrated, with two browsers (Internet Explorer and Firefox) accounting for 95% of the total market [101]. Solutions implemented by these two browsers would provide the majority of users with a defense against phishing.

Finally, experts pointed out that ISPs are in the best position to clean up compromised machines, as described earlier.

We asked experts to comment on and prioritize a set of recommendations for securing the computing environment. Experts ranked the following as top priorities.

Recommendation (R3): OS vendors should continue to secure operating systems by implementing secure coding practices, investing in secure vulnerability patching, and building anti-malware capability directly into the operating systems to enhance default security. To secure the operating system, experts suggested Microsoft protect the hosts file in Windows XP and earlier versions, as done by some Antivirus software [149], to prevent pharming attacks.

Another way to secure the operating system is by constantly patching with the latest updates, as a fully patched computer with firewall enabled provides a strong defense against exploit-based malware. However, one of the problems with patching is that distributing a patch provides information to criminals about the security vulnerability that is being patched. Even if the description is vague, a patch can be disassembled and compared to the code that it replaces. Once a new exploit is known, a malware exploit can be quickly crafted using pre-built components. It currently takes less than three days – sometimes only a matter of hours – between the time a patch is released and the time a malicious exploit appears. After this short period of time, most computers are still vulnerable to infection. Research and application development into securely delivering patches to computers, possibly using public-key cryptography, would help alleviate the problem [52].

Finally, some experts suggested building anti-virus and anti-malware capability directly into the OS. Experts pointed out that XP service pack 2 has a security center with firewalls enabled and suffers fewer attacks than service pack 1 [12]. These experts also praised Microsoft's effort to distribute malware removal tools and updated malware signatures monthly, and argued that Microsoft should provide some default protection to computer users who do not buy anti-virus software.

Recommendation (R4): Stakeholders should focus on improving the security of web applications, providing support and incentives for fixing applications. Currently, over 70% of phishing websites are hosted on hacked websites or free hosting sites. Many vulnerabilities for web applications exist (e.g. SQL injection, cross site scripting, remote code execution), making them a tempting target for criminals. Experts suggested a few ways to improve the security of web applications. One expert felt that technical authorities such CERT or APWG should produce a list of most frequently hacked websites and notify the website operators of their vulnerability.

However, not all website operators have the technical capability or incentives to fix the problem. A recent paper by Moore and Clayton showed that 25% of the hosts used for phishing end up being compromised again within a couple of months [94]. If the compromise is due to a lack of technical capability, then there needs to be a way to provide tools and educational resources to help them secure their web application. On the other hand, if repeated compromises are due to a lack of incentives to fix, then there needs to be a way of punishing transgressors, with escalating consequences.

Another approach is to involve the hosting provider. For example encourage these providers run intrusion detection on the applications they are hosting, and scanning newly created pages for phishing and malware.

Recommendation (R5): Web browser vendors should continue to improve the performance of integrated browser anti-phishing warning systems, with a goal to catch 90% of phishing URLs within an hour after they go online. As mentioned previously in this section, web

browsers is at a strategic position as they can warn users effectively, and faster than other methods. Currently, browser-integrated phishing warning systems catch only 40-60% of the URLs 3 hours after the attacks are launched [128]. To provide the majority of Internet users with adequate protection, these warning systems should be improved.

To accomplish this, the key is heuristics. Currently major browsers only use human-verified blacklists. To raise detection rates significantly, heuristics need to be used to supplement existings blacklists and block attacks more quickly [128]. Another way to improve the coverage of the blacklists is to gather phishing feeds from multiple sources to maximize their coverage [93]. However, as discussed in the next section, browser vendors are extremely cautious in using heuristics because of false positives, incorrectly labeling a legitimate site as phishing, which could potentially expose them to costly lawsuits. We present recommendations to address this issue in the next section.

Recommendation (R6): Academics and for-profit protectors should develop better techniques to quickly identify botnets and proxies, shut down botnet command and control, and clean compromised machines. To shut down botnets, experts recommended that we either go after their command and control centers or clean the bot machine themselves.

In November 2008, a hosting company named McColo that hosted a bot command and control center was disconnected by its upstream providers, causing a nearly 70% drop in spam volume [65]. More efforts to identify and shutdown comand and control centers would diminish the usefulness of other bots. However, we have to be mindful that criminals will continue to regroup and attack again. A good illustration is that two months after the McColo case, the spam volume was back to the previous level [20]. Spammers find other bot command and control centers, and they are getting more sophisticated in using P2P tools to control bots instead of traditional IRC commands. Defenders need to learn from successes and failures to ensure faster reaction in the future.

