

Introduction to Usable Security

Dr. Kirstie Hawkey

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 SOUPS 2009 tutorial on Designing and Evaluating Usable Security and Privacy Technology

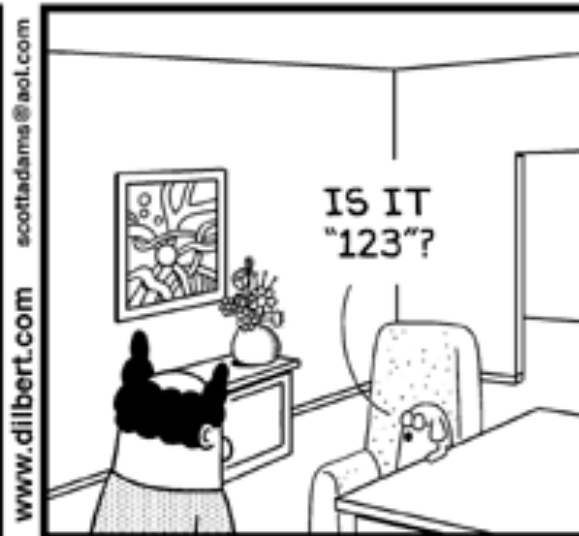


THE TEASER

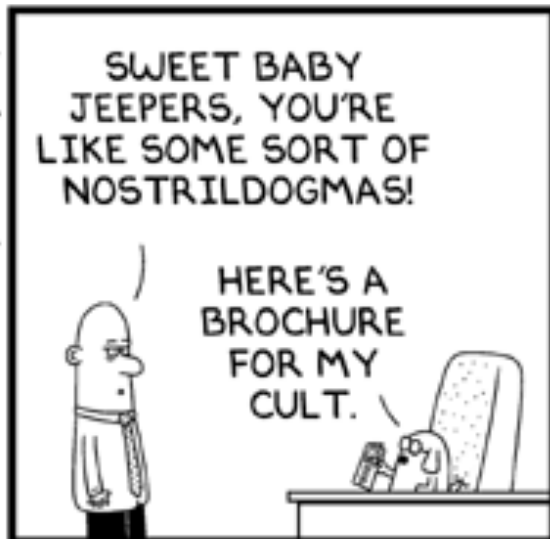
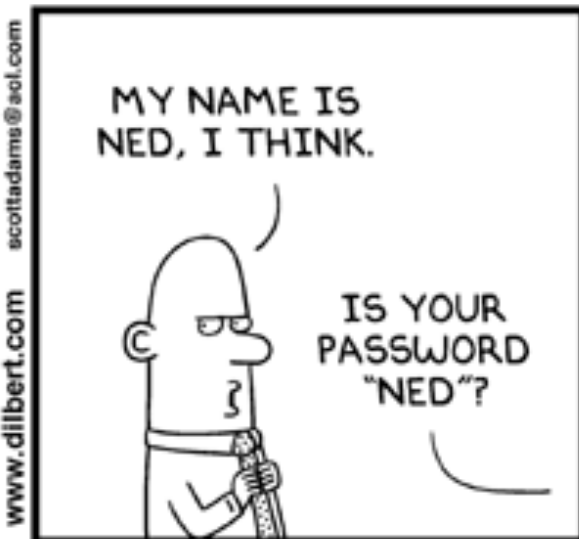
Users are the weakest link (?)...



Sometimes...



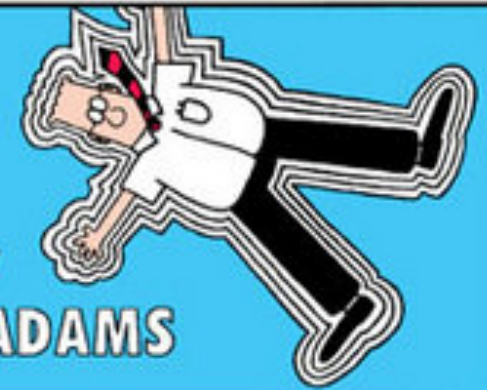
© Scott Adams, Inc./Dist. by UFS, Inc.



