

A POLICY ANALYSIS OF PHISHING COUNTERMEASURES

Submitted in partial fulfillment of the requirements for

the degree of

Doctor of Philosophy

in

Engineering and Public Policy

Xinguang (Steve) Sheng

B.S., Computer Science and Engineering, University of Pennsylvania

M.S., Computer and Information Science, University of Pennsylvania

Carnegie Mellon University

Pittsburgh, PA

December 2009

© Copyright by Xinguang (Steve) Sheng December 2009

All Rights Reserved

To my wife Phoebe Chao, for her loving support every step along the way.

ACKNOWLEDGMENTS

I would like to thank all the people who have helped and inspired me during my doctoral study. I especially want to thank my advisor, Prof. Lorrie Cranor, for her guidance during my research and study at Carnegie Mellon. Her warm and encouraging spirit, enthusiasm in research, and invaluable research insights had motivated all her advisees, including me.

I am grateful for the rest of my thesis committee. They are Profs. Alessandro Acquisti, Jason Hong and Adrian Perrig. All of them have offered innumerable comments, suggestions, and feedback about the research presented in my thesis.

I had the privilege of working with many bright and fun collaborators. I would like to thank Bryant Magnien, Patrick Kelly, Elizebeth Nunge and Ponnurangam Kumaraguru for Anti-phishing Phil; Yue Zhang, Brad Wardman, Gary Warner, Chengshan Zhang for the phishing blacklist study; Mandy Holbook and Julie Downs for the mechanical turk study; and Ponnurangam Kumaraguru for the expert interview study.

All my lab mates at the Cylab Usable Security Privacy and Security Laboratory (CUPS) made it a convivial place to study. In particular, I would like to thank Ponnurangam Kumaraguru, Serge Egelman, Justin Crenshaw, Kami Vaniea, Patrick Kelley, Janice Tsai, Rob Reeder and Robert McGuire for their friendship and help in the past five years. Thanks.

I owe my deepest gratitude to my family for their unflagging love and support throughout this dissertation is simply impossible without them. I am indebted to my father, Xiangchen Sheng, for his care and love and I cannot ask for more from my mother, Fengzhi Wang, as she is the most loving mother that I have met. My wife Phoebe has been an encourager, motivator, and counselor along every step of this thesis, in fact this thesis cannot be completed without her, therefore I will dedicate this thesis to her.

I would regret my doctoral years at Carnegie Mellon if I did not join Antioch cell group at Pittsburgh Chinese Church Oakland (PCCO). I cherished the fellowship and support between me and them, and the friendships with my Christian brothers and sisters at PCCO. I treasured all precious moments we shared and would really like to thank them.

I would also like to acknowledge the support of National Science Foundation under grant CCF-0524189, the Army Research Office under grant number DAAD19-02-1-0389.

Last but not least, thanks be to God for my life through all tests in the past five years. You have enlarged my tent and made my life more bountiful. May your name be exalted, honored, and glorified.

ABSTRACT

Phishing is a kind of attack in which criminals use spoofed emails and fraudulent web sites to trick people into giving up personal information. This thesis looks at the phishing problem holistically by examining various stakeholders and their countermeasures, and by surveying experts' opinions about the current and future threats and the kinds of countermeasures that should be put in place. It composed of four studies.

In the first study, we conducted semi-structured interviews with 31 anti-phishing experts from academia, law enforcement, and industry. We surveyed experts' opinions about the current and future of phishing threats and the kind of countermeasures that should be put in place. Our analysis led to eight key findings and 18 recommendations to improve phishing countermeasures. In the second study, we study the effectiveness of popular phishing tools that are used by major web browsers. We used fresh phish that were less than 30 minutes old to conduct two tests on eight anti-phishing toolbars. We found blacklists were ineffective when protecting users initially. The tools that uses heuristics to complement blacklists caught significantly more phish than blacklist-only tools with very low false positives. In the third study, we describe the design and evaluation of Anti-Phishing Phil, an online game that teaches users good habits to help them avoid phishing attacks. We used learning science principles to design and iteratively refine the game. We evaluated Anti-Phishing Phil through laboratory and real-world experiments. These experiments showed that people trained with Anti-Phishing Phil were much better at detecting phishing websites, and they retain knowledge after one week. In the fourth and final study we present our results of a roleplay survey instrument administered to 1001 online survey respondents to study both the relationship between demographics and phishing susceptibility, and the effectiveness of several anti-phishing educational materials. Our results suggest that women are more susceptible than men to phishing

and participants between the ages of 18 and 25 are more susceptible to phishing than other age groups. We explain these demographic factors through a mediation analysis. Educational materials reduced users tendency to enter information into phishing webpages by 40% percent; however, some of the educational materials we tested also slightly decreased participants tendency to click on legitimate links.