The McColo case offers several lessons. There invariably exists some rogue hosting companies (also known as bullet-proof hosting), so persuading them to clean up their network would be difficult and likely have limited effect. Therefore it is important to involve upstream connectivity

providers. However, these providers face some challenges for proactive monitoring. For example, the infrastructure for monitoring is expensive, the legal justification is unclear, and because of contractual agreements, they are likely to be very cautious. So other stakeholders such as public protectors or for-profit companies needs to help provide as much evidence as possible. Second, media can play an important role. In the case of McColo, a Washington Post report played a critical role in pursuading the upstream providers. Similarly, the media played an important role in having the Russian authorities shut down the Russian business network, a known hosting provider for Internet miscreants [30]. Finally, the higher the level of coordination between stakeholders, the better they are at identifying and shutting down these rogue providers.

Another approach focuses on cleaning up individual machines. This is a much more challenging task as there are millions of compromised machines to fix. ISPs need to be involved. Recognizing the disincentives mentioned in section VI, one expert suggested a notice and take down approach: certain third parties can notify an ISP that a certain computer on its network is in a botnet or doing something malicious. Once the ISP receives the notification, it becomes obligated to clean up the machine.

The cost for ISP in this instance is the cost of cleaning up the compromised machine, elevated customer service costs, and potential costs due to customer leaving. The benefit to ISP in this case is little, however the benefit to other stakeholders are more pronounced. Therefore, it is still necessary to implement a notice and take down approach. Another challenge for the notice and take down approach is who is providing the notice? and whether ISP will trust the notice served. With some kind of safe harbor regulation similar to DMCA's notice and takedown provision, this problem can be solved.

Finally, efforts are needed to automate the clean up process. Experts suggested that we won't see much of an impact on crime rate until we clean up a large fraction of compromised machines. Hence, better automatic solutions are needed to complement the notice and take-down approach.

Although no actions have been taken so far, the ISPs we interviewed acknolwedged that compromised machines are a big problem. During the interviews, they asked about academic research

on automated tools to quarentine these compromised machines. We suggest conducting more research and development focusing on automated mitigation of malware-infected computers.

Organizations are conservative about filtering and warning about phish because they are worried about false positives. However, this often leads to repeated efforts and slow reaction.

The issue of false positives came up frequently during our interviews. Generally speaking, phishing detection falls into two categories: blacklist-based methods in which humans verify suspicious phishing URLs, and heuristic approaches that utilize HTML or content signatures to identify phish automatically. In our interviews, we found that providers favor blacklists over heuristics, and even those who do use heuristics are using them conservatively. For example, an expert at an ISP told us that they had a system that warns users if a certain email appears to be phish (based on blacklists and heuristics), but they did not delete these emails because they consider their false-positive rate to be too high.

Browser vendors are also extremely concerned about false positives. The expert from a major browser vendor said that they take false positives very seriously and manually verify each URL on their blacklist to avoid false positives. All of the major browsers appear to favor human-verified blacklists with extremely low false positives over heuristics that may potentially have higher false positives.

Registries consider false positives as their biggest concern in implementing anti-abuse policies. One registry told us that they do not take act on phishing URLs submitted by third parties (such as takedown vendors) until the URLs have undergone a review process to determine if they are really phishing URLs. In other words, a phishing site is verified multiple times by different parties before action is taken, wasting precious time.

Infrastructure providers are concerned about potential liability from mislabeling or taking down legitimate websites. There have been cases where companies have attempted to hold service providers responsible for false positives, but as of yet no company has been held responsible.

For example, in a 2005 court case, Associated Bank-Corp sued Earthlink after the Earthlink anti-phishing software ScamBlocker blocked the bank's legitimate page [11]. Earthlink was able to fend off the suit on the basis that it was using a blacklist of phish provided by a third party, thus, under a provision in the Communication Decency Act (CDA), it could not be held liable as a publisher when that information is erroneous. Although the bank apparently did not sue the provider of the blacklist, the court opened the door for them to do that.

False positives based on heuristics have more subtle concerns. If heuristic-based software blocks a phish that turns out to be a false positive, the vendor may be regarded as a publisher under the CDA, and thus not immunized. Because of these fears, heuristics are not favored in integrated browser phishing protection.