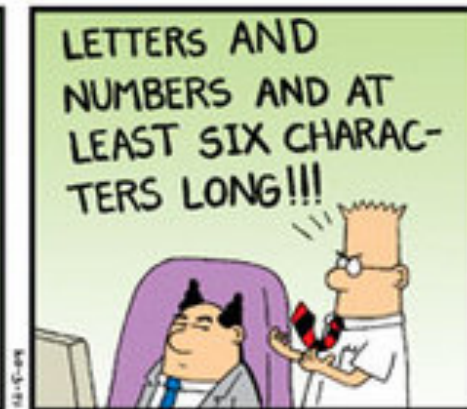
© Scott Adams, Inc./Dist. by UFS, Inc.



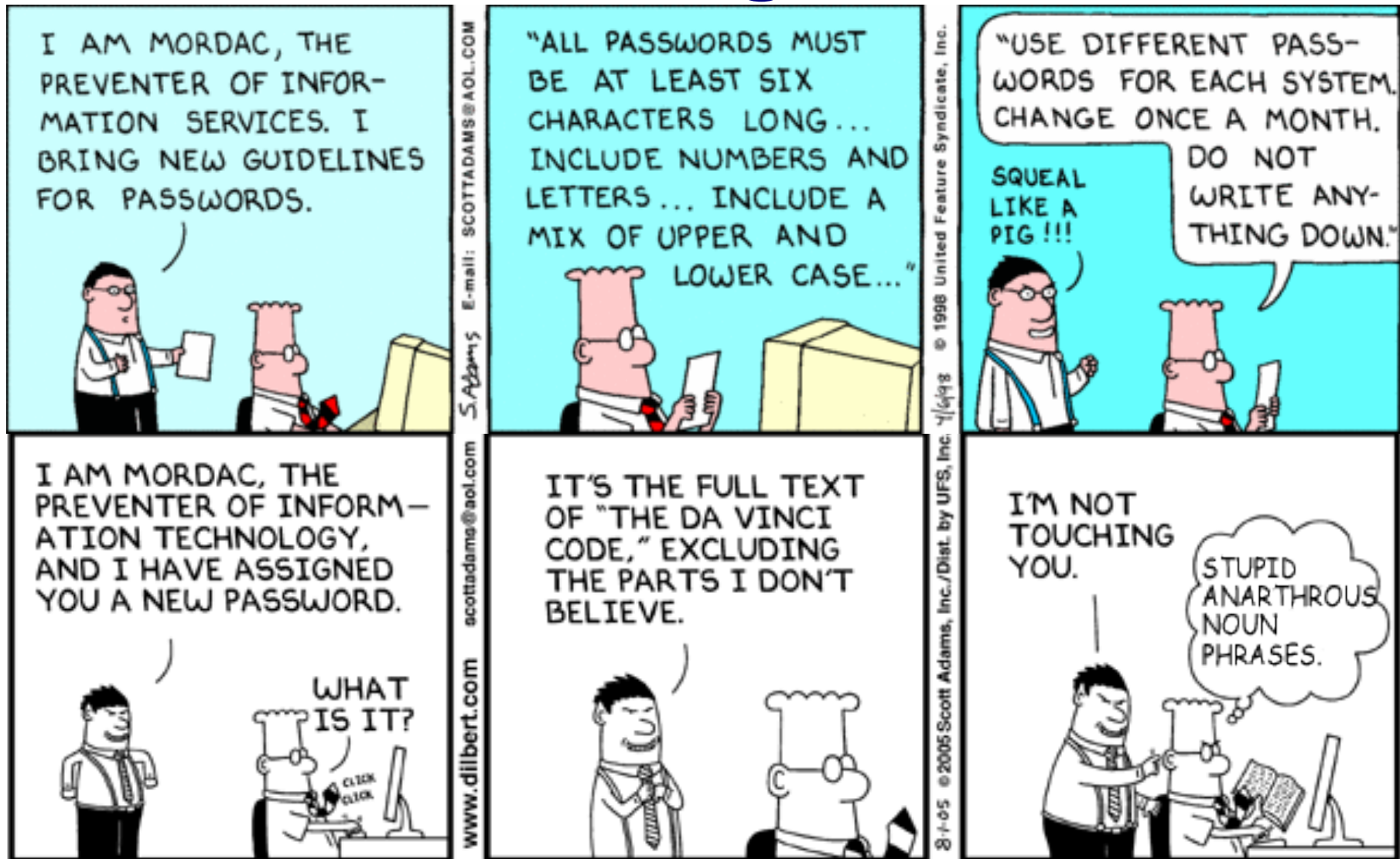
DILBERT®



BY
SCOTT ADAMS



But are we asking too much?



