Leveraging Human Factors for Effective Security Training

FISSEA 2012

Jason Hong
jasonh@cs.cmu.edu
About the Speaker

- Associate Prof, Carnegie Mellon University, School of Comp Science
- Research and teaching interests:
  - Usable privacy and security
  - Mobile computing
- Co-author
- Startup

©2012 Carnegie Mellon University
About this Talk

- Useful for people interested in:
  - How to effectively train people?
  - How to effectively design better user interfaces for privacy and security?

- Two case studies from my research
Human Element of Security

- People are key part of computer security for every organization
  - Keeping passwords strong and secure
  - Avoiding social engineering
  - Avoiding malware
  - Appropriate use of social networking
  - Keeping mobile devices secure

- Overlooking human element is most common mistake in computer security
What is Human-Computer Interaction?

Field that seeks to understand the relationship between people & computers

- Designing useful, usable, desirable artifacts
- Understanding how people use systems
- Expanding the ways we can use computers

Combines behavioral sciences, interaction design, and computer science
Interactions Can Be Successful
Interactions Can Also Fail
How do people believe how things work?

Mental models describe how a person thinks something works.
Incorrect mental models can make things very hard to understand and use.
Mental Models Example: Refrigerator

Freezer
(temperature too cold)

Fresh food
(temperature just right)
Refrigerator Controls

Normal Settings: C and 5
Colder Fresh Food: C and 6-7
Coldest Fresh Food: B and 8-9
Colder Freezer: D and 7-8
Warmer Fresh Food: C and 4-1
OFF (both): 0

What is a typical conceptual model?
A Common Conceptual Model

Most people think of

independent controls
Now can you fix the problem?

Two general solutions:
- make controls map to user’s mental model
- foster a more accurate mental model
Three Different Models

- **Design Model**
  (How you intend the system to work)

- **User Model**
  (How users think the system works)

- **System Image**
  (Your implementation)

Users create a model from what they hear from others, past experiences, and usage – interactions with system image.
Mental Models

People inevitably build models of how things work
- Ex. children and computers
- Ex. you and your car
- Ex. how hackers work (and why)
- Ex. visibility in social networking sites
- Ex. app stores (all apps vetted by Google?)

Two options:
- Make the system match people’s models
- Foster a better mental model
Example: Phishing Attacks

Interviewed 40 people as part of an “email study” (Downs et al, SOUPS 2006)

Only 55% of participants said they had ever noticed an unexpected or strange-looking URL

– Most did not consider them to be suspicious
Example: Phishing Attacks

- 55% of participants reported being cautious when email asks for sensitive financial info
  - But very few reported being suspicious of email asking for passwords

- Knowledge of financial phish reduced likelihood of falling for these scams
  - But did not transfer to other scams, such as an amazon.com password phish
We Educate End-Users?

Users not motivated to learn
Security is a secondary task
Difficult to teach
Without increasing false positives
Basically, educating users is
As hard as herding cats
Yes, End-Users **Are** Trainable

Our research demonstrates users can learn how to protect themselves... if you can get them to pay attention to training.

Problem is that today’s training often boring, time consuming, and ineffective:
- All day lecture, no chance to practice skills
- Or passively watching videos
- Or posters and mugs and calendars
- Raise awareness, but little on what to actually do
How Do We Get People Trained?

Create “teachable moments”

Micro-games for training (fun)

