Introduction to Usable Security

Content from:
- Teaching Usable Privacy and Security: A guide for instructors (http://cups.cs.cmu.edu/course-guide/)
- some slides/content from Dr. Lorrie Cranor, CMU
- some slides/content from Dr. Kasia Muldner, ASU
- some slides/content from Dr. Kirstie Hawkey, UBC
- some slides/content from SOUPS 2009 tutorial on Designing and Evaluating Usable Security and Privacy Technology
- some slides from presentations of LERSSE (lersse.ece.ubc.ca) members
THE TEASER
Users are the weakest link (?)…

A CRYPTO NERD'S IMAGINATION:

His laptop's encrypted. Let's build a million-dollar cluster to crack it.

No good! It's 4096-bit RSA!

Blast! Our evil plan is foiled!

WHAT WOULD ACTUALLY HAPPEN:

His laptop's encrypted. Drug him and hit him with this $5 wrench until he tells us the password.

Got it.
Sometimes...

Dogbert's Password Recovery Service for Morons

I don't remember my password.

Is it "123"?

That's just spooky.

Dogbert's Password Recovery Service for Morons

My name is Ned, I think.

Is your password "Ned"?

Sweet baby jeepers, you're like some sort of nostrildogmas!

Here's a brochure for my cult.
Now what?

Create a password that's at least six characters long with a mix of letters and numbers.

How about 123?

Uh, no.

It has to include letters and be at least six characters long.

How about ABC?

Letters and numbers and at least six characters long!!!

Foursome?

Gaaa!!!
But are we asking too much?

I AM MORDAC, THE PREVENTER OF INFORMATION SERVICES. I BRING NEW GUIDELINES FOR PASSWORDS.

“ALL PASSWORDS MUST BE AT LEAST SIX CHARACTERS LONG… INCLUDE NUMBERS AND LETTERS… INCLUDE A MIX OF UPPER AND LOWER CASE…”

USE DIFFERENT PASSWORDS FOR EACH SYSTEM. CHANGE ONCE A MONTH. SQUEAL LIKE A PIG !!!

DO NOT WRITE ANYTHING DOWN.

I AM MORDAC, THE PREVENTER OF INFORMATION TECHNOLOGY, AND I HAVE ASSIGNED YOU A NEW PASSWORD.

IT’S THE FULL TEXT OF “THE DA VINCI CODE,” EXCLUDING THE PARTS I DON’T BELIEVE.

I’M NOT TOUCHING YOU.

STUPID ANARTHROUS NOUN PHRASES.

© Scott Adams, Inc./Dist. by UFS, Inc.
Even biometrics can be painful...
Security as a barrier...

MORDAC, THE PREVENTER OF INFORMATION SERVICES.

SECURITY IS MORE IMPORTANT THAN USABILITY.

IN A PERFECT WORLD, NO ONE WOULD BE ABLE TO USE ANYTHING.

To complete the log-in procedure, stare directly at the sun.

© Scott Adams, Inc./Dist. by UFS, Inc.
Humans like to get past barriers.
Learning Objectives

- Develop awareness of usable security
- Understand the challenges of designing for security AND usability
- Obtain a little practical experience of looking at systems from a usability perspective
WHAT’S USABLE SECURITY?
Humans

“Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy when performing cryptographic operations. (They are also large, expensive to maintain, difficult to manage, and they pollute the environment. It is astonishing that these devices continue to be manufactured and deployed. But they are sufficiently pervasive that we must design our protocols around their limitations.)”

-- C. Kaufman, R. Perlman, and M. Speciner.

*Network Security: PRIVATE Communication in a PUBLIC World.*

Can we make systems secure AND usable?
usable security is about making systems secure and usable
example: access control in Windows

Designing and Developing Usable and Secure Systems

User-centred iterative approach

- Requirements gathering
- Iterative design and development process
- Prototype evaluation
- Design walkthroughs
- Heuristic evaluation
- Usability tests
  - Lab or field studies
Defining usability

Usability of fruit
Understand the user

WE'VE NARROWED OUR TARGET MARKET TO THIS GUY.

HE'S THE ONLY ONE RICH ENOUGH AND STUPID ENOUGH TO BUY OUR HIGH-END PRODUCT.

OUR DIAMOND-ENCRUSTED TIME MACHINE WILL TAKE YOU ONE HOUR INTO THE FUTURE IN ONLY SIXTY MINUTES!