It is unclear, however, how future cases, if any, will be handled. One legal expert thought there was no case to be made. He said:

> I think everything will depend on what statements are made about the blocked site by the anti-phishing software. For example, when it says, 'we think this site might be a phishing site,' unless they were grossly negligent (in which case the thinking would not be reasonable), there would probably be no liability. If it said 'This site is absolutely a phishing site' it would be a whole different story.

It is worth noting that vendors have developed blacklist processes and heuristics with extremely low false positive rates. One software vendor told us at their current false positive rate is so low that a user would encounter a false positive only once in a few years. Another takedown provider told us that they only had one or two false positives in the past four or five years, and even those false positives were arguably true positives. Recent academic work has shown that heuristics seem to detect websites with near zero false positives ([75], [128]). It is therefore, unclear why vendors remain so reluctant to use heuristics more aggressively.

To address this issue, we introduce three recommendations based on our findings.

Recommendation (R7): Clarify the legal issues surrounding false positives of blacklists and heuristics. Companies are adopting conservative strategies to avoid false positives for fear of

liability, even when false positives occur rarely. This is hurting phishing protection, especially when heuristics offer real-time protection against phishing and have considerable benefits over blacklists. We encourage more discussion on liability surrounding the use of phishing blacklists and heuristics. So far, there has been no test case on this matter. The question at hand is at what level of accuracy heuristics can be applied to block phish and not be held liable? Some experts argued that zero false positive is the only acceptable level, but most of the experts interviewed feel that it would be reasonable to block with less-than perfect accuracy if a procedure were in place to correct errors. Safe harbor legislation, which immunizes providers from liability if they meet certain standards, may be necessary to make companies comfortable that they will not be held liable.

Clarifying liability is important because lack of clarity on these matters could further reduce vendors' incentives to use heuristics to detect phishing and get protections in place rapidly. Major browser vendors and ISPs potentially take on liability for false positives, but do not lose money directly from phishing. Therefore, an uncertain legal situation may reduce their willingness to be proactive.

Recommendation (R8): Create a central clearinghouse to quickly verify phishing reports coming into APWG and on vendor blacklists. Currently there is a great deal of duplicated effort as phishing reports end up getting verified by multiple sources. For example, many vendors and service providers will not trust phishing reports until they have verified them themselves. A verification organization could serve as a clearinghouse for phishing reports and allow these reports to be verified rapidly using a standard process in which the evidence supporting each report is fully documented. In addition, it is important to report whether each phishing site is a domain setup for phishing or a legitimate domain that has been hacked. This distinction is important for registrars and registries, as these cases require different actions to be taken.

Recommendation (R9): Researchers should focus on heuristics that minimize false positives.

A sampling of published research has found that current anti-phishing heuristics have a false

positive rate of 0.43% - 12% [128]. However, to make sure these heuristics are used, the false positive rate needs to be extremely low. Since billions of websites are visited each day, even if a heuristic has a 1% false positive rate, it means millions of webpages are falsely labeled. For heuristics to be used widely, the false positive of heuristics needs to be at near zero levels. Recent efforts such as [143] and [109] is a good start.

Registrars and registries can play an important role in fighting phishing.

As mentioned earlier, registrars and registries have been generally regarded as lagging in terms of phishing countermeasures, but many experts interviewed agreed that they could play a more active role. For example in the case of fast flux attacks, registrars need to be prepared to suspend phishing domains. The Anti-Phishing Working Group produced a set of recommendations for registrars and registries [6].

One key player is the Internet Corporation of Assigned Names and Numbers (ICANN). It is responsible for managing the root zone DNS, setting and negotiating contractual standards for registrars and registries. ICANN is not a regulatory body like the Federal Communication Commission (FCC) and it has limited capabilities to regulate. Going forward, many experts think that ICANN can and should play a more active role in combating phishing and other crimes. Experts suggested that ICANN establish a minimum set of standards for registrars and registries, coupled with self-regulation and better enforcement. However, experts acknowledged that ICANN needs to play a delicate role and achieve consensus with the parties involved to avoid backlash.

We asked experts to comment on and prioritize a set of recommendations for registrars and registries. Experts ranked the following recommendations as top priorities.

Recommendation (R10): ICANN should improve enforcement of domain abuse. Experts agree that one thing ICANN can do better is to enforce compliance. One expert familiar with ICANN said:

> Some registrars . . . are very good at enforcing compliance. Other registrars are very good at looking as if they can't do it. KnujOn lists top 10 registrars with domain

> abuses. Most of my anecdotal research, we see those same names that come up again and again. But they are just confident enough to keep their accreditation.