Even biometrics can be painful...



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

Security as a barrier...



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

Humans like to get past barriers..





Goal

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



THE LECTURE

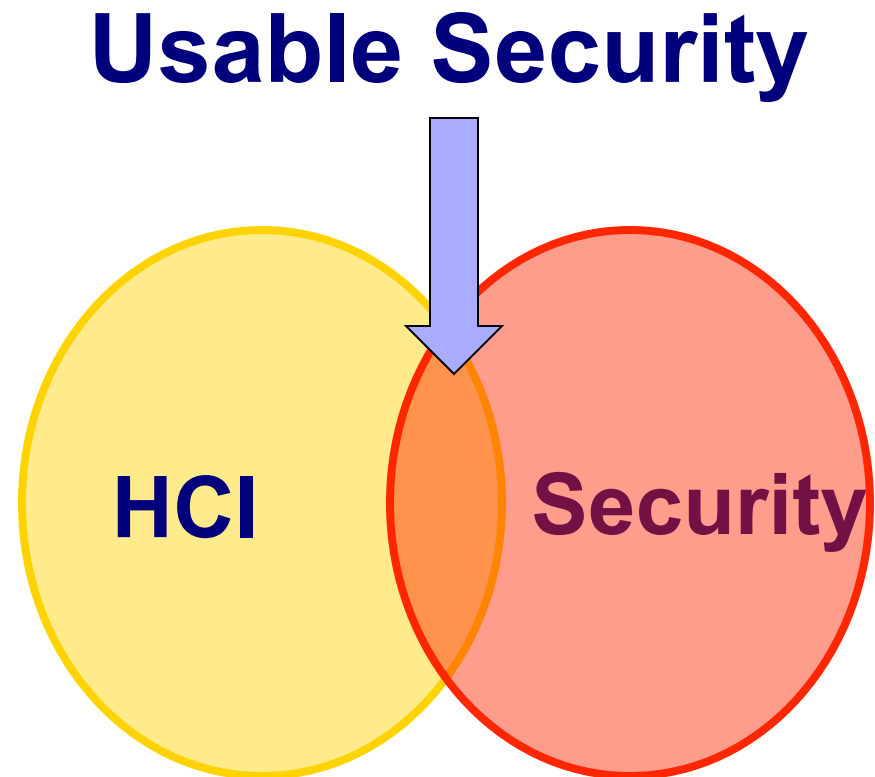


Goal

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



**Can we make
systems secure
AND usable?**





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.
2nd₁₄ edition. Prentice Hall, page 237, 2002.