© Scott Adams, Inc./Dist. by UFS, Inc.

$20,000 http://www.mobilewhack.com
Understand the usage context

Understand their expectations

- Society's expectations are reset every time a radically new technology is introduced.
- Expectations then move up the pyramid as that technology matures.
Plan the human-centred process

Understand and specify the context of use

Evaluate design against requirements

Specify the user and organizational requirements

 Produce design solutions

System meets requirements?
Can you accelerate the process?

- Ground your design in theory/related work
- Perform heuristic evaluation before involving users
  - Pros:
    - Quick & Dirty (do not need to design experiment, get users, etc)
    - Good for finding obvious usability flaws
  - Cons:
    - Experts are not the “typical” user!
General Usability Heuristics

- Heuristics as guidelines
  - Simple and natural dialogue
  - Speak the users' language
  - Minimize user memory load
  - Be consistent
  - Provide feedback
  - Provide clearly marked exits
  - Provide shortcuts
  - Deal with errors in positive and helpful manner
  - Provide help and documentation
Principles for Secure Systems (Yee 2002)

- **Path of Least Resistance**
  - Match the most comfortable way to do tasks with the least granting of authority.

- **Active Authorization**
  - Grant authority to others in accordance with user actions indicating consent.

- **Revocability**
  - Offer the user ways to reduce others' authority to access the user's resources.

- **Visibility**
  - Maintain accurate awareness of others' authority as relevant to user decisions.

- **Self-Awareness**
  - Maintain accurate awareness of the user's own authority to access resources.
Principles for Secure Systems (Yee 2002)

- **Trusted Path**
  - Protect the user's channels to agents that manipulate authority on the user's behalf.

- **Expressiveness**
  - Enable the user to express safe security policies in terms that fit the user's task.

- **Relevant Boundaries**
  - Draw distinctions among objects and actions along boundaries relevant to the task.

- **Identifiability**
  - Present objects and actions using distinguishable, truthful appearances.

- **Foresight**
  - Indicate clearly the consequences of decisions that the user is expected to make.

Users should:

■ Be reliably made aware of the security tasks they must perform
■ Be able to figure out how to successfully perform those tasks
■ Not make dangerous errors
■ Be sufficiently comfortable with the interface to continue using it
■ Be able to tell when their task has been completed
■ Have sufficient feedback to accurately determine the current state of the system
WHY IS USABILITY SO IMPORTANT TO CONSIDER?
Humans are weakest link

- Most security breaches attributed to “human error”
- Social engineering attacks proliferate
- Frequent security policy compliance failures
- Automated systems are generally more predictable and accurate than humans
Example

PRINCIPLE OF LEAST PRIVILEGE IN WINDOWS
User Account Usage

All 45 participants used Administrator user account on their laptops.
User Account Control (UAC)

- Implemented in Windows Vista & 7.
- UAC intended to make the use of low privilege accounts (LUAs) more convenient.

- Two user account types
  - Run with standard privileges
  - Elevate privilege by UAC prompt.
Windows administrative application

Signed application

Unsigned application
UAC prompt for admin account

Do you want to allow the following program to make changes to this computer?

- Program name: VNC Enterprise Edition for Windows
- Verified publisher: RealVNC Limited
- File origin: Hard drive on this computer

Show details

Yes   No

Change when these notifications appear

UAC prompt for non-admin account

Do you want to allow the following program to make changes to this computer?

- Program name: 7capture
- Verified publisher: IBE Software
- File origin: Hard drive on this computer

To continue, type an administrator password, and then click Yes.

Sara
Password

Yes   No
When participants were downloading, installing and running an application, 49% did not respond to UAC prompts correctly.

