A Policy Analysis of Phishing Countermeasures

Steve Sheng
Thesis Presentation
Sept 8, 2009

Committee
Lorrie Cranor (chair)
Alessandro Acquisti
Jason Hong
Adrian Perrig

Carnegie Mellon

CyLab Usable Privacy and Security Laboratory
http://cups.cs.cmu.edu/
Dear eBay Member,

We regret to inform you that your eBay account could be suspended if you don’t re-update your account information.
To resolve this problem please visit link below and re-enter your account information:

https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerid=2&siteid=0

If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

Regards,
Safeharbor Department eBay, Inc
The eBay team
This is an automatic message, please do not reply.
Dear eBay Member,

We regret to inform you that your eBay account could be suspended if you don’t re-update your account information.
To resolve this problem please visit link below and re-enter your account information:

https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerid=2&siteid=0

If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

Regards,
Safeharbor Department eBay, Inc
The eBay team
This is an automatic message, please do not reply
We regret to inform you that you eBay account could be suspended if you don’t update your account information.

https://signin.ebay.com/ws/eBayISAPI.dll&Signln&sid=verify&co_partnerid=2&siteid=0

If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

Regards,
Safeharbor Department eBay, Inc
The eBay team
This is an automatic message, please do not reply
Dear eBay Member,

We regret to inform you that your eBay account could be suspended if you don’t re-update your account information.

https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerid=2&sidteid=0

If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

Regards,
Safeharbor Department eBay, Inc
The eBay team
This is an automatic message, please do not reply
This entire process known as phishing.
Phishing a widespread problem

- Estimated 0.4% of emails are phishing (Messagelabs 2009)
- Average 27,000 unique phishing sites each month (APWG 2008)
- Estimated $350m – $3.2b direct loss a year (Moore and Clayton 2007, Gartner 2007)
- Attacks methods and targets evolving

More profitable to phish than rob the bank!
Research Question

As phishing continues to evolve, what can and should stakeholders do to fight it better?
Thesis Statement

This thesis analyzes phishing stakeholders and their stakes, generates recommendations to fight phishing better through expert interviews. Case studies on the effectiveness of web browser anti-phishing toolbars and anti-phishing education inform this analysis.
Outline

- Anti-Phishing expert interview study
- Empirical study on browser phishing warnings
- Anti-Phishing Phil
- Phishing Susceptibility Study
- Conclusions
Outline

- Anti-Phishing expert interview study
- Empirical study on browser phishing warnings
- Anti-Phishing Phil
- Phishing Susceptibility Study
- Conclusions
Anti-Phishing expert interview study

- 31 experts from academia, CERT, the Anti-Phishing Working Group (APWG), law enforcement, and key industry stakeholders
  - Examined the incentives of various stakeholders
  - Gathered information about the current and future state of phishing attacks
  - Ranked and prioritized countermeasures to be focused

SHENG, S., KUMARAGURU, P., ACQUISTI, A., CRANOR, L., AND HONG, J.
## Experts

<table>
<thead>
<tr>
<th>Affiliations</th>
<th>No of Experts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Academic researchers</td>
<td>5</td>
</tr>
<tr>
<td>Law enforcements</td>
<td>5</td>
</tr>
<tr>
<td>Computer Emergency Response Teams (CERT)</td>
<td>4</td>
</tr>
<tr>
<td>Financial institutions</td>
<td>4</td>
</tr>
<tr>
<td>APWG officers</td>
<td>3</td>
</tr>
<tr>
<td>Registrars, Registries</td>
<td>3</td>
</tr>
<tr>
<td>Internet service providers</td>
<td>3</td>
</tr>
<tr>
<td>Other experts</td>
<td>3</td>
</tr>
<tr>
<td>Browsers vendors</td>
<td>1</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>31</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Country</th>
<th>No of Experts</th>
</tr>
</thead>
<tbody>
<tr>
<td>US</td>
<td>26</td>
</tr>
<tr>
<td>Europe</td>
<td>2</td>
</tr>
<tr>
<td>Asia</td>
<td>2</td>
</tr>
<tr>
<td>South America</td>
<td>1</td>
</tr>
</tbody>
</table>
Methodology

- Interview Protocol
  - 60 minute in-person or phone interviews
  - 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 different countermeasures
  - comment and prioritize on a set of 31 recommendations

- Analysis
  - Full interviews transcribed
  - Themes labeled and clustered
Overview of Findings

- Evolving threat
- Stakeholder incentives
- What stakeholders should do
- Issues of false positives
- Law enforcement
- Education

Recommendations

R1, R2
R3 - R6, R10 – R11
R7 - R9
R12 – R15
R16 - R18
Evolving threats

- Phishing is evolving to be more organized
  - Majority of phishing messages suspected to come from organized phishing gangs (Moore and Clayton 09)
- Phishing is becoming more targeted and evolving
- Phishing and malware increasingly blended together
“You 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.”