ICANN has been improving their efforts. In October 2008, they de-accredited one of the ill-behaving registrars. Experts think more of these efforts would be good, because de-accreditation produces a credible penalty for non-compliance, as it essentially terminated the registrar's business.

Recommendation (R11): ICANN should encourage registries to adopt anti-abuse policies. Several registries have implemented anti-abuse policies, and anecdotal evidence [7] suggests that registries who have implemented anti-abuse policies have much less fraud than those who have not. An expert who works for a registry that recently adopted anti-abuse policies told us his company adopted these policies after they observed how similar policies helped other registries.
However, some registries may not have enough incentives to adopt anti-abuse policies because adding policies creates overhead. ICANN can provide some incentives. One way to encourage adoption is for registries who have adopted anti-abuse policies to share their stories and explain how they led to cost savings and how they handle the issue of false positives. To some extent this is already being done, but ICANN can encourage this further. Another inducement to adopt anti-abuse policies is for ICANN or APWG to publish phishing data based on different registries' performance on phishing takedowns, and to share this information regularly with registrars and registries. Finally, as a stronger incentive, ICANN could use anti-abuse metrics as part of their evaluation criteria for future registry applications, for example approving new gTLDs.

3.5.4 Law enforcement and education

Experts agreed that law enforcement should be emphasized, but law enforcement lacks the necessary tools, personnel, and resources to catch phishers.

Experts agreed that law enforcement is essential to deter phishers, and the top priority for law enforcement anti-phishing efforts is to catch organized phishing operations such as rock phish, which are responsible for more than 50% of the phishing attacks. One expert commented:

> If we can take out the major hubs, it is not going to solve the problem, but it can show that law enforcement can catch them . . . On top of that, these criminals have complex network, and it is not easy to set up. If we can get these gangs, then we may still have the coding kiddies, but those are a lot easier to catch.

However, experts acknowledged that law enforcement face significant challenges:

International nature of the problem. Experts acknowledged that the underground economy is very specialized. One gang is using compromised web servers in many countries that launch attacks with victims in multiple countries. Currently the Mutual Legal Assistance Treaty (MLAT) forms the basis for cooperation between different nations. However, the law enforcement experts that we interviewed complained that this process is very slow.

Proxies. Phishers use proxies so that it is difficult to catch them when they check balances on compromised accounts. This problem is hard to overcome, as there are estimated to be over 10,000 active proxies and it is necessary for law enforcement agents to perform network monitoring of the proxy machine to catch phishers. However, a warrant is required for law enforcement to legally monitor proxy machines, and by the time a warrant has been issued, the phisher has moved on to a different proxy.

Lack of accuracy in Whois data: Phishes are aware that law enforcement uses Whois data to trace illegal activity, so phishes fabricate contact information when they register domain names using stolen credit cards.

Lack of analytical capabilities: Law enforcement often lacks the ability to analyze the data they have. One law enforcement officer that we interviewed said:

> It takes a lot to identify a criminal. There is a lot of data submitted to us from members of APWG or DPN (Digital PhishNet). We don't have time to look at it all. We have to pick out a few variables we know historically told us that is a good target. But the question is that what are we missing? Is there something on that phishing kit are we missing?

Lack of case development tools to process the subpoena request: Multiple law enforcement agents commented on the lace of case development tools. One local law enforcement agent commented:

> When we issue subpoenas, some will give searchable PDFs, others give us Microsoft Access database, and some even give us paper. We need tools to conform to the same form of dataset. This is usually done case by case. If law enforcement has a centralized place to do that so that agents all over the country can use it.

We asked experts to comment on and prioritize a set of recommendations for more effective law enforcement. Experts ranked the following recommendations as top priorities.

Recommendation (R12): Improve and invest more into law enforcement, specifically for international cooperation. Experts commented that it is currently fairly difficult to cooperate with different law enforcement in different jurisdictions because there is often not a lot of money set aside for cooperation. At this time, the cooperation is through the MLAT process, which is very slow. One way to improve on this is to have a joint-task force between two police jurisdictions.

Recommendation (R13): The US Government should invest in technologies to provide law enforcement with better analytical capabilities to prioritize and manage cases. There are over 40,000 classic phishing attempts every month, and prioritizing which cases to pursue is critical. One expert said:

> Just speaking on [our organization's] behalf, we get a lot of information in, but we are overloaded. People can share data now, that's occurring, but what's not happening is the analysis piece. We have limited resources . . . We do it manually. We need resources, software and hardware to enable that, also more bodies looking at it. There is no magic about the data, but the magic is in the analysis. . . taking institutional knowledge and applying some data mining algorithms.