Because

They incorrectly thought the fake prompt was related to their current task.
When participants *initiated* an action that raised UAC prompts, most (95%) consented to these prompts.
Conclusions

- The User Account Control (UAC) was not applied by at least 69% of participants correctly
  - Those who understood UAC approach could use it correctly

- Low Privilege Accounts (LUA) were not used by any participants on their laptops
  - Lack of awareness about the benefit of LUAs and high risks of administrator accounts
  - Unsuccessful experience with LUAs
  - Relying on expertise and security software for keeping the system secure
The human threat

- Malicious humans who will attack system
- Humans who don’t know when or how to perform security-critical tasks
- Humans who are unmotivated to perform security-critical tasks properly or comply with policies
- Humans who are incapable of making sound security decisions
Key Usable Security Problem

- Security is a secondary task
  - Nobody buys a computer so they can spend time securing it.
  - Time we spend configuring security and privacy tools is time we are not spending doing what we really want to be doing with our computers.
Other Key Usability Problems

- Security systems and solutions are often complex
  - If the user cannot understand it, costly errors will occur
- Diverse users with diverse skills and diverse knowledge need to incorporate security in their daily lives
Grand Challenge

“Give end-users security controls they can understand and privacy they can control for the dynamic, pervasive computing environments of the future.”

- Computing Research Association 2003
Approaches to usable security

- Make it “just work”
  - Invisible security

- Make security/privacy understandable
  - Make it visible
  - Make it intuitive
  - Use metaphors that users can relate to
  - Help users make decisions

- Persuade the user to adopt security
- Train the user
Invisible Security

- When might this approach work?
example

Windows Vista Firewall
Personal Firewall
in
Windows Vista
Context Dependent Functionality

Settings *automatically* applied depending on network context detected

- **Public** (public networks)
- **Private** (home / work networks)
- **Domain** (controlled by Windows domain admin)
## Network Context in Vista Firewall

<table>
<thead>
<tr>
<th></th>
<th>Public Network Location</th>
<th>Private Network Location</th>
<th>Domain Network Location</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Wireless Network Connection</strong></td>
<td>On</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td><strong>Local Area Connection</strong></td>
<td>On</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td><strong>Bluetooth Network Connection</strong></td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
</tr>
</tbody>
</table>
2 User Interfaces:
Basic and Advanced
not intended for average users
complex
Does not provide necessary contextual information for the functionality it does support
Changes applied **only** to profile associated with current network location and that is not obvious.
Simplified interface:

- Hidden network context
- Automatic switching of firewall profiles

But at a cost!
What is the Cost?

• Users can be left in a **dangerous situation**
  • Only protected in the current network context
  • But, believing to be protected for future network contexts

- Must remember to replicate the change, if a similar change is wanted for future networks
Proposed Alternative Interface: Reveals the Hidden Context
Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

How does a firewall help protect my computer?

- **Public Network**
  - Windows Firewall is on for both inbound and outbound connections.
  - Inbound connections that don't match exceptions are dropped.
- **Private Network**
  - Windows Firewall is on for both inbound and outbound connections.
  - Inbound connections that don't match exceptions are dropped.
- **Domain Network**
  - Windows Firewall is on for both inbound and outbound connections.
  - Inbound connections that don't match exceptions are dropped.
- **Local Area Connection**
  - Windows Firewall is on for both inbound and outbound connections.
  - Inbound connections that don't match exceptions are dropped.
- **Bluetooth Network Connection**
  - Windows Firewall is on for both inbound and outbound connections.
  - Inbound connections that don’t match exceptions are dropped.

**Turn Windows Firewall On for All Network Locations and Connections** *(recommended)*

This setting blocks outside sources from connecting to this computer, except for those unblocked on the Exceptions tab above.

**Turn Windows Firewall Off for All Network Locations and Connections** *(not recommended)*

Avoid using this setting. Turning off Windows Firewall will make this computer more vulnerable to hackers or malicious software.

Tell me more about these settings

[OK]  [Cancel]
User Study
Goal

To investigate the impact of addition of contextual information to Vista Firewall basic interface on:

- Users’ mental model of Vista Firewall functionality
- Users’ understanding of Vista Firewall configuration
Study Design

- Within-subjects lab study
- Screen and voice recorded

Recruitment:
- Online classifieds: Craigslist, Kijiji
- University email lists
- Flyers: posted and handed out
  - University
  - Vancouver public places

Participants:
- 13 pilot testers
- 60 actual study
  - 30 first Vista firewall basic interface, then our interface
  - 30 first our interface, then Vista firewall basic interface
- 10 training at the beginning
Gender Balance

30 30
All Daily Computer Users

- Vista
- Windows 2000
- Linux
- Mac OS
- Windows XP
As you know we can use different network connections to connect to the Internet, like wireless or a cable. For this experiment, I set the laptop to use a wireless connection. I also can set my network for different network locations, for example public network like a coffee shop, or private network like at home. First, let's set the location to public. Could you do that?