from an academic expert
Misalignment of incentives

- Consumer made liable for phishing in some countries
- ISPs have little incentives to clean up compromised machines
  - A major US ISP has 10% computers infected with malware
Recommendations

- Financial institutions should produce and report accurate estimates of phishing losses
  - A major US bank lost $4.5 million to phishing and malware in 12 months
  - without reliable statistics, difficult for corporations to manage the risk and for law enforcement to prioritize cases
  - Financial institutions lack incentives to report
  - Key: collaborate with law enforcements to gather statistics and regulators should require mandatory reporting
Recommendations

- Fixing compromised machines
  - Recommend the US government institute a notice and takedown regime for bot C&C
  - Research on automatically cleaning compromised machines needed
What stakeholders should do

- OS vendors are doing a lot of good work, but web applications insecurity is a major hurdle
- Browsers are at a strategic place to warn users
  - Highly concentrated market (NetApps 2009)
  - Effective warning (Egelman et al 2008)
- ISPs in the best position to clean up compromised hosts
Recommendations

- Web browser 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
  - Key: more diverse feed and use heuristics to complement blacklist
Law enforcement

- Experts agreed law enforcement is crucial and needs to be emphasized

- Challenges:
  - Lack of necessary analytical capabilities in determining investigative priorities
  - International nature of the crime
  - Sophistication of criminals to hide traces
“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.”

A law enforcement expert
Recommendations

- Law enforcement
  - Recommend US government invest in tools for better case management and better digital evidence processing
  - Expand scholarship programs to recruit graduates in computer science
Education

- Education and awareness are important
- Experts disagree on the effectiveness of education
“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.”

From an industry expert
“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. . . . 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.”

From an industry expert
Related work

- Technical phishing analysis
  - FSTC Phishing white paper 2005
  - Identity theft Technology Council report 2005
  - DHS and APWG report 2006
- Best Practices (APWG 2006 2008 2009)
- Economics of Security
  - Security Economics and the Internal Market (Anderson et al 2008)
  - Economics of malware (OECD 2008)
Outline

- Anti-Phishing expert interview study
- Empirical study on browser phishing warnings
- Anti-Phishing Phil
- Phishing Susceptibility Study
- Conclusions
Empirical study on browser phishing warning

- Browser is a strategic place to protect users, and major browsers provide phishing warnings based on blacklists and heuristics
  - What is the accuracy and update speed of blacklists?
  - What is the accuracy of heuristics?
  - How to improve protection?

Methodology

- Used an automated test bed with fresh phish to evaluate 8 popular phishing toolbars
- Conducted two tests in October and December 2008
- Tested 191 fresh phish and 13,458 HAM URLs
- For each phish tested 9 times in 48 hours for blacklist update
Automated Testbed

<table>
<thead>
<tr>
<th>Toolbar</th>
<th>Version</th>
<th>Techniques</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Explorer 7</td>
<td>7.0.5730.11</td>
<td>Blacklist + heuristics</td>
</tr>
<tr>
<td>Internet Explorer 8</td>
<td>8.0.6001.18241</td>
<td>Blacklist only</td>
</tr>
<tr>
<td></td>
<td>BETA 2</td>
<td></td>
</tr>
<tr>
<td>Firefox 2</td>
<td>2.0.0.16</td>
<td>Blacklist only</td>
</tr>
<tr>
<td>Firefox 3</td>
<td>3.0.1</td>
<td>Blacklist only</td>
</tr>
<tr>
<td>Google Chrome</td>
<td>0.2.149.30</td>
<td>Blacklist only</td>
</tr>
<tr>
<td>Netcraft</td>
<td>1.8.0</td>
<td>Blacklist only</td>
</tr>
<tr>
<td>Siteadvisor</td>
<td>2.8.255</td>
<td>Blacklist only</td>
</tr>
<tr>
<td>Norton 360</td>
<td>13.3.5</td>
<td>Blacklist + heuristics</td>
</tr>
</tbody>
</table>
Summary of results

- 70% of phishing campaigns in our dataset lasted less than one day
- Zero hour protection for blacklists is between 15-40%
- Most tools detect > 60% after 5 hours
- Tools that use heuristics caught significantly more phish
- False positive rates are very low for both blacklists and heuristics
Blacklist performance - October

- Firefox 2, 3
- Chrome blacklist
- IE8 / IE7 blacklist
- NetCraft blacklist
- McAfee Site Advisor blacklist
- Symantec Norton 360 blacklist