Recommendation (R14): Get more corporations to aggregate and submit fraud data to law enforcement to identify proxies. Currently, most phishing attacks are from botnets and proxies and almost all criminal organizations use proxies to check account balances of phished accounts. Aggregating these data from various sources will help law enforcement to determine where to request subpeonas for wire taps. One way to do this is by having corporations work together and give law enforcement fraud data with a single list of IP addresses that have checked balances on compromised accounts. Another way is for Internet service providers who have information to share that with law enforcements.

Recommendation (R15): Continue to strengthen collaboration between public protectors, private protectors, and between law enforcement in different countries. Collaboration is key to catch phishers due to the international nature of phishing. It is vitally important for law enforcement to develop good relationships with their peers in other countries. One noteable effort is the Digital PhishNet conferences that NCFTA and Microsoft organize each year. More efforts like these are needed.

Experts agree that shutting down money trails is very important to defeat phishers.

Experts said that shutting down the money trail can make phishing less attractive. For example, phishers often use "money mules," persons recruited to receive stolen funds (or goods bought using stolen funds) and then transfer the money out of the country. Mules are recruited by a variety of methods, including spam emails, advertisement on genuine recruitment web sites and newspapers, approaching people who have their CVs available online, and instant messaging.

To shut down money trails, one expert recommended we find out where the mules typically are and how mules are recruited. Another expert suggested that banks and take-down organizations put more effort into shutting down mule recruitment websites. He mentioned recent research that mule recruitment sites takes much longer to shutdown than normal phishing websites.

Another expert proposed a clearinghouse of accounts where each participating bank submit accounts that have been used as mules. Currently, bank fraud systems can detect some suspicious transactions to mule accounts, but there is no system in place to share this information with other banks. If this list of suspicious accounts were shared, a lot of money laundering could be stopped.

Education and awareness are important factors that are not emphasized enough. However, not all experts agree on the effects of education.

Most experts agreed that anti-phishing education for end users needs to be implemented better. However, some experts strongly endorses it, while others say eductaion should *not* be a focus. Both sides have strong words to say. For example, one expert in favor of more education said:

> There needs to be some accountability on Internet users .... People still click on URLs they shouldn't. So we need to stress user education, and a little bit of common sense. We are a society that becomes desensitized to our responsibility. You really end up paying for this over time. You are going to end up paying high interest rates. So you really do need to pay more attention.

Another expert who has worked on anti-phishing campaigns at a large US institution doubted the efficacy of such efforts:

> My experience of education is that it won't make that much difference. You have to do it, because if you don't, consumers will get mad at you. There is trust and there is safety. You have to balance both of them. ...However, education doesn't impact phishing losses, or make it less. It doesn't do any of that, what it does is making people feel safer. If your goal is to improve security, then education shouldn't be of top priority."

Based on these comments, we introduced a set of recommendations.

Recommendations (R16): Academic researchers and industry should continue to make education fun, engaging and up to date. Current academic research shows that popular online

user education materials are effective if users *actually* read them. For example, Kumaraguru et. al asked users to read four popular training materials online and tested their ability to recognize phishing websites. They found that users were able to distinguish phishing websites from legitimate ones much better after reading these training materials [70]. However, the problem is that users normally don't read security training materials [69].

To make education more effective, we recommend developing more innovative ways to make education fun, engaging, and up to date (e.g. [127], [67]).

Recommendation (R17): Launch an education campaign to educate the public about mules, and encourage social networking sites to take the initiative to educate their customers about phishing. Experts mentioned the need to educate money mules, some of whom unknowingly become accomplices to crimes. To educate mules, experts recommend we find out where the mules typically are and how mules are recruited. Finding out where they are recruited can help determine whether national campaigns or if targeted campaigns are needed.

Experts also thought social networking sites should take the initiative to educate their customers about phishing, as they are increasingly becoming targets of phishing campaigns.

Recommendation (R18): Complement education with other countermeasures such as filtering and better user interfaces. Where possible, efforts should focus on automatic filtering that does not require user knowledge, and designing better user interfaces that make it more obvious to users what the right trust decision is.

However, education remains an important part of combating phishing because it is unlikely that any automated system will ever be completely accurate in detecting phishing attacks, especially when detection requires knowledge of contextual information. There will still remain many kinds of trust decisions that users must make on their own, usually with limited or no assistance.