Use learning science principles throughout
PhishGuru Embedded Training

Send simulated phishing emails
If recipient falls for it, show intervention
that teaches what cues to look for in
succinct and engaging format
– Useful for people who don’t know
  that they don’t know
Multiple user studies have demonstrated
that PhishGuru is effective
Delivering training via direct email
not effective
<table>
<thead>
<tr>
<th>Name</th>
<th>Date</th>
<th>Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jones</td>
<td>Mar 12, 2007</td>
<td>Will pick you up in 60 minutes</td>
</tr>
<tr>
<td>Li</td>
<td>Mar 12, 2007</td>
<td>Conference room #2 - reservation</td>
</tr>
<tr>
<td></td>
<td>Mar 12, 2007</td>
<td>Your IKEA order confirmation</td>
</tr>
<tr>
<td></td>
<td>Mar 12, 2007</td>
<td>Reactivate your eBay account</td>
</tr>
<tr>
<td></td>
<td>Mar 12, 2007</td>
<td>How about lunch together tomorrow?</td>
</tr>
<tr>
<td>How Fitzgerald</td>
<td>Mar 12, 2007</td>
<td>sexy baby and bad erection?</td>
</tr>
<tr>
<td>Josh Dicosta</td>
<td>Mar 12, 2007</td>
<td>tomorrow's meeting rescheduled</td>
</tr>
<tr>
<td>Taka Berdford</td>
<td>Mar 12, 2007</td>
<td>View my photos on Yahoo! Photos</td>
</tr>
<tr>
<td>Josh Dicosta</td>
<td>Mar 12, 2007</td>
<td>document dropped - your office - please fax</td>
</tr>
<tr>
<td>Days Bank</td>
<td>Mar 12, 2007</td>
<td>Update your account information</td>
</tr>
<tr>
<td>Williams</td>
<td>Mar 12, 2007</td>
<td>Sushi making party</td>
</tr>
<tr>
<td>Cheng</td>
<td>Mar 12, 2007</td>
<td>[cognizx] Dinner menu selection - Annual day</td>
</tr>
<tr>
<td>Bank</td>
<td>Mar 12, 2007</td>
<td>Citibank Urgent E-mail Verification</td>
</tr>
<tr>
<td>Li</td>
<td>Mar 12, 2007</td>
<td>Business cards</td>
</tr>
<tr>
<td></td>
<td>Mar 12, 2007</td>
<td>A warm Hello from Jesse</td>
</tr>
</tbody>
</table>
Subject: Revision to Your Amazon.com Information

From: "Amazon" <service@amazon.com>
Date: Mon, March 12, 2007 4:15 pm
To: bsmith@cognix.com
Priority: Normal

Please login and enter your information

[updated link to update personal information]

Please note the verification process you must fill in all the required fields.

Important: If you don't update your information within next 48 hours, we will be forced to suspend your account until you have the time to contact us by

We appreciate your support and understanding, as we work together to keep amazon market a safe place to trade. Thank you for your attention on this matter and we apologize.
Learning Science

- Area of research examining learning, retention, and transfer of skills
- Example principles
  - Learning by doing
  - Immediate feedback
  - Conceptual-procedural
  - Reflection
  - ... many others
Evaluation of PhishGuru

- Is embedded training effective?
  – We’ve conducted 4 peer-reviewed studies showing embedded training works well
  – Studies showed significant decrease in falling for phish and ability to retain what they learned


Results of One Study

Tested 500+ people in one month
- 1 simulated phish at beginning of month, testing done at end of month

~50% reduction in falling for phish
- 68 out of 85 surveyed said they recommend continuing doing this sort of training in the future
- “I really liked the idea of sending [organization] fake phishing emails and then saying to them, essentially, HEY! You could've just gotten scammed! You should be more careful – here's how...”
Can Browser Interfaces Help?

- Modern web browsers come with blacklists and special interfaces for identifying phish
  - Our evaluation of several blacklists show they catch ~80% of phish after 24 hours, not very good in first few hours

- Are these browser interfaces effective?
  - And, what can we learn from them?
  - Science of Warnings from human factors
This might be a phishing website.

Phishing websites impersonate trustworthy websites for the purpose of obtaining your personal or financial information.

Microsoft recommends that you do not give any of your information to such websites.

Report whether or not this is a phishing website.
This is a reported phishing website


Internet Explorer has determined that this is a reported phishing website. Phishing websites impersonate other sites and attempt to trick you into revealing personal or financial information.

We recommend that you close this webpage and do not continue to this website.

✔ Click here to close this webpage.

❌ Continue to this website (not recommended).

More information

Report that this is not a phishing website.
Suspected Web Forgery

This page has been reported as a web forgery designed to trick users into sharing personal or financial information. Entering any personal information on this page may result in identity theft or other fraud.  

Get me out of here! Ignore this warning

[ This isn't a web forgery ]
How Effective are these Warnings?

Tested four conditions
- FireFox Active Block
- IE Active Block
- IE Passive Warning
- Control (no warnings or blocks)

“Shopping Study”
- Setup phishing pages and added to blacklists
- Phished users after real purchases (2 phish)
- Used real email accounts and personal info

S. Egelman, L. Cranor, and J. Hong. You’ve Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing
How Effective are these Warnings?

<table>
<thead>
<tr>
<th>Condition Name</th>
<th>Size</th>
<th>Clicked</th>
<th>Phished</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firefox</td>
<td>20</td>
<td>20</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>Active IE</td>
<td>20</td>
<td>19</td>
<td>9 (45%)</td>
</tr>
<tr>
<td>Passive IE</td>
<td>10</td>
<td>10</td>
<td>9 (90%)</td>
</tr>
<tr>
<td>Control</td>
<td>10</td>
<td>9</td>
<td>9 (90%)</td>
</tr>
</tbody>
</table>

Almost everyone clicked, even those without a technical background.
How Effective are these Warnings?