Percentage of Phish in blacklist vs Hours After Receiving URL
## Heuristics

<table>
<thead>
<tr>
<th></th>
<th>Detected by blacklist at hour 0</th>
<th>Detected by heuristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>IE 7 – Oct 08</td>
<td>23%</td>
<td>41%</td>
</tr>
<tr>
<td>Symantec – Oct 08</td>
<td>21%</td>
<td>73%</td>
</tr>
<tr>
<td>IE 7 – Dec 08</td>
<td>15%</td>
<td>25%</td>
</tr>
<tr>
<td>Symantec – Dec 08</td>
<td>14%</td>
<td>80%</td>
</tr>
</tbody>
</table>
Recommendations

- Clarify the legal issues surrounding false positives of heuristics
- Focus heuristics research on reducing false positives
- Leverage heuristics to improve blacklist
Leverage heuristics to improve blacklist
Related work

- Phishing toolbar test
  - HP study (2006)

- Effectiveness of spam blacklists
  - J. Jung and E. Sit (2006)
Outline

- Anti-Phishing expert interview study
- Empirical study on browser phishing warnings
- Anti-Phishing Phil
- Phishing Susceptibility Study
- Conclusions
Design Motivations

- Security is secondary task
- Learning by doing
- Fun and engaging
- Better strategies
Anti-Phishing Phil

- **Online game**
  - Teaches people how to protect themselves from phishing attacks
  - Identify phishing URLs
  - Use web browser cues
  - Find legitimate sites with search engines

Design Methodology

- Design Principles
  - Reflection principle, story-based agent environment principle, conceptual and procedural knowledge principle
- Multiple iterations
  - Early iterations made use of paper and Flash prototypes
  - Play-testing and feedback from research group
  - Developed a working prototype that we tested with actual users
  - Iterated on the design several more times based on user feedback and behavior
  - Polish with attractive images and enticing sounds
http://165.246.121.80/wamu/
Good job spotting numbers in the URL.
Don't trust URLs with all numbers in the front.

Congratulations! You May Proceed to the Next Round

(✓) correct choice  (✗) incorrect choice

✓ http://165.246.121.80/wamu/  SCAM ALERT! URLs with all numbers in the front are usually scam.

✓ http://www.msn-verify.com/  SCAM ALERT! Keywords such as verify, update in the domain usually means it is scam.

✓ http://www.chase.com  Chase.com is part of the J.P. Chase Corporation.

✓ https://www3.nationalgeographic.com/  Don't be fooled by the www3, this site belongs to nationalgeographic.com

✓ http://www.onlineregionsbank.com/  SCAM ALERT! Regions bank website is regions.com, not onlineregionsbank.com


✗ http://147.91.75.1/ebay/  SCAM ALERT! URLs with all numbers in the front are usually scam.

✗ http://www.amazon.com  amazon.com is the shopping site Amazon.
How to Avoid Online Scams!

You can also search the brand name "Citizens Bank", and go to the real site.
Summary of Evaluation of Anti-Phishing Phil

- Test participants’ ability to identify phishing web sites before and after 15 min of training
  - 10 web sites before training, 10 after, randomized order

- Evaluation I: Lab study
  - How does Phil compare with existing training materials?

- Evaluation II: Online study
  - How well do people retain what they learned
Evaluation I Results

- Game group had the best performance overall
- Game group had fewest false positives
- No significant difference in false negatives among the three groups
Evaluation II: Online Study

Help Us With Our Research!

Enter to win a $100 Amazon gift certificate!!!

Take a short 6-question phishing quiz before you play the game, another 6-question quiz after you play the game, and another 6-question quiz one week later for a chance to win a $100 Amazon gift certificate. The quizzes and game should take about 12 minutes. If you get at least 80% of the quiz questions right you will get an extra raffle ticket.

We will record your quiz scores and answers to the survey questions and use them in our research. However your scores and responses will not be identified with your name.

You must be 13 or older to participate.

CONTINUE

Study Set-up

- 6 websites before training, 6 immediately after and 6 one week later
- Conditions
  - Control: 2496 in control group
  - Game: 2021 users, 674 returned one week after
Results

<table>
<thead>
<tr>
<th>Level</th>
<th>Pre test</th>
<th>Post test</th>
<th>One Week Later</th>
</tr>
</thead>
<tbody>
<tr>
<td>Novice (N = 46)</td>
<td>29.7%</td>
<td>77.5%</td>
<td>76.8%</td>
</tr>
<tr>
<td>Intermediate (N = 256)</td>
<td>59.9%</td>
<td>84.6%</td>
<td>85.0%</td>
</tr>
<tr>
<td>Expert (N = 372)</td>
<td>92.5%</td>
<td>93.5%</td>
<td>93.9%</td>
</tr>
</tbody>
</table>
Comments

- “I liked the game! It was fun to play and had a useful message.”
- “Excellent game. Getting people to actually learn is the tough part.”
- “Is it available to training facilities for use with Corporate compliance and Internet training classes?”
- “I plan to direct my mother to this site.”
Anti-Phishing Phil Dissemination