DISCARD THIS PAGE

TABLE OF CONTENTS

	Page
ABSTRACT	iii
1 Introduction	1
1.1 Thesis statement	2
1.2 Thesis contribution	3
1.3 Outline of the thesis	4
2 Background	5
2.1 Anatomy of Phishing	5
2.1.1 Planning	5
2.1.2 Setup	8
2.1.3 Attack	9
2.1.4 Collection	14
2.1.5 Fraud	16
2.2 Why people fall for phishing	16
2.3 Cost of phishing	18
2.4 Recent developments in phishing	19
2.5 Phishing countermeasures	22
2.5.1 Legal solutions	22
2.5.2 Technology countermeasures	23
2.5.3 Social response: awareness and education	26
2.6 Economics of Information Security	27
2.6.1 Security investment	28
2.6.2 Security as externality	28
2.6.3 Misaligned incentives	29
3 Improving Phishing Countermeasures: An Analysis of Expert Interviews	31
3.1 Introduction	31
3.2 Related Work	32

	Page
3.3 Stakeholders	33
3.3.1 Primary victims:	34
3.3.2 Infrastructure providers:	34
3.3.3 For-profit protectors:	35
3.3.4 Public protectors:	35
3.4 Methodology	35
3.4.1 Recruitment and Participants	36
3.4.2 Interview Protocol	37
3.4.3 Analysis	37
3.4.4 Limitations	38
3.5 Results	39
3.5.1 Evolving threat	39
3.5.2 Stakeholder incentives	42
3.5.3 What stakeholders should do	47
3.5.4 Law enforcement and education	56
3.6 Discussion	62
3.6.1 Applicability of the Recommendations against Spear-phishing	62
3.6.2 Summary of findings	63
4 Case Study of Browser-based Anti-phishing Solutions	73
4.1 Background and Related Work	74
4.1.1 Anti-Phishing Heuristics	75
4.1.2 Phishing blacklists	76
4.1.3 Related Work	77
4.2 Methodology	78
4.2.1 Anti-phishing Testbed	78
4.2.2 Phishing Feed	79
4.2.3 Evaluation Procedure	80
4.3 Results	82
4.3.1 Length of Phishing Campaign	82
4.3.2 Blacklist Coverage	83
4.3.3 False Positives	86
4.3.4 Accuracy of Heuristics	88
4.3.5 Total Protection	89
4.4 Discussion	91
4.4.1 Limitations	91
4.4.2 Opportunities for Defenders	91
4.4.3 Improving blacklists	93

Appendix

	Page
4.4.4 Use of heuristics	94
5 Anti-Phishing Phil: A Case study in User education	95
5.1 Introduction	95
5.2 Background and Related Work	97
5.2.1 Why people fall for phishing	97
5.2.2 Tools to protect people from phishing	98
5.2.3 Anti-phishing education	99
5.3 Design of Anti-phishing Phil	100
5.3.1 Game Design Principles	100
5.3.2 Game Description	103
5.3.3 Training Messages	105
5.3.4 Pilot Test	109
5.3.5 Modified Game	110
5.4 Evaluation 1: Lab Study	111
5.4.1 Study design	111
5.4.2 Participant Recruitment and Demographics	113
5.4.3 Results	114
5.5 Evaluation 2: Anti-Phishing Phil Field Study	121
5.5.1 Study design	121
5.5.2 Participants	121
5.5.3 Results	122
6 Phishing Susceptibility Study	126
6.1 Background and related work	127
6.1.1 Demographics and Phishing Susceptibility	127
6.1.2 Susceptibility vs. Risk Behavior	128
6.1.3 Security User Education	128
6.2 Study Design	130
6.2.1 Recruitment	130
6.2.2 Roleplay	130
6.2.3 Education Materials	134
6.2.4 Previous Experiences and Demographics	135
6.2.5 Knowledge and Technical Background	136
6.2.6 Risk Perceptions	137
6.3 Results	137
6.3.1 Measuring User Performance	137
6.3.2 Regression Analysis	137

Appendix

	Page
6.3.3 Gender and Falling for Phish	139
6.3.4 Age and Falling for Phish	141
6.3.5 Effects of Education	143
6.4 DISCUSSION	145
6.4.1 Limitations	145
6.4.2 Summary of findings	145
6.4.3 Role of education	146
7 Conclusions	156
LIST OF REFERENCES	160
APPENDIX Appendix I: List of Recommendations	172