No one in Firefox condition fell for our phish
People in Firefox condition not more technically savvy

<table>
<thead>
<tr>
<th>Condition Name</th>
<th>Size</th>
<th>Clicked</th>
<th>Phished</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firefox</td>
<td>20</td>
<td>20</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>Active IE</td>
<td>20</td>
<td>19</td>
<td>9 (45%)</td>
</tr>
<tr>
<td>Passive IE</td>
<td>10</td>
<td>10</td>
<td>9 (90%)</td>
</tr>
<tr>
<td>Control</td>
<td>10</td>
<td>9</td>
<td>9 (90%)</td>
</tr>
</tbody>
</table>
Discussion of Phish Warnings

Nearly everyone will fall for highly targeted and contextualized phish

Passive IE warning failed for many reasons

– Didn’t interrupt the main task
– Can be slow to appear (up to 5 seconds)
– Not clear what the right action was
– Looked too much like other ignorable warnings (habituation)
– Bug, any keystroke dismissed
**Internet Explorer – Passive Warning**

http://www.amazonaccounts.net/gp/sign-in.htm

Suspicious website

This might be a phishing website.

Phishing websites impersonate trustworthy websites for the purpose of obtaining your personal or financial information.

Microsoft recommends that you do not give any of your information to such websites.

Report whether or not this is a phishing website.
Discussion of Phish Warnings

Active IE warnings
- Most saw the warning, but many did not believe it
  - “Since it gave me the option of still proceeding to the website, I figured it couldn’t be that bad”
- Some element of habituation (looks like other warnings)
- Saw two pathological cases
This is a reported phishing website


Internet Explorer has determined that this is a reported phishing website. Phishing websites impersonate other sites and attempt to trick you into revealing personal or financial information.

We recommend that you close this webpage and do not continue to this website.

- Click here to close this webpage.
- Continue to this website (not recommended).

More information

Report that this is not a phishing website.
This website has been reported as unsafe
207.68.169.170

We recommend that you do not continue to this website.

✔ Go to my homepage instead

取消 and continue (不推荐)

This website has been reported to Microsoft for containing threats to your computer that might reveal personal or financial information.
Report that this is not an unsafe website.

更多信息

This website has been reported to contain the following threats:
- Malicious software threat: This site contains links to viruses or other software programs that can reveal personal information stored or typed on your computer to malicious persons.
A Science of Warnings

- HIP model for real-world warnings

See the warning?
Understand it?
Believe it?
Motivated?
Can and will act?
Designing for Path of Least Resistance

Where possible, make the default behavior safe
- Ex. The two pathological cases
  - Assume people won’t see, read, believe, or be motivated

Active warnings over passive warnings
- Interrupt people if warning is important
- Need to balance this with habituation

Make important warnings look very different
Summary

- Human element most overlooked aspect of computer security
  - Ex. phishing scams, passwords, mobile
- Mental models important to design
  - Mismatched models can cause failures
- Security training can work if done right
  - Learning sciences
- C-HIP model for security warnings
  - Do people see, understand, believe, and can act on warnings?
More of Our Research

Our team does research on:
- Better password policies
- Alternatives to passwords
- Mobile apps, privacy and security
- Location-based services and privacy
- Social networking and privacy
- Configuring firewalls
More of Our Research

- http://cups.cs.cmu.edu
- http://mcom.cs.cmu.edu
- http://cmuchimps.org/
Thanks, where can I learn more?

Find more at wombatsecurity.com

jasonh@cs.cmu.edu
Micro-Games for Cyber Security

Training doesn’t have to be long & boring

Micro game format, play for short time

Two-thirds of Americans played a video game in past six months

Not just young people
  - Average game player 35 years old
  - 25% of people over 50 play games

Not just males
  - 40% of casual gamers are women
Case Study: Anti-Phishing Phil

Tested Anti-Phishing Phil with ~4500 people
- Huge improvement by novices in identifying phishing URLs
- Also dramatically lowered false positives
Good job spotting numbers in the URL.
Don't trust URLs with random looking letters and numbers.
Round 1 Over

Congratulations! You may proceed to the next round.