<table>
<thead>
<tr>
<th>Network Connection</th>
<th>Public Network Location</th>
<th>Private Network Location</th>
<th>Domain Network Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless Network Connection</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local Area Connection</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bluetooth Network Connection</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Results
Mental Models

- Incorrect
- Incomplete
- Partially complete
- Complete
Mental Models

- **Incorrect:** Incorrect basic understanding of firewall operation
Mental Models

- Incorrect

- Incomplete: correct basic understanding of firewall operation, without context of network location and connection
Mental Models

- Incorrect
  - Incomplete

- Partially complete: correct basic understanding of firewall operation, with either context of network location or
Mental Models

- Incorrect
  - Incomplete
  - Partially complete

- Complete: correct basic understanding of firewall operation, context, and connections.
First Vista Firewall Basic, then Alternative

Complete

Partially complete

Incomplete

Incorrect

Initial

After VF

After Alt

Complete

Partially complete

Incomplete

Incorrect

25

25

28

11

16

2

3

1

2
First Alternative, then Vista Firewall Basic

Complete

Partially complete

Incomplete

Incorrect

Initial

After Alt

After VF
Understanding Firewall Configuration

<table>
<thead>
<tr>
<th></th>
<th>Public Network Location</th>
<th>Private Network Location</th>
<th>Domain Network Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless Network Connection</td>
<td>On ✗</td>
<td>On ✗</td>
<td>Unsure</td>
</tr>
<tr>
<td>Local Area Connection</td>
<td>On ✗</td>
<td>Off</td>
<td>Unsure</td>
</tr>
<tr>
<td>Bluetooth Network Connection</td>
<td>On ✓</td>
<td>Unsure</td>
<td>Unsure</td>
</tr>
</tbody>
</table>
Understanding Firewall Configuration

Public Network

<table>
<thead>
<tr>
<th>Before Checking Interface</th>
<th>After Checking Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>VF</td>
<td>Incorrect 68%</td>
</tr>
<tr>
<td>Alt</td>
<td>Correct 100%</td>
</tr>
<tr>
<td>Alt</td>
<td>Correct 97%</td>
</tr>
<tr>
<td>VF</td>
<td>Correct 48%</td>
</tr>
<tr>
<td>VF</td>
<td>Correct 64%</td>
</tr>
<tr>
<td>Alt</td>
<td>Correct 100%</td>
</tr>
<tr>
<td>Alt</td>
<td>Correct 100%</td>
</tr>
<tr>
<td>VF</td>
<td>Correct 37%</td>
</tr>
</tbody>
</table>

Vista-basic: large % of incorrect
Alternative interface: Understood config.
Incorrect Understanding of *Vista* Firewall Configuration

Incorrect off: Incorrectly believe that firewall is off, when it is on
Incorrect on: Incorrectly believe that firewall is on, when it is off
Feedback on Vista Firewall Basic Interface

“For some reason it is not on, the first thing that I am looking at is this red. This states to me is not right. It says it is on. If it is on, this should not be highlighted in red. This should be highlighted in green saying that it is on.”

Personal trainer-Laptop user with medium level of security experience
Feedback on Alternative Interface

- 56 (93%) participants liked images, fine-grained control
  “The second interface is much better. The pictures are very instructive. I have more control on it and that is nice.”
  Librarian—Both laptop and desktop user

- Some confusion about firewall state diagram
  “The arrow rebounding off the firewall should only be portrayed as such if all the incoming connections are blocked. Otherwise, the arrow should be shown going through the firewall, but narrower on the other side to represent the exceptions.”
  Grad Student in Electrical Eng.—Both laptop and desktop user
Multiple Firewall Profiles

- 39 (65%) participants preferred to have only one profile
  - Easier to use as they would not have to worry about context
  - Would avoid confusion
  - The multiple firewall profiles adds overhead without a perceived benefit

  “I would like the computer to be protected in any possible type of connection, regardless of where it is or how it is connected to the Internet.”

  Undergrad Student in Biology-Laptop user
Conclusions

- Design of Vista Firewall basic interface does not provide enough context for mobile users
  - If unaware that configuration changes only applied to current network location, may be left with dangerous misconceptions

- The users’ mental models can be supported by revealing the hidden context
  - Possible to balance complexity with security
Making security and privacy visible

- Users could better manage online privacy and security if cues were more visible
- Cues must be understandable
How do we know if a security or privacy cue is usable?