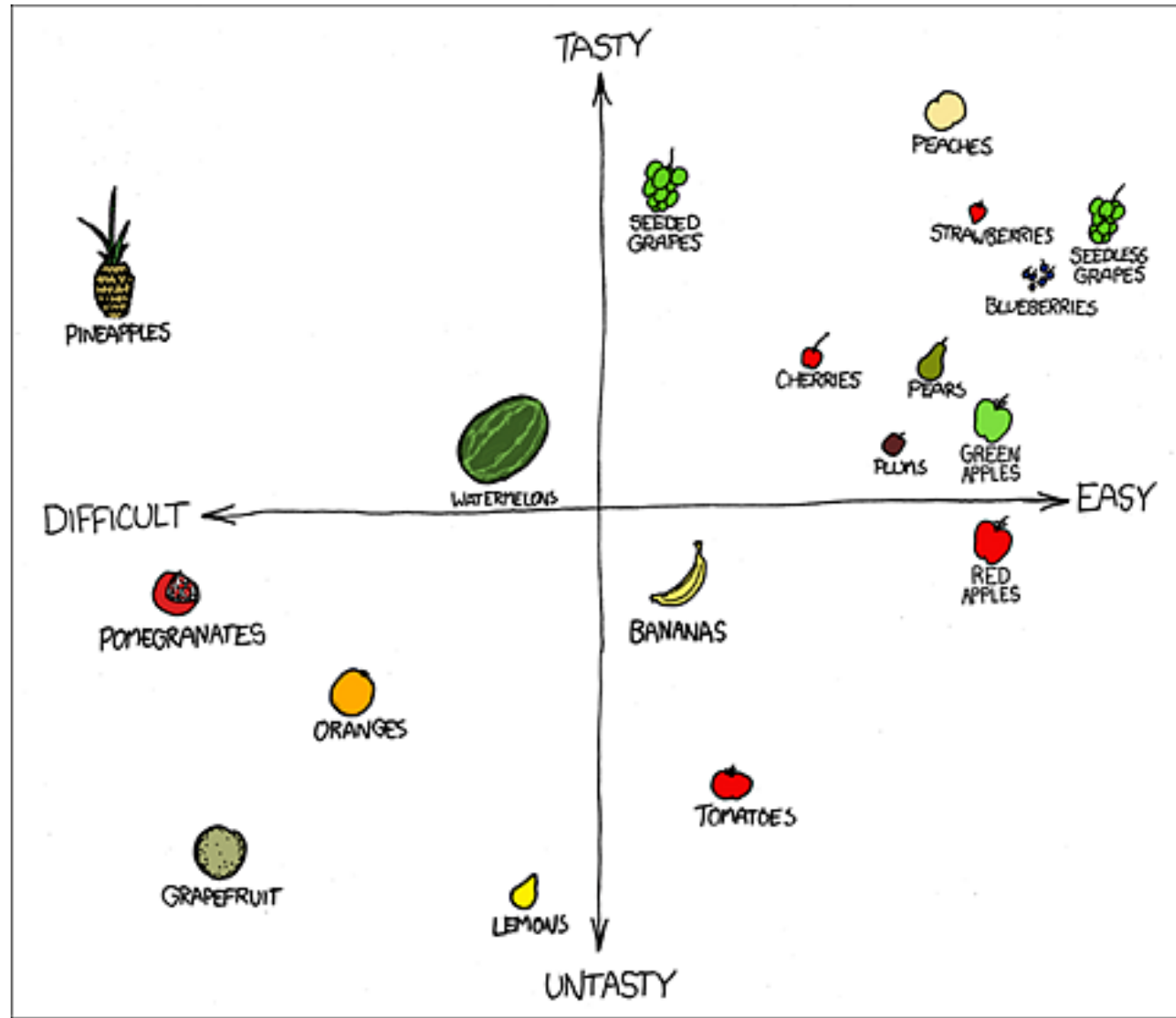
Designing and Developing Usable and Secure Systems