- Online since 9/2007, played over 110,000 times
- Covered in more than 30 articles
- Commercialized by Wombat Securities Technologies, and translated into Portuguese, Italian, and Japanese
Related work

- Why people fall phishing

- Education approaches
  - Online Training materials (Microsoft 07, eBay 06, MySecureCyberSpace 07)
  - Contextual training (Jagatic et al 2006, New York State Office 2007)
  - Embedded training (Kumaraguru et al 2007 2008)

- Other approaches
  - Phoolproof phishing (Parno et al 2006)
Outline

- Anti-Phishing expert interview study
- Empirical study on browser phishing warnings
- Anti-Phishing Phil
- Phishing Susceptibility Study
- Conclusions
Phishing Susceptibility Study

- A mechanical Turk study of 1001 users
  - Understand what demographics factors correlate with falling for phishing
  - Understand the effectiveness of educational interventions in bridging the divide
Methodology

- 1001 Participants completed survey from mTurk
  - 1962 responded, 64.4% (1263) qualified
- Participants assigned in one of 10 conditions:
  - Popular training material
  - Anti-Phishing Phil
  - PhishGuru Cartoon
  - Phil with PhishGuru Cartoon
  - Control

\[ X \times 2 \text{ orderings} \]
Role play survey

- Participants play the role of Pat Jones, a staff member from Baton Rouge University
- Each role play showed participants fourteen images of emails along with context about Pat Jones
- Participants were asked how they would handle the emails

Subject: Bandwidth Quota Offer
From: "Info Sec" <infosec@bru.edu>
Date: Thu, May 14, 2009 10:55am
To: "Pat Jones" <patjones@bru.edu>
Priority: Normal
Options: View Full Header | View Printable Version

Dear Student/Faculty/Staff,

Please click on the link below and read the ways that you read the guidelines and acknowledge that you have read

http://www.brubandwithamnesty.org/bandwidth/agree.htm

Info Sec
Baton Rouge University

☐ reply by email
☐ contact the sender by phone or in person
☐ forward the email to someone else
☐ delete the email
☐ keep, save or archive the email
☐ click on the selected link in the email
☐ click on a different link in the email
☐ other (please specify)
Please login to review the guidelines for increasing your quota.

User ID
Password
Login

Baton Rouge Certificates: Many of the services that use WebISO also use the Baton Rouge Certificates. If you haven’t already done so, you should install the Baton Rouge CA Root Certificates in your browser.

About this service. WebISO verifies the identity of Baton Rouge users. WebISO does not require installation of specialized software. However, your browser must be configured to accept cookies. This is the default configuration for all major web browsers. If you have disabled cookies in the past you will need to enable cookie support in your browser to use WebISO... [more]

☐ click on one or more links on this page
☐ enter requested information
☐ bookmark, save or archive this webpage
☐ visit another related webpage
☐ leave or close this website
☐ other (please specify)
Analysis

- Regression analysis of 22 variable predicting phishing
- 5 variables were significant at .01 level

<table>
<thead>
<tr>
<th>Model</th>
<th>Standardized Coefficients</th>
<th>t</th>
<th>Sig.</th>
</tr>
</thead>
<tbody>
<tr>
<td>info avoid phish: ever seen information</td>
<td>0.189</td>
<td>5.787</td>
<td>0.000</td>
</tr>
<tr>
<td>gender: survey</td>
<td>0.140</td>
<td>3.964</td>
<td>0.000</td>
</tr>
<tr>
<td>age_numeric</td>
<td>-0.116</td>
<td>-3.142</td>
<td>0.002</td>
</tr>
<tr>
<td>tech_knowledge</td>
<td>-0.103</td>
<td>-2.840</td>
<td>0.005</td>
</tr>
<tr>
<td>risk_financial_investing</td>
<td>-0.080</td>
<td>-2.518</td>
<td>0.012</td>
</tr>
</tbody>
</table>
Prior Exposure

- Participants who have seen phishing education before are less likely to click on phishing links or giving information to phishing websites (no significant difference for legitimate links and webpages)

<table>
<thead>
<tr>
<th>Ever seen information on avoiding phishing before?</th>
<th>No. of People (pnt)</th>
<th>Pre-test click phish</th>
<th>Pre test phish give</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>556 (57%)</td>
<td>2.64 (44%)</td>
<td>2.34 (39%)</td>
</tr>
<tr>
<td>Maybe</td>
<td>85 (9%)</td>
<td>3.46 (58%)</td>
<td>3.15 (53%)</td>
</tr>
<tr>
<td>No</td>
<td>342 (35%)</td>
<td>3.83 (64%)</td>
<td>3.58 (60%)</td>
</tr>
</tbody>
</table>
Gender