- Evaluate it
  - Why is it there?
  - Do users notice it?
  - Do they know what it means?
  - Do they know what they are supposed to do when they see it?
  - Will they actually do it?
  - Will they keep doing it?
Example: Privacy Bird

Problem: Web site privacy policies – many are posted, few are read

Approach:
- Determine whether the policy matches the user’s privacy preferences
- Notify the user
Privacy Bird Icons

Privacy policy *matches* user’s privacy preferences

Privacy policy *does not match* user’s privacy preferences
Help Users Make Decisions

- Developers should not expect users to make decisions they themselves can’t make
- Present choices, not dilemmas
Example: Certificate warnings
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

The security certificate has expired or is not yet valid.

The name on the security certificate is invalid or does not match the name of the site.

Do you want to proceed?

Yes  No  View Certificate
Users Don’t Check Certificates
The site's security certificate is not trusted!

You attempted to reach lersse.ece.ubc.ca, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Google Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications. You should not proceed, especially if you have never seen this warning before for this site.

Proceed anyway  Back to safety

Help me understand
The identity of this website has not been verified.

Your connection to lersse.ece.ubc.ca is not encrypted.

You first visited this site on Sep 4, 2008.
Reminder:
• Why is it there?
• Do users notice it?
• Do they know what it means?
• Do they know what they are supposed to do when they see it?
• Will they actually do it?
• Will they keep doing it?

Evaluate the usability of the warning and security cues.

The site’s security certificate is not trusted!
You attempted to reach lersse.ece.ubc.ca, but the server presented a certificate issued by an entity that is not trusted by your computer’s operating system. This may mean that the server has generated its own security credentials, which Google Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications. You should not proceed, especially if you have never seen this warning before for this site.

Proceed anyway  Back to safety

Help me understand

Security information

Identity
The identity of this website has not been verified.

Connection
Your connection to lersse.ece.ubc.ca is not encrypted.

Visit history
You first visited this site on Sep 4, 2008.
Making concepts understandable

Privacy Alert

The Web site "doubleclick.net" has requested to save a file on your computer called a "cookie." This file may be used to track usage information. Do you want to allow this?

- Apply my decision to all cookies from this Web site

- Allow Cookie
- Block Cookie
- More Info
- Help
• Internet Explorer 6.0 prompts the user to accept a cookie.
• This prompt doesn’t tell users much about what a cookie is or how it is relevant to them.
• It focuses on the act of setting a cookie, not on the replay, which is much more critical.
Cranor’s Human in the Loop Security Framework

Communication

Communication Impediments
- Environmental Stimuli
- Interference

Personal Variables
- Demographics and Personal Characteristics
- Knowledge and Experience

Intentions
- Attitudes and Beliefs
- Motivation

Capabilities

Communication Delivery
- Attention Switch
- Attention Maintenance

Communication Processing
- Comprehension
- Knowledge Acquisition

Application
- Knowledge Retention
- Knowledge Transfer

Human Receiver

Behavior
Phishing
What is phishing?

Phishing attacks use both **social engineering** and **technical subterfuge** to steal consumers' personal identity data and financial account credentials

(http://www.antiphishing.org)

Phishing targets the end user
I HAVE A NEW HOBBY. IT’S CALLED PHISHING.

I SEND FAKE BANKING E-MAILS TO GULLIBLE EXECUTIVES. THEN I FIND OUT THEIR FINANCIAL INFORMATION AND USE IT TO STEAL THE MONEY THEY DON’T DESERVE.

Dear Customer,
This is your bank. We forgot your social security number and password. Why don’t you send them to us so we can protect your money.

Sincerely,
I. B. Banker

© Scott Adams, Inc./Dist. by UFS, Inc.
Dear US Bank Customer,

Recently there have been a large number of identity theft attempts targeting US Bank Customers. In order to safeguard your account, we require that you confirm your banking details.

This process is mandatory, and if not completed within the nearest time your account or credit card may be subject to temporary suspension.

To securely confirm your US Bank Account details please follow the link:

https://www.usbank.com/internetBanking/RequestRouter?requestCmdId=upt

Note: You may have to report this message as "Not Junk Mail" if update link does not work.