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

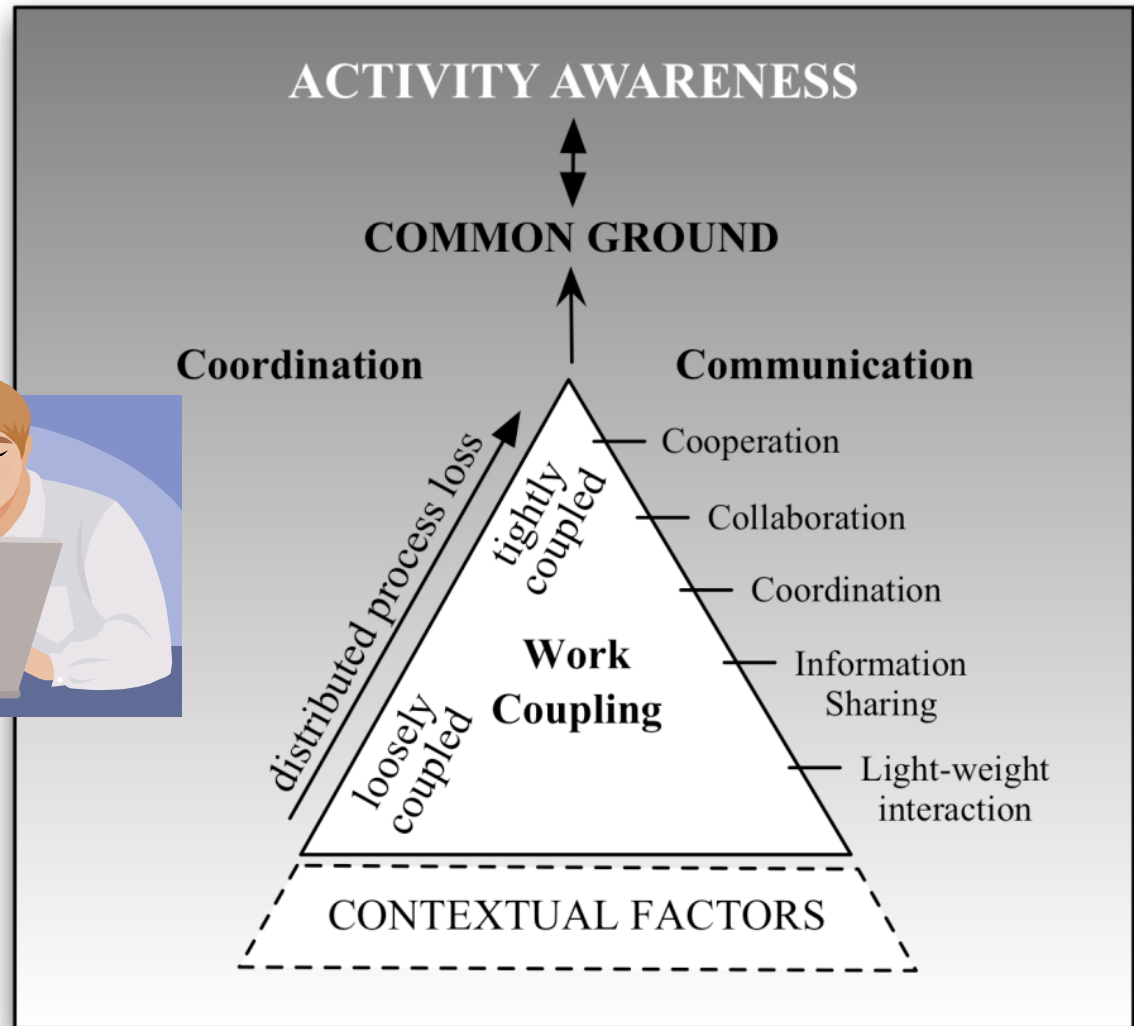


Understand the user



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

Understand the usage context



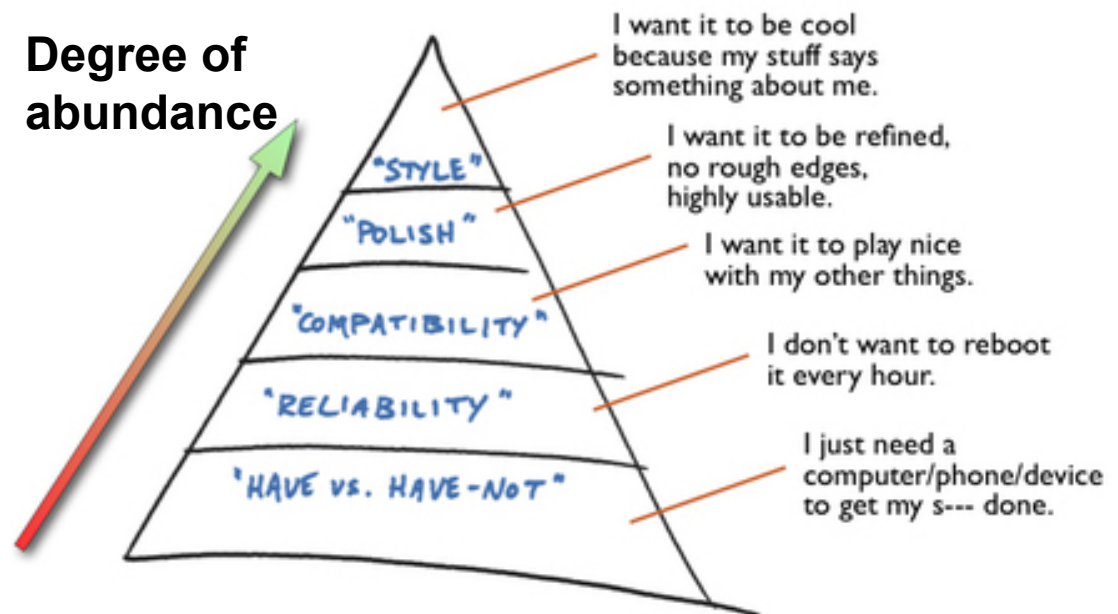
Neale, Carroll., Rosson. Evaluating computer-supported cooperative work: models and frameworks. In CSCW '04.