- Women were more likely than men to click on phishing links (5 percentage points) and enter information to phishing websites (12 percentage points)
- 97% of women continue to give information to the corresponding phishing website, while only 84% of men did

<table>
<thead>
<tr>
<th>Gender</th>
<th>No. of People (pnt)</th>
<th>Pre-test click phish</th>
<th>Pre test phish give</th>
</tr>
</thead>
<tbody>
<tr>
<td>Male</td>
<td>516 (52%)</td>
<td>2.95 (49%)</td>
<td>2.47 (41%)</td>
</tr>
<tr>
<td>Female</td>
<td>485 (48%)</td>
<td>3.28 (55%)</td>
<td>3.19 (53%)</td>
</tr>
</tbody>
</table>
Age

- Participant ages 18-25 fell for phishing more than other age groups
- Participant ages 36 – 45 fell for fewest phish

<table>
<thead>
<tr>
<th>Age Groups</th>
<th>No. of People (pnt)</th>
<th>Pre-test click phish</th>
<th>Pre test phish give</th>
</tr>
</thead>
<tbody>
<tr>
<td>18 - 25</td>
<td>415 (41%)</td>
<td>3.71 (62%)</td>
<td>3.30 (55%)</td>
</tr>
<tr>
<td>26 - 35</td>
<td>353 (35%)</td>
<td>2.96 (49%)</td>
<td>2.65 (44%)</td>
</tr>
<tr>
<td>36 - 45</td>
<td>118 (12%)</td>
<td>2.23 (37%)</td>
<td>2.24 (37%)</td>
</tr>
<tr>
<td>46 - 55</td>
<td>79 (8%)</td>
<td>2.39 (40%)</td>
<td>2.42 (40%)</td>
</tr>
<tr>
<td>&gt; 56</td>
<td>36 (4%)</td>
<td>2.50 (42%)</td>
<td>2.39 (40%)</td>
</tr>
</tbody>
</table>
Gender and phishing susceptibility

- Women were more likely than men to click on phishing links and enter information to phishing websites
  - H1: Women fall for more phishing because they have less technical knowledge and less technical training
  - H2: Women fall for more phishing because they have less exposure to phishing education

- Tested both hypothesis through a mediation analysis (Preacher and Hayers 2008)
Gender and phishing susceptibility

- H1: Accepted
- H2: Rejected
Age and phishing susceptibility

Exposed to training before

-0.30**

Total effect: 0.34 **
Direct effect: 0.12

Education

-0.16**

Year on internet

-1.31**

-0.06*

-0.13*

financial _risk_ investing

-0.14**

1.00**

Exposed to training before

-0.30**

Total effect: 0.34 **
Direct effect: 0.12

Education

-0.16**

Year on internet

-1.31**

-0.06*

-0.13*

financial _risk_ investing

-0.14**

1.00**
Effects of education

- Women learned more than men during the training on not following phishing links
- People of different age, education groups learned similarly during the training
Conclusions

- Education is effective and needed but not cure all
  - Make education fun and engaging
  - Focus education on people ages between 18 to 25
  - Complementing education with effective warning and better law enforcement
Outline

- Anti-Phishing expert interview study
- Empirical study on browser phishing warnings
- Anti-Phishing Phil
- Phishing Susceptibility Study
- Conclusions
Policy Recommendations

- Law enforcement
  - Recommend US government invest in tools for better case management and better digital evidence processing
  - Expand scholarship programs to recruit graduates in computer science and digital forensics and analysis
  - Facilitate greater information sharing between law enforcement and industry
Policy Recommendations

- Botnets
  - Recommend the US government institute a notice and takedown regime for bot C&C
  - Recommend the US government leverage technologies used in national defense
  - Recommend the US government establish close working relationship with other countries to share intelligence of the botnets
  - Research on automatically cleaning compromised machines needed
Policy Recommendations

- Misalignment of incentives
  - Recommend that the US government institute mandatory reporting for electronic crime

- False positives
  - Recommend that legislators clarify the legal issues surrounding the false positives of heuristics or provide incentives such as safe harbor legislation
Acknowledgements

- **Thesis committee:** Lorrie Cranor, Jason Hong, Alessandro Acquisti, and Adrian Perrig
- **Cybertrust Group and CUPS Lab**
- **Expert Interview study:** Ponnurangam Kumaraguru, Julie Downs
- **Anti-Phishing Phil:** Bryant Magnien, Ponnurangam Kumaraguru, Elizabeth Nunge, Patrick Kelly
- **Empirical Study on Phishing blacklists:** Serge Egelman, Yue Zhang, Brad Wardman and Gary Warner
- **Mechanical turk study:** Mandy Holbrook, Julie Downs and Joanna Breese
CMU Usable Privacy and Security Laboratory

http://cups.cs.cmu.edu/

Carnegie Mellon
Methodology

- Limitations
  - US centric view
  - Self selection bias
  - Experts not neutral
Varying Incentives