3.6 Discussion

3.6.1 Applicability of the Recommendations against Spear-phishing

In this chapter, we reported on 18 recommendations from 31 qualitative interviews with anti-phishing experts. These recommendations are effective for combating generic phishing. However, as spear-phishing increases, what are the unique challenges that it poses? Can we combat it by applying our anti-phishing recommendations? In the concluding section of this chapter, we address these questions.

Compared with traditional phishing, spear-phishing poses two unique challenges. First, unlike traditional phishing scams that send mass phishing emails to everyone, spear-phishers send fewer, more targeted emails. This poses challenges to the current signature-based email filtering systems, which rely on large number of emails for fingerprinting. Second, Spear-phishing is a highly targeted phishing scam. Phishers exploit the social context to send spoofed emails to consumers that appear to come from someone they know. These attacks pose a severe threat for the end users, who normally use social context as cues in determining email legitimacy [50]. As a result, users fall for more spear-phishing attacks compared to regular phishing attacks [53].

Although spear-phishing poses these problems, the majority of our recommendations are likely not affected. Our recommendations attack the root problem of phishing by improving law enforcement (R12 - R15), improving incentives for stakeholders with better statistics and more research (R1, 2), and hardening the underlying infrastructure to make phishing less easy to conduct (R3,4, 6, 10,11). All of these efforts can lead to the reduction of both generic phishing and spear-phishing.

A few of our recommendations would be particularly useful in terms of combating spear-phishing. Heuristics would be very important in identifying spear-phishing emails, as it does not use signature-based fingerprinting that relies on a large number of emails to be accurate. Therefore the two recommendations on improving heuristics would be particularly helpful in combating spear-phishing (R7,9).

The majority of our recommendations on education will be effective against spear-phishing as well, although for recommendation R16, educators need to additionally incorporate elements of spear-phishing into their education curriculum.

Finally, spear-phishing poses challenges to two of our recommendations: R5, for web browser phishing protection and R8, for a central clearinghouse to quickly verify phishing reports. The challenge is that spear-phishes are harder to detect, and therefore may take a longer time to verify and warn. However, by deploying heuristics more aggressively, the deficiencies of these two recommendations can be overcome.

3.6.2 Summary of findings

In this chapter, we reported on seven findings (summarized in Table 3) and 18 recommendations (summarized in Appendix A) from 31 qualitative interviews with anti-phishing experts.

Our findings suggest that phishing is evolving into a more organized effort. It is part of a larger crime eco-system, where it is increasingly blended with malware and used as a gateway for other attacks.

Experts identified several places where incentives for fighting phishing may be misaligned, in the sense that the stakeholders who are in a position to have the largest impact do not have much incentive to devote resources to anti-phishing. To resolve this, we recommend further study of these misalignments and development of policy alternatives to correct them.

In terms of countermeasures, experts identified improving law enforcement and shutting down money trails as top priorities. We identified key difficulties that law enforcement organizations face, and recommend investment into specific types of technologies made to equip law enforcement to better prioritize cases. Collaboration is the key in these investigations, so we recommend ways to foster it.

Experts agreed that education is an important factor that is not emphasized enough, however, they did not agree on the effects of education. We recommend developing more innovative ways to make education fun, engaging and up to date and propose content areas that education needs to be focused on.

Finally, we qualitatively analyzed the challenges and obstacles for implementing these recommendations, their associated costs, and benefits, and actionable items that stakeholders can do to (see Table 3.4).

Table 3.4: Obstacles and Challenges, benefits, costs, and actionable items for the recommendations

Recommendation	**Obstacles and Challenges**	**Costs**	**Benefits**	**Actionable Items**
1. Financial institutions should produce more accurate estimates of phishing losses and report these statistics.	1. Financial institutions do not have incentives to report estimates of phishing losses, and fear of negative publicity serves as a disincentive. 2. It is hard to separate phishing from other kinds of losses such as malware. 3. Phishing losses appear in different units of the company and could be difficult to compile.	Cost to FI: 1. researching the phishing damage holistically. 2. Implementing measures to record the losses if no measures are in place.	Benefit to FIs: they will have a clearer picture how phishing impacts their organization. Benefit to others: They can make more informed decisions about the investment and management of the risk.	Federal regulators draft rules to require mandatory anonymous reporting, such as in the case of the UK payment association (APACS).
2. Regulators and academic researchers need to investigate the issue of incentives further (a study comparing different phishing liability regimes around the world)	1. Data hard to get from financial institutions. 2. Regulatory environments are different around the world.	Costs: Time and resources of academicians and regulators for the research	Benefits: Solid research can help regulators to assign liability to the party who is most capable of fixing the problem.	Regulators in different regions compel financial institutions to provide the data.