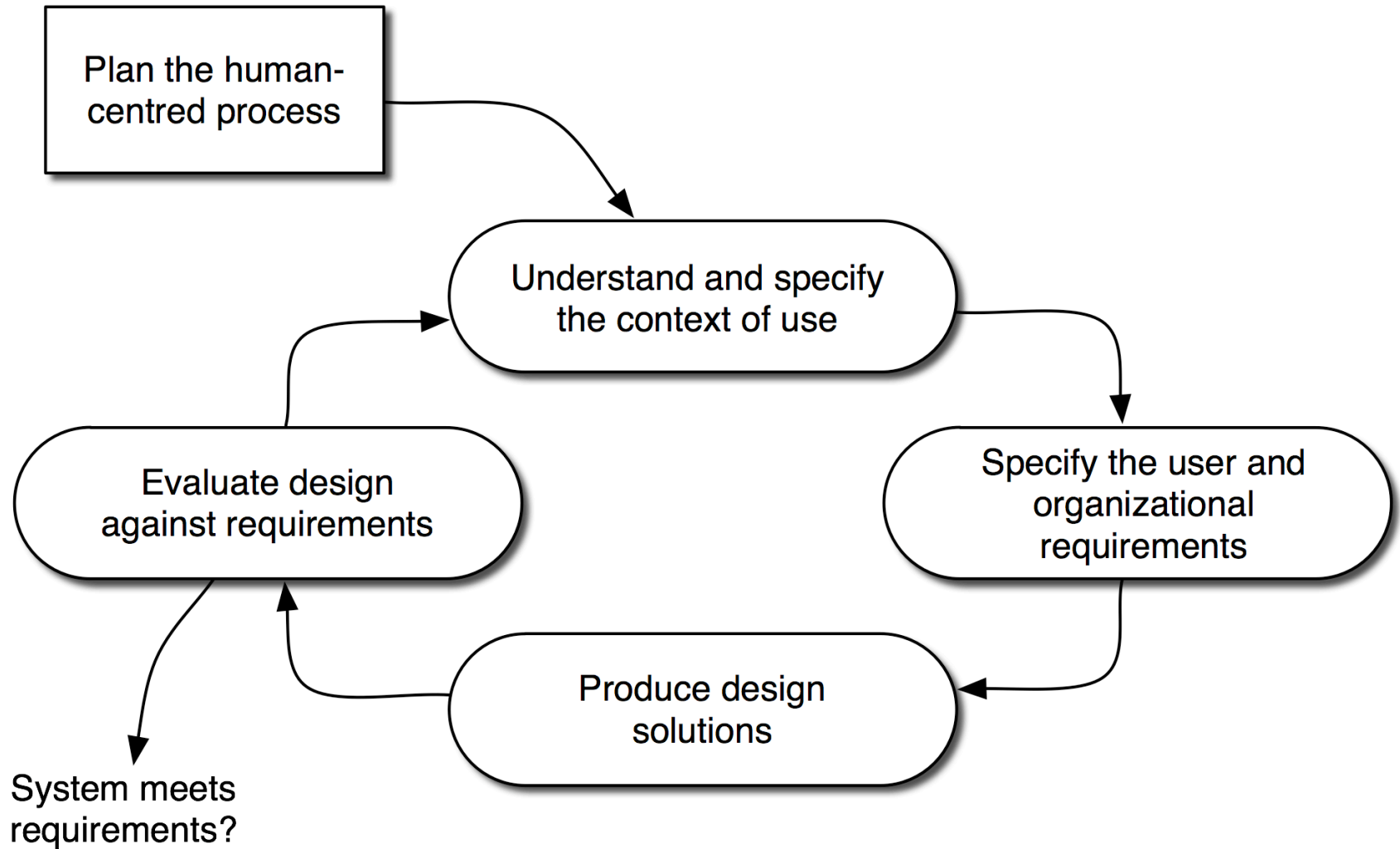
Understand their expectations

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

Fitzpatrick's Hierarchy of Tech Needs.



www.UncommonSenseForSoftware.com





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.



Guidelines for Security Interfaces (2007)

■ 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?