- Financial loss, regulatory oversight and reputation are primary drivers for financial institutions
  - A major US bank lost $4.5 million to phishing and malware in 12 months

- ISPs consider phishing as part of the spam problem
  - When phishing targets their webmail system, they are more aggressive
  - A major US ISP has 10% computers infected with malware
Issues of false positives

- Organizations conservative with filtering and warning of false positives
  - Browser vendors prefer blacklist over heuristics
- Fear of potential liability due to false positives
- Leads to repeated efforts and slow reaction
  - Registries consider false positive as their number one concern in anti-abuse policies
Recommendations

- Clarify the legal issue surrounding false positives of blacklists and heuristics
  - Lack of clarity reduce vendors’ incentives to use heuristics
  - “fear” of false positives rather than “actual” false positives
  - What level of accuracy heuristics can be used and not held liable?
## Stakeholders

<table>
<thead>
<tr>
<th>Category</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consumers</td>
<td>--</td>
</tr>
<tr>
<td>Organizations</td>
<td>US Military, Universities, Corporations</td>
</tr>
<tr>
<td>Financial Institutions</td>
<td>Bank of America, Citibank, Wachovia, Paypal</td>
</tr>
<tr>
<td>Merchants</td>
<td>eBay, Amazon</td>
</tr>
<tr>
<td>Internet Service Providers</td>
<td>SBC, Comcast, AOL</td>
</tr>
<tr>
<td>Email Providers</td>
<td>Gmail, YahooMail, Hotmail, Outlook</td>
</tr>
<tr>
<td>Browsers</td>
<td>Internet Explorer, Firefox, Safari, Opera, Netscape.</td>
</tr>
<tr>
<td>Registrars and Registries</td>
<td>Verisign, GoDaddy.</td>
</tr>
<tr>
<td>Software Vendors</td>
<td>Symantec, RSA, MarkMonitor.</td>
</tr>
<tr>
<td>Law Enforcements</td>
<td>Federal Bureau of Investigation(FBI), Secret Service, Identity Theft Divisions in Law enforcements.</td>
</tr>
<tr>
<td>Computer Emergency Response Teams</td>
<td>CERT, CSIRT</td>
</tr>
<tr>
<td>Academic Institutions</td>
<td>Carnegie Mellon University,</td>
</tr>
</tbody>
</table>

**Victims**

**Infrastructure providers**

**For-profit protectors**

**Public Protectors**
Summary of Recommendations

<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Responsible Parties</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1: Financial institutions should produce more accurate estimates of phishing losses and report these statistics.</td>
<td>Financial Institutions</td>
</tr>
<tr>
<td>R2: Regulators and academicians need to investigate the issue of incentives further.</td>
<td>Regulators and academicians</td>
</tr>
<tr>
<td>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.</td>
<td>Operating System vendors</td>
</tr>
<tr>
<td>R4: Stakeholder should focus on improving on the security of web applications.</td>
<td>Various stakeholders</td>
</tr>
<tr>
<td>R5: 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.</td>
<td>Web browser vendors</td>
</tr>
<tr>
<td>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.</td>
<td>Academics, for-profit protectors</td>
</tr>
<tr>
<td>R7: Clarify the legal issues of the false positives of blacklists and heuristics.</td>
<td>Legal community</td>
</tr>
<tr>
<td>R8: Create a central clearinghouse to quickly verify phishing reports coming into APWG and on vendor blacklists.</td>
<td>APWG</td>
</tr>
<tr>
<td>R9: Academics should focus heuristic research on reducing false positives.</td>
<td>Academia</td>
</tr>
</tbody>
</table>
# Summary of Recommendations

<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Responsible Party</th>
</tr>
</thead>
<tbody>
<tr>
<td>R10: ICANN should improve enforcement on domain abuse.</td>
<td>ICANN</td>
</tr>
<tr>
<td>R11: ICANN should encourage registries to adopt anti-abuse policies.</td>
<td>ICANN</td>
</tr>
<tr>
<td>R12: Improve and invest more into law enforcement, specifically for international cooperation.</td>
<td>US Government</td>
</tr>
<tr>
<td>R13: US Government should invest in technologies to provide law enforcement with better analytical capability to prioritize and manage cases.</td>
<td>US Government</td>
</tr>
<tr>
<td>R14: More corporations aggregating fraud data and submit to law enforcement to identify proxies.</td>
<td>Law enforcement, ISP, academia</td>
</tr>
<tr>
<td>R15: Continue to strengthen collaboration between law enforcement in different countries, public and private protectors.</td>
<td>Law enforcement</td>
</tr>
<tr>
<td>R16: Academicians and industry continue to make education fun and engaging and up to date.</td>
<td>Academician, industry</td>
</tr>
<tr>
<td>R17: Launch education campaign to educate the public about mules, and encourage social networking sites to take initiative to educate their customers.</td>
<td>US Government</td>
</tr>
<tr>
<td>R18: Complement education with other countermeasures such as filtering and better user interface design.</td>
<td>Academician</td>
</tr>
</tbody>
</table>
BACKGROUND BACKUP SLIDES
Phishing Life cycles

- Preparation
- Attack
- Fraud
- Collection
- Post-attack
Traditional criminal techniques

Burglary: Breaking into a building with the intent to steal.