Table 3.4: Obstacles and Challenges, benefits, costs, and actionable items for the recommendations

Recommendation	**Obstacles and Challenges**	**Costs**	**Benefits**	**Actionable Items**
2a. Regulators develop a notice-takedown approach for botnet C&C removal	Challenges: privacy and contractual considerations for ISPs and hosting providers; potential for abuse	Costs: time to address concerns of opponents and negotiate compromises; cost of enforcement	Benefits: faster notice-takedown of botnet command and control would reduce the effectiveness of botnets dramatically in the short term	Regulators develop a process for takedown and appeal.
3. OS vendors should continue to secure operating systems by implementing secure coding practices, investing in secure vulnerability patching, and building anti-malware capability directly into the operating systems to enhance default security.	Challenges: 1. Secure coding takes time to mature. 2. OS vendors may lack expertise and experience in antivirus and anti-malware tools.	Costs to OS vendors: investment of resources (time, personnel)	Benefits to OS vendor: Improved security and visibility of the operation system. Benefits to others: a cleaner network environment with default security enabled	

Table 3.4: Obstacles and Challenges, benefits, costs, and actionable items for the recommendations

Recommendation	**Obstacles and Challenges**	**Costs**	**Benefits**	**Actionable Items**
4. Stakeholder should focus on improving on the security of web applications.	Challenges: 1. The total number of web applications needs to be fixed is large and owners may not know about them. 2. Attacks are continuous, so requires constant vigilance. 3. Website application owners lack expertise or may not care. 4. Hosting providers lacks incentive to proactively scan their network	Costs to technical authority: gather knowledge and tools for reporting them. Cost to web application operators: time, resource and expertise to fix the vulnerabilities	Benefit to web applications: reduce the risk of being blacklisted, improve the security. Benefit to others: Overall improvement in the general security.	1. technical authorities such CERT or APWG produce a list of most frequently hacked websites and notify the website operators of their vulnerability. 2. Provide educational resources for those who lack technical capability. 3. Punishing continuing transgressors, with escalating consequences such as a reputation-based systems.
5. Web browser vendors should continue to improve the performance of integrated browser anti-phishing warning systems, with a goal to catch 85-95% of phishing URLs within an hour after they go online.	Challenges: browsers are conservative in using heuristics because of false positives	Cost to browsers: continual investment in improving anti-phishing capacity with better feeds	Benefits: significant default protection offered to the end user.	1. Browsers use heuristics as a way to label websites for blacklist review. 2. Legal authorities clarify the liabilities surrounding the use of heuristics.

Table 3.4: Obstacles and Challenges, benefits, costs, and actionable items for the recommendations

Recommendation	**Obstacles and Challenges**	**Costs**	**Benefits**	**Actionable Items**
6. Academics and for-profit protectors should develop better techniques to quickly identify botnets and proxies, shut down botnet command and control, and clean compromised machines.	Challenges: 1. Botnet C&C is very adaptable and tend to regroup after being shutdown. 2. Hosting providers are cautious because infrastructure for monitoring is expensive, the legal justification is unclear, contractual agreements could pose problems. 3. We need to fix a significant amount of machines to significantly impact to ecrime infrastructure. 4. There are privacy concerns of sharing fraud data between institutions	Costs to ISP: the cost of cleaning up the compromised machine, elevated customer service costs, potential costs due to customer leaving.	Benefits to ISP: little. Benefit to others: significant reducing in the key ecrime infrastructure.	1. Other stakeholders such as public protectors or for-profit companies need to help provide as much evidence as possible. 2. The higher the level of coordination between stakeholders, the better they are at identifying and shutting down these rogue providers.
7. Clarify the legal issues of the false positives of blacklists and heuristics.	Challenges: Determining the right level of false positives; legal risks for companies who are the test case.	Cost: legal research and proceedings	Benefits: extremely high for stakeholders such as browsers and ISPs	APWG set the standard for acceptable level of false positives.