Correct choice  Incorrect choice

SCAM ALERT! Don't trust URLs with all numbers in the front.

http://0xd3.0x8a.0x03/chase.com/
SCAM ALERT! URLs with all numbers in the front are usually a scam.

http://www.citicbanking.net
The real site is citibank.com.

https://bankus.etrade.com/
If you are not familiar with this site, google "etrade".

http://147.46.236.55/PayPal/login.html
SCAM ALERT! URLs with all numbers in the front are usually a scam.

https://www.wellsfargo.com
www.wellsfargo.com belongs to Wellsfargo Bank.

https://www.citizensbank.com
citizensbank.com belongs to Citizens Bank.

https://www.chase.com
chase.com is part of the J.P. Chase Corporation.
How to Avoid Online Scams

Within the address the right hand side is the most important! It shows the site name.

I got it PhishGuru! The name of the site is wombank.com!
False negatives for users who played Anti-Phishing Phil ("game condition"). False negatives are situations where people incorrectly label a phishing site as legitimate. Novices saw the greatest reduction in false negatives, and retained what they had learned.
False positives for users who played the Anti-Phishing Phil game. False positives are situations where people incorrectly label a legitimate site as phishing. Again, novices saw the greatest improvement in reducing false positives, and retained what they had learned.
Example Topic: Email Security

eight security

To: Phyllis
From: Human Resources
Subject: Information required

Dear Phyllis,

We are moving our tax records to a new system and need you to verify your tax information for us. Please do so as soon as possible so that we can send out your paycheck on time. Please reply with the following information filled in:

Full name:
Soc. Sec. #:
Date of Birth:
Number of dependents:

Thank you for your attention in this matter.
Office of Human Resources
Example Topic: Passwords

Great job!
Congratulations! Click "Next" to continue...

Phrase-based passwords

1. Read the provided phrase
2. Use the phrase method to create a strong password
3. Use the "hint" button if you get stuck

three times seven

3X$sevEn

strong

Create two strong passwords to move on!
Other Training: Social Networks

4 ways to Spot scams.

3.b The message doesn’t look “normal”
Does the grammar of the message not match how your friend usually writes?

Bob Sullivan
"Looking forward to hiking this weekend!"
2 hours ago · Like · Comment

Normal post from Bob.

Bob Sullivan
"I found out who has a crush on me! You can 2!!
2 hours ago · Like · Comment

Weird post from Bob.

Bob’s account has probably been compromised and the message is a scam.
Measurable
Most Missed

- http://member.bankofthewest-online.com/
- https://onlinebanking.bankofoklahoma.com/OnlineBancorp/
- http://newyork.craigslist.org/cgi-bin/apartments.c
- http://www.latam.citibank.com/uruguay/
- https://www.regionamortgage.com
- http://www.msn-vetry.com/
- http://entertainment-memorabilia.listings.ebay.com
- http://www.regionsbanking.com
- https://www.Officewear.com

Welcome admin! Change Password Log Off
Case Study #1: PhishGuru

Canadian healthcare organization
Three-month embedded training campaign
- 190 employees
- Security assessment and effective training in context
Simulated Phishing Email

Dear Yahoo Client,

Your records indicate that you have not changed your account password in the last 90 days, if you do not change your password in the next 5 days, your access to the email system will be terminated. Click the link below to update your password.

https://www.yahoo.com/password/change.htm

Sincerely,

Yahoo Service Desk
Case Study

PhishGuru™

Campaign Responses

Viewed and Clicked Link
35
18.42%

Campaign Statistics

Emails Sent: 190 of 190
Views: 55 of 190 people have viewed or clicked the email.
Campaign Start Date: May 04, 2010
Campaign End Date: Jun 01, 2010
# Measurable Reduction in Falling for Phish

<table>
<thead>
<tr>
<th>Campaign</th>
<th>Viewed Email Only</th>
<th>%</th>
<th>Viewed Email and Clicked Link</th>
<th>%</th>
<th>Employees</th>
</tr>
</thead>
<tbody>
<tr>
<td>Campaign 1</td>
<td>20</td>
<td>10.53%</td>
<td>35</td>
<td>18.42%</td>
<td>190</td>
</tr>
<tr>
<td>Campaign 2</td>
<td>37</td>
<td>19.47%</td>
<td>23</td>
<td>12.11%</td>
<td>190</td>
</tr>
<tr>
<td>Campaign 3</td>
<td>7</td>
<td>3.70%</td>
<td>10</td>
<td>5.29%</td>
<td>189</td>
</tr>
</tbody>
</table>
Can We Educate End-Users?

- Users are motivated to learn.
- Security is a secondary task.
- Difficult to teach people right decisions without increasing false positives.

"Users can not make time consuming decisions with a nail in their head."  

"Use of time consuming decisions with a nail in their head."  

-- An IBM security specialist