Deceptive callers: Criminals who telephone their victims and ask for their financial and/or personal identity information.

Extortion: Illegal use of force or one’s official position or powers to obtain property, funds, or patronage.

Fraud: Deceit, trickery, sharp practice, or breach of confidence, perpetrated for profit or to gain some unfair or dishonest advantage.

Identity theft: Impersonating or presenting oneself as another in order to gain access, information, or reward.

Child exploitation: Criminal victimization of minors for indecent purposes such as pornography and sexual abuse.

Cybercrime

Hacking: Computer or network intrusion providing unauthorized access.

Phishing: A high-tech scam that frequently uses unsolicited messages to deceive people into disclosing their financial and/or personal identity information.

Internet extortion: Hacking into and controlling various industry databases (or the threat of), promising to release control back to the company if funds are received or some other demand satisfied.

Internet fraud: A broad category of fraud schemes that use one or more components of the Internet to defraud prospective victims, conduct fraudulent transactions, or transmit fraudulent transactions to financial institutions or other parties.

Identity theft: The wrongful obtaining and using of another person’s identifying information in some way that involves fraud or deception, typically for economic gain.

Child exploitation: Using computers and networks to facilitate the criminal victimization of minors.

Source: GAO 2007
New Phishing Sites Reported to APWG by Month
Number of brands hijacked
Average time online for phishing sites

![Bar chart showing the average time online for phishing sites from October 2004 to December 2007. The x-axis represents the months, and the y-axis represents time in minutes. The chart shows a decrease in average time online over the years.](http://cups.cs.cmu.edu/)

---

**CyLab Usable Privacy and Security Laboratory**

[http://cups.cs.cmu.edu/](http://cups.cs.cmu.edu/)
Anti-phishing phil backup slides
Anti-Phishing Zé

Este jogo tem a finalidade de testar os conhecimentos sobre Phishing, ou seja, a análise e detecção de páginas de Internet falsas que têm como objectivo o roubo de logins e passwords.

Ao longo de quatro níveis serão apresentados urls que o utilizador terá de analisar e classificar como verdadeiros ou falsos, recebendo antes e durante cada nível dicas sobre Phishing.

Porque se trata de um jogo educativo relacionado com um tema sensível de segurança online, os resultados obtidos são enviados, sem qualquer informação sobre os utilizadores, para o SAPO e para a Universidade de Carnegie Mellon, para depois serem analisados e trabalhados quer no melhoramento do jogo, quer em campanhas educativas sobre Phishing.

O jogo Anti-Phishing Zé resulta de uma parceria entre a Carnegie Mellon University e o SAPO. Tendo sido desenvolvido inicialmente pelo CUPS (CMU Usable Privacy and Security Laboratory com fundos da US National Science Foundation e ARD/Cylab).
Evaluations I: Lab study

- Test participants’ ability to identify phishing web sites before and after training
  - 10 URLs before training, 10 after, randomized
  - Up to 15 minutes of training
- Training conditions:
  - Web-based phishing education
  - Tutorial
  - Game
- 14 participants in each condition
  - Screened out security experts
  - Younger, college students
### View Your Accounts

1. **Username:**
2. **Password:**
   - **Username Help**
   - **Password Help**

3. **Sign On to:**
   - **Account Summary**
   - **Sign On**

### Learn More About:

<table>
<thead>
<tr>
<th>Banking</th>
<th>Loans &amp; Credit</th>
<th>Investing &amp; Insurance</th>
<th>Financial Planning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online Banking</td>
<td>Credit Cards</td>
<td>Mutual Funds</td>
<td>Credit</td>
</tr>
<tr>
<td>Bill Pay</td>
<td>Home Equity Loans</td>
<td>Brokerage</td>
<td>Taxes</td>
</tr>
<tr>
<td>Checking</td>
<td>Home Mortgage</td>
<td>IRAs</td>
<td>Fraud Prevention</td>
</tr>
<tr>
<td>Check Card</td>
<td>Student Loans</td>
<td>Private Client Services</td>
<td>Retirement</td>
</tr>
<tr>
<td>Savings &amp; CDs</td>
<td>Auto Loans</td>
<td>Insurance</td>
<td>Maximize Your Account</td>
</tr>
<tr>
<td>More &gt;&gt;</td>
<td>More &gt;&gt;</td>
<td>More &gt;&gt;</td>
<td>More &gt;&gt;</td>
</tr>
</tbody>
</table>

### About Wells Fargo

- **Our Security Guarantee**
  - We guarantee your online security and partner with you to prevent fraud.

