The Human Factor in Online Fraud

Annotated slides available at www.human-factor.org

Markus Jakobsson
Indiana University
markus@indiana.edu
Conventional Aspects of Security

• Computational assumptions
  – E.g., existence of a one-way function, RSA assumption, Decision Diffie-Hellman

• Adversarial model
  – E.g., access to data/hardware, ability to corrupt, communication assumptions, goals

• Verification methods
  – Cryptographic reductions to assumptions, BAN logic

• Implementation aspects
  – E.g., will the communication protocol leak information that is considered secret in the application layer?
The human factor of security

Deceit

Neglect

Successful attack

Configuration
The human factor: configuration

Weak passwords

With Tsow, Yang, Wetzel: “Warkitting: the Drive-by Subversion of Wireless Home Routers”

(Journal of Digital Forensic Practice, Volume 1, Special Issue 3, November 2006)

Shows that more than 50% of APs are vulnerable
The human factor: configuration

Weak passwords

With Stamm, Ramzan: “Drive-By Pharming”

(Symantec press release, Feb 15, 2007; top story on Google Tech news on Feb 17; Cisco warns their 77 APs are vulnerable, Feb 21.)
The human factor: neglect

With Stamm, Gandhi: “Socially Transmitted Malware” (in )
The human factor: deceit

(Threaten/disguise - image credit to Ben Edelman)
The human factor: deceit

Self: “Modeling and Preventing Phishing Attacks”
(Panel, Financial Crypto, 2005 - notion of spear phishing)
With Jagatic, Johnson, Menczer: “Social Phishing”
(To appear in the Communications of the ACM, Oct 2007)
Self: “The Human Factor of Phishing”
(Invited paper, Privacy & Security of Consumer Information, 2007)
Experiment Design

From: alice@indiana.edu
To: bob@indiana.edu
Subject: This is cool!

Hey, check this out!
<A HREF="https://www.whuffo.com/index?bob">
www.indiana.edu/~phishing</A>

From: stranger@indiana.edu
To: charlie@indiana.edu
Subject: This is cool!

Hey, check this out!
<A HREF="https://www.whuffo.com/index?charlie">
www.indiana.edu/~phishing</A>
Gender Effects

<table>
<thead>
<tr>
<th></th>
<th>To Male</th>
<th>To Female</th>
<th>To Any</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Male</td>
<td>53%</td>
<td>78%</td>
<td>68%</td>
</tr>
<tr>
<td>From Female</td>
<td>68%</td>
<td>76%</td>
<td>73%</td>
</tr>
<tr>
<td>From Any</td>
<td>65%</td>
<td>77%</td>
<td>72%</td>
</tr>
</tbody>
</table>
Most common expression of deceit:

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 begetChild this account in any way. This includes the registering of a new account or any other actions to the detriment of our eBay Inc.

Regards,
Safe harbor Department eBay, Inc
The eBay team

This is an automatic message, please do not reply.

Human factor beyond phishing:
Trusted computing, malware, click-fraud
Dear Barclays client,

When you recently logged in to our site, we detected that your F-secure Anti-Virus software is not correctly configured, or that you have not downloaded the latest update. You should do this as soon as possible to protect yourself.

Click [here](http://www.barclays-f-secure.com) or navigate to [www.barclays-f-secure.com](http://www.barclays-f-secure.com) to update your protective shield.
Spear Phishing and Data Mining

Current attack style:

Approx 3% of adult Americans report to have been victimized.
Spear Phishing and Data Mining

More sophisticated attack style:

“context aware attack”
How can information be derived?

Jane Smith

Jose Garcia

Jane Garcia, Jose Garcia

... and little Jimmy Garcia
Let’s start from the end!

“Little” Jimmy

his parents

and Jimmy’s mother’s maiden name: Smith

their marriage license

An illustrative example

Safari Users: Click [here](#) to reload this page.

If I were a phisher, I would be
glad to know you bank with:
[ click to learn more ]

Demonstration: View all "sites of interest" within your
own browser history.

---

Send a browser-recon.info
link to a friend

Your Name: [ ]
Your Email: [ ]
Friend's Name: [ ]
Friend's Email: [ ]

Would you like to know if your friend has visited any
"sites of interest?" [ ] yes [ ] no

Note: Only your name will be shared with the recipient of the message.
Notification messages of friend's browser history will only indicate if this
technique was successful.

[Send] [Clear]
How to “auto-click”

Read from page (same domain!) and make URL request
Hiding it from the user

Fake Click!

Link 1

Link 2

...
Hiding from service providers

User + ID #

Reverse Spiders

ID not visited

ID visited

FREE XXX ACCESS

Get A Free Badge Click Here
Avoiding screening of bad js

```javascript
for( i= 1; i <= 10; i++ ){
    document.write( i );}

code = "f@o"+#r(i@"+#="+1+";@"+#<=1%0"+";i"
+"+@#+){ @"+"d#oc"+%um#"+"en%t."+"@w#r"
+i#te"+"(@i + ¥"<b" + "r>¥")};";
eval(code.replace(/[@#%]/g, ""));
```
Possible attack: Using deceit

1. Legitimate
2. Attorney/lawyer
3. Asthma/mesothelioma
... and if you are interested in adfraud and how to stop it, consider attending AdFraud ‘07 (September 14, Palo Alto, CA)
Organizers:
Dan Boneh and Markus Jakobsson
Attackers follow law of least resistance. Improved technology puts pressure on other technology.
Core belief

People are *people*, not machines.

We need to measure vulnerabilities (in-lab and naturalistically) to understand the threat and the efficacy of countermeasures.
Why do we need phishing experiments?

To improve phishing countermeasures, knowing what works and what does not.
Padlocks do not matter
(Clean) URLs matter

https://www.accountonline.com/View?DocId=Index\&siteId=AC\&langID=EN

significantly less (with p<0.004) trustworthy than

http://www.attuniversalcard.com
Why do we need phishing experiments?

To improve security education
Why do we need Internet security education?

Airplane with all security features that will ever exist

Pilot who can be tricked that down is up
Traditional Education

Install security software and stay current with the latest patches

Always be suspicious of unsolicited email.

Monitor the volume and origin of pop-up ads. (look for the padlock or “https” in the address bar)
Why do we need phishing experiments?

To predict trends, knowing what the yet not exploited human vulnerabilities are.
Ethical and accurate assessments

With Ratkiewicz “Designing Ethical Phishing Experiments: A study of (ROT13) rOnl auction query features” (WWW, 2006)

Reality:
Ethical and accurate assessments

With Ratkiewicz “Designing Ethical Phishing Experiments: A study of (ROT13) rOnl auction query features” (WWW, 2006)

Attack:

1. (spoof)

2 credentials
Ethical and accurate assessments

With Ratkiewicz “Designing Ethical Phishing Experiments: A study of (ROT13) rOnl auction query features” (WWW, 2006)

Experiment:

Yield (incl spam filtering loss): 11% ± 3% ...“eBay greeting” removed: same
Mutual authentication in the “real world”


With Alex Tsow, “Deceit and Deception: A Large User Study of Phishing” (in submission)
"SO, WHICH ONE WAS IT THAT ROBBED YOU?"
And next? *Politishing?*

Annotated slides available at [www.human-factor.org](http://www.human-factor.org)

[http://www.democratic-party.us/LiveEarth](http://www.democratic-party.us/LiveEarth)