Table 3.4: Obstacles and Challenges, benefits, costs, and actionable items for the recommendations

Recommendation	**Obstacles and Challenges**	**Costs**	**Benefits**	**Actionable Items**
8. Create a central clearinghouse to quickly verify phishing reports coming into APWG and on vendor blacklists.	Challenges: Providing phishing feed is a legitimate business, a central clearinghouse would likely drive these out of the business; also likely to be reinventing the wheels	Costs: building the system and the ongoing administration of the system and verifying of phishing feeds	Benefits: A single source reduce the duplicated efforts by various organizations and provides uniform protections for its users.	NOTE: These obstacles means that there would be little incentives for APWG or other parties to take initiatives on this; a more likely scenario is for APWG to define certain performance metrics and certify the existing feed providers
9. Academics should focus heuristic research on reducing false positives.	Challenges: Transforming research into production is nontrivial.	Costs: Time and resources for the research	Benefits: Low false positive heuristics would benefit browsers, email providers greatly.	NSF or industries provide more research funding.
10. ICANN should improve enforcement on domain abuse.	1. ICANN has limited capability regulating registrars and registries. 2. The ICANN consensus process could be time-consuming.	Costs to ICANN: developing technical capabilities for spotting domain abuse.	Benefits: deterrence effect for criminals and registrars who opt to play with them.	Action: ICANN should define metrics for domain abuse, and devise incentives to reward registrars with low abuse rates.

Table 3.4: Obstacles and Challenges, benefits, costs, and actionable items for the recommendations

Recommendation	**Obstacles and Challenges**	**Costs**	**Benefits**	**Actionable Items**
11. ICANN should encourage registries to adopt anti-abuse policies.	Registries concern for false positives would slow their action time. 2. Registries may push the responsibilities to registrars.	Cost to registries: building the system, receiving and verifying the phishing feed, and dealing with false positives.	Benefits to registries: Improved security, competitive advantage. Benefits to others: fewer entities for takedown companies to interface with and faster takedown time.	1. Registries who have adopted anti-abuse policies to share their stories and explain how they led to cost savings and how they handle the issue of false positives. 2. ICANN or APWG to publish phishing data based on different registries' performance on phishing takedowns. 3. ICANN provide incentives to registries who have implemented abuse policies, for example giving them priority for new gTLDs applications.
12. Improve and invest more into law enforcement, specifically for international cooperation.	Challenges: Phishers hide their traces in many countries; ecrime cases in other countries may have a low priority.			Action items: FBI to establish a joint-task force between two police jurisdictions.

Table 3.4: Obstacles and Challenges, benefits, costs, and actionable items for the recommendations

Recommendation	**Obstacles and Challenges**	**Costs**	**Benefits**	**Actionable Items**
13. US Government should invest in technologies to provide law enforcement with better analytical capability to prioritize and manage cases.	Challenges: Which law enforcement agencies to invest?			US government invest in tools for better case management and better digital evidence processing; Expand scholarship programs to recruit graduates in computer science
14. More corporations aggregating fraud data and submit to law enforcement to identify proxies.	1. Corporations may not be willing to share because of privacy, and consumer trust concerns (reminiscent of telecom's wiretapping scandal after 9/11). 2. Corporations may not share for competitive reasons.	Costs to law enforcements: costs to set up the system and cost of analysis	Benefits: law enforcement would be able to determine which proxies to place wiretaps, significantly improving the opportunity to identify the criminals' originating machine.	Action items: FBI to produce a list of fraud data variables that it wants financial institutions to share.
15. Continue to strengthen collaboration between law enforcement in different countries, public and private protectors.	Challenges: Law enforcement in different countries may not know each other, hard to find the right people to handle the case; phishing and ecrime cases in other countries maybe of low priority.	Costs: organizing and subsidizing conferences, supporting mutual exchanges,	Benefit: Getting the good people organized better is crucial in fighting cybercrime.	

Table 3.4: Obstacles and Challenges, benefits, costs, and actionable items for the recommendations

Recommendation	**Obstacles and Challenges**	**Costs**	**Benefits**	**Actionable Items**
16. Academic researchers and industry continue to make education fun and engaging and up to date.	Challenges: Lack resources; quickly evolving nature of the phishing threat so need continual education	Costs: Resources to design and disseminate these materials	Benefit: education that are engaging and fun is important as otherwise users will not proactively read them.	Industry and government to fund licensing and deployment of some of the training materials that are proven to be effective.
17. Launch education campaign to educate the public about mules, and encourage social networking sites to take initiative to educate their customers.	Challenges: some of the mules knowingly participate in the crime; educating people about mules may make some more likely to become mules	Cost: developing materials and disseminating them	Benefit: Mule education will help those who are unaware to be more cautious; education on social network phishing can reduce people falling for them	Action: FTC, APWG, US Postal service and other industry groups take lead in designing the materials, fund licensing and deployment of existing materials that are proven to be effective.
18. Complement education with other countermeasures such as filtering and better user interface design.	N/A	N/A	N/A	N/A