- **Check Today's Rates**
  - Mortgage, Home Equity, Credit Card, Personal Loans and more.

- **Open an Account Online**
  - It's fast, secure, and easy!
  - **Apply** instantly, or **finish** a saved application.
  - **Check** application status for select accounts.
  - **Learn** about your new account.

- **Need homebuying power?**
  - Becoming a Priority Buyer™ can help close the deal. >> Learn More

- **Business Ownership Opens Doors**
  - Build on your accomplishments

---

**Brokerage Products: Not FDIC Insured • No Bank Guarantee • May Lose Value**

Brokerage is offered through Wells Fargo Investments, LLC (member SIPC), a non-bank affiliate of Wells Fargo & Company and is intended only for United States residents. System response and account access times may vary due to a variety of factors.
CyLab Usable Privacy Laboratory

h7p://cups.cs.cmu.edu/
mTurk study backup slides
Study Design

CMU Email Usage Study (40-minute study for those who qualify)

Research study about computer use.
Sponsor: National Science Foundation.

Researchers at Carnegie Mellon University in Pittsburgh, PA are looking for people over the age of 18 to participate in a survey about emails and websites and also to review computer-related educational materials. The survey will take around 40 minutes to complete. Participants will be paid $4.00 through mTurk if qualified. Those who don't qualify get 20¢ bonus for a 2-minute short survey, however your HIT will be rejected.

1) Must use Internet Explorer or Firefox.
2) Must be over 18 to participate.
3) Have not participated in this study before.

How to participate:
1) Accept this HIT from mTurk.

2) Go the following url and fill out the survey
http://cups.cs.cmu.edu/email_survey/

3) At the end of the survey, you will be given a completion code by us, paste the completion code from the survey into the question box below, and click Submit HITs to finish.

Please contact risk-center [at] andrew.cmu.edu if you have any questions about this study.
Effects of education

- All training materials reduce users' tendency to enter information into phishing webpages by 16 - 21 percentage points (no significant change for control group)
- All training except for Anti-Phishing Phil decrease participants’ tendency to click on legitimate links slightly
Technology knowledge

- Participants’ self-rated tech knowledge also significant predicts whether they will fall for phishing

<table>
<thead>
<tr>
<th>Tech knowledge</th>
<th>No. of People (pnt)</th>
<th>Pre test phish give</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low (1 - 3)</td>
<td>63 (6%)</td>
<td>3.33 (56%)</td>
</tr>
<tr>
<td>Medium (3 – 6)</td>
<td>531 (54%)</td>
<td>3.18 (53%)</td>
</tr>
<tr>
<td>High (6 – 7)</td>
<td>389 (40%)</td>
<td>2.29 (38%)</td>
</tr>
</tbody>
</table>
Financial risk perception

- The more risk averse a participant is, the less likely he or she will fall for phish

<table>
<thead>
<tr>
<th>Risk Aversion</th>
<th>No. of People (pnt)</th>
<th>Pre test phishing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low (1 - 3)</td>
<td>201</td>
<td>3.2 (53%)</td>
</tr>
<tr>
<td>Medium (3 – 5)</td>
<td>515</td>
<td>2.9 (48%)</td>
</tr>
<tr>
<td>High (5 – 7)</td>
<td>267</td>
<td>2.6 (43%)</td>
</tr>
</tbody>
</table>
Testbed backup slides
Length of Phishing Campaigns

- March - April (5491 URLs)
- Testbed data (191 URLs)
Protect Rate - October

- Firefox 2, 3, Chrome
- IE 7
- IE 8
- NetCraft
- McAfee Site Advisor
- Symantec Norton 360
- Sites taken down
Other backup slides
Contributions

- Anti-Phishing Phil showed that computer users can be trained to make better online trust decisions if the training materials are presented in a fun and interactive manner and grounded in learning science principles.

- Semi-structured interviews with 31 anti-phishing led to eight key findings and 18 recommendations to improve phishing countermeasures.
Contributions

- We studied the effectiveness of popular phishing tools that is used by major web browsers. 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. We recommend toolbars vendors use heuristics to complement blacklists to speed up phishing detection.

- We studied demographics and phishing susceptibility with an role play survey administered to 1001 users of Mechanical Turk. This research is the first study that studied demographics factors contributing to susceptibility to semantic attacks. We also demonstrated the successful use of mechanical turk to conduct online experiments.