

## Chapter 7

### Conclusions

As phishing and related crimeware continue to evolve, what should be the US government's role? In the concluding chapter of this thesis, we answer this question based on our analysis of the interests of phishing stakeholders, experts' recommendations, and insights from case studies. We discuss several measures that the US government can take to combat phishing.

First, experts in our study agreed that catching criminals would provide a strong deterrent as it shows the determination and capability of law enforcement. However, in our interviews with law enforcement, we found that they face three major challenges: lack of necessary analytical capabilities in determining investigative priorities (including qualified investigators and software tools), the international nature of the crime, and sophistication of criminals to hide their traces. To address the first challenge, we recommend the US government invest in tools for better case management and better digital evidence processing. To attract more talent, the US government could provide incentives to recruit from top computer science programs around the country for digital forensics and analysis, possibly through the expansion of DHS scholarship program. To address the second challenge of the international nature of the crime, we recommend the US government fund international operations and facilitate the communication and connection of law enforcement in various countries. To address the third challenge we recommend that the US government facilitate greater information sharing between law enforcement and industry.

Second, botnets are major pieces of crimeware infrastructure that have greatly enabled spamming and phishing operations. Our analysis shows that Internet service providers, who are in the best position to address this issue, do not have enough incentives to address this problem. In the short run, we recommend the US government institute a notice and takedown regime which

mandates ISPs or upstream providers to disconnect bot command and controls once they were identified. Such policies will relieve the ISPs of potential liability and will be applied to all ISPs. It is not wise for the government to set standards for ISPs to clean up the compromised machines as currently such methods are costly and will have little benefits unless a majority of the compromised machines are fixed. To secure this key piece of infrastructure, the government can also leverage some of the technologies used in national defense and apply them to fixing ISP networks. In the long term, research is needed on automatically cleaning compromised machines. Finally, fixing botnets in the US alone will not be likely to solve the problem, as there are compromised machines overseas as well. To address this issue, relevant agencies in the US government need to establish close working relationship with other countries to share intelligence of the botnets.

Third, experts in our study agreed that better statistics about phishing and related electronic crime are necessary for law enforcement to prioritize and for corporations to manage their security risks better. However, as of today, little accurate statistical information exists because financial institutions are not required to report, and they have little incentives to do so, thus making loss estimates differ by orders of magnitude. To correct this misalignment of incentives, we recommend that the US government institute some mandatory reporting.

Fourth, our case study showed that the window of opportunity for defenders is limited as close to half of the phishing campaigns lasted less than 2 hours. Although leveraging heuristics is a key solution, experts in our study pointed out major legal issues with false positives that hinder the use of heuristics. However in our case study we found that the group of heuristics that we tested yielded extremely low false positives. Therefore, we conclude it is the “fear” of false positives, not “actual” false positives that is hindering the adoption of heuristics. We recommend that legislators step in to clarify the legal issues surrounding the false positives, and provide incentives such as safe harbor legislation.

Fifth, experts in our study disagreed on the effectiveness of user education. In our mTurk study and other studies, we showed that currently the best education materials could reduce the number of people falling for phishing by 40 - 50%. This finding shows that education is effective and needed but is not a cure all. In our study, 61% of the US participants have seen phishing education

before; the task for the various stakeholders is to reach out to those 39% of the population who have not been exposed to training. However, even with the best educational materials, participants in our study still fall for around 28% of phish after training. Women and younger populations such as college students are especially vulnerable. These findings show that education should be complemented with other countermeasures such as filtering and law enforcements.

Last but not least, we detailed the recommendations that various stakeholders should take to better fight for phishing as summarized in Table 7.1. By implementing these measures, we can drastically reduce phishing and other related electronic crimes that use the same infrastructure.

Table 7.1 Summary of Recommendations

Stakeholders	Recommendations
Financial Institutions	Produce more accurate estimates of phishing losses and report these statistics
OS vendors	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
Web browser vendors	Continue to improve the performance of integrated browser anti-phishing warning systems in order to catch 85-95% of phishing URLs within an hour after they go online
ISPs	Develop or deploy better techniques to quickly identify botnets and proxies, shut down botnet command and control, and clean compromised machines
US Government	Develop notice and takedown regimes for botnet C&C removal
US Government	Invest in international cooperations through funding joint operations, facilitating the communication and connection of law enforcement in various countries
US Government	Invest in tools for better case management and better digital evidence processing; Expand DHS Scholarship program to recruit master students from top computer science schools
Corporations	Aggregate fraud data (proxies) and submit to law enforcement to identify proxies
Various stakeholders	Focus on improving the security of web applications
Academic researchers and industry	Continue to make education engaging and up to date
Academic researchers and industry	Focus heuristic research on reducing false positives
Legal Community	Clarify the legal issues of the false positives of blacklists and heuristics