Thank you for your prompt attention to this matter and thank you for using US Bank.

© 2004 U.S. Bancorp
The next page requests:

- Name
- Address
- Telephone
- Credit Card Number, Expiration Date, Security Code
- PIN
- Account Number
- Personal ID
- Password
Your account information will be verified by US Bank Department in the next 24 hours. Thank you for your cooperation.
But wait…

WHOIS 210.104.211.21:
Location: Korea, Republic Of

Even bigger problem:
I don’t have an account with US Bank!

Images from Anti-Phishing Working Group’s Phishing Archive; Slide from “Pholproff Phishing Prevention” by B. Parno, C. Kuo, A. Perrig
Phishing Techniques

- The cuckoo's egg: mimic a known institution (relies on graphical similarity)

- Or narrow your focus:
  - Socially-aware mining:
    - E-mail is from a “known” individual
  - Context-aware attacks
    - Your bid on e-bay has won…
Why is Phishing Successful?

- Some users trust too readily
- Users cannot parse URLs, domain names or PKI certificates
- Users are inundated with requests, warnings and pop-ups
Usable security approaches

- Educate Users
- Good user interface design (usability guidelines)
- Help users make good decisions rather than presenting dilemmas
Phishing Education

- Anti-Fishing Phil
- http://cups.cs.cmu.edu/antiphishing_phil/
Other Solutions: Toolbars

- Trustbar
- spoofguard
- Accountguard
1) If you are on a verified eBay or PayPal web site.

2) If you are on a non eBay or PayPal web site.
3) If you are on a potential spoof site, the icon turns red.

Will warn you when you are about to enter your eBay password into a non-eBay site.
Account Guard Usability

Will users:

- Be reliably made aware of the security tasks they must perform?
- Be able to figure out how to successfully perform those tasks?
- Not make dangerous errors?
- Be sufficiently comfortable with the interface to continue using it?
- Be able to tell when their task has been completed?
- Have sufficient feedback to accurately determine the current state of the system?
Cranor’s Human in the Loop Security Framework
Participants purchased items from 2 web stores with their own credit cards.

Phishing emails asking them to log in to confirm their purchase were sent.

Participants “returned” to the site.

Control group + 3 phishing warning techniques.
Passive IE Phishing Warning
Active IE Phishing Warning

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.
Active Firefox Phishing Warning

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. **Read more »**

**Get me out of here! Ignore this warning**

*This isn't a web forgery*
How well do you think the phishing warnings work?
How well do the techniques work?

<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 (100%)</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>Active IE</td>
<td>20</td>
<td>19 (95%)</td>
<td>9 (45%)</td>
</tr>
<tr>
<td>Passive IE</td>
<td>10</td>
<td>10 (100%)</td>
<td>9 (90%)</td>
</tr>
<tr>
<td>Control</td>
<td>10</td>
<td>9 (90%)</td>
<td>9 (90%)</td>
</tr>
</tbody>
</table>

Table 1. An overview depicting the number of participants in each condition, the number who clicked at least one phishing URL, and the number who entered personal information on at least one phishing website. For instance, nine of the control group participants clicked at least one phishing URL. Of these, all nine participants entered personal information on at least one of the phishing websites.

<table>
<thead>
<tr>
<th>Condition Name</th>
<th>Sample</th>
<th>Saw Warning</th>
<th>Read Warning</th>
<th>Recognized Warning</th>
<th>Understood Meaning</th>
<th>Understood Choices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firefox</td>
<td>20</td>
<td>20</td>
<td>13</td>
<td>4</td>
<td>17</td>
<td>19</td>
</tr>
<tr>
<td>Active IE</td>
<td>20</td>
<td>19</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>12</td>
</tr>
<tr>
<td>Passive IE</td>
<td>10</td>
<td>8</td>
<td>3</td>
<td>5</td>
<td>3</td>
<td>5</td>
</tr>
</tbody>
</table>

Table 2. This table depicts the number of participants in each experimental condition, the number who saw at least one warning, the number who completely read at least one warning, the number who recognized the warnings, the number who correctly understood the warnings, and the number who understood the choices that the warnings presented.
Cranor’s Human in the Loop Security Framework
This Talk’s Goals

- Provide awareness of usable security
- Discuss the challenges of designing for security AND usability
- Give you a little practical experience of looking at systems from a usability perspective