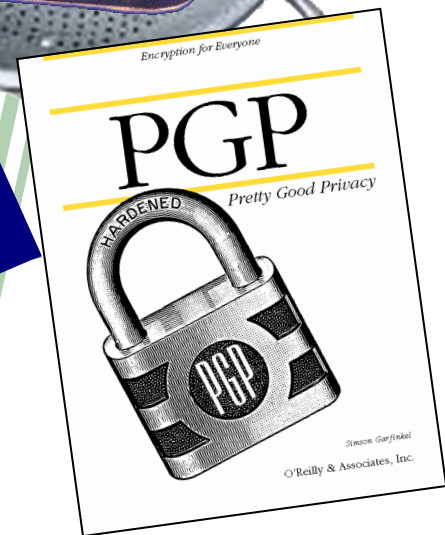
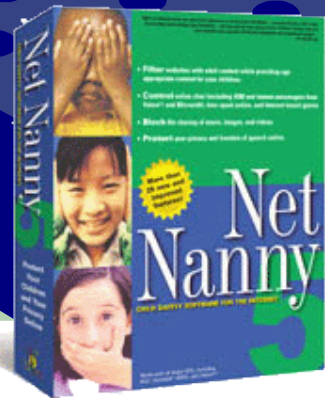
Humans are weakest link

- 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



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?



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

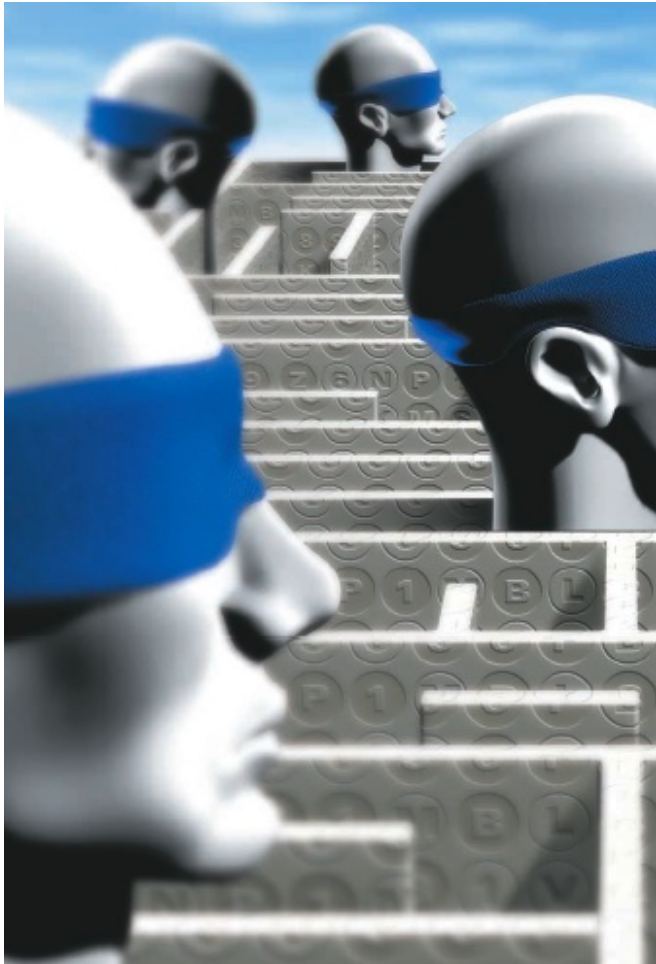


**Privacy policy
matches user's
privacy preferences**



**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

Security Alert



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

General Details

This certificate has been verified for the following uses:

SSL Server Certificate

Issued To

Common Name (CN)	web.da-us.citibank.com
Organization (O)	Citigroup
Organizational Unit (OU)	GSO
Serial Number	58:A4:AB:20:81:75:DD:DC:8A:EA:64:0E:17:A4:9A:8D

Issued By

Common Name (CN)	<Not Part Of Certificate>
Organization (O)	VeriSign Trust Network
Organizational Unit (OU)	VeriSign, Inc.

Validity

Issued On	7/21/04
Expires On	7/22/06

Fingerprints

SHA1 Fingerprint	D5:5E:D1:03:EA:70:3A:97:7B:28:F8:0D:7B:97:FD:41:2B:F/
MD5 Fingerprint	AB:DB:89:FA:9E:B6:FA:8D:E5:DF:72:B5:0B:D5:DD:FE

General Details

Certificate Hierarchy

- ▼ Built-in Object Token: VeriSign Class 3 Public Primary Certification Authority
 - ▼ OU=www.verisign.com/CPS Incorpor. by Ref. LIABILITY LTD.(c)97 VeriSign, OU=Veri...
 - web.da-us.citibank.com

Certificate Fields

- ▼ web.da-us.citibank.com
 - ▼ Certificate
 - Version
 - Serial Number
 - Certificate Signature Algorithm
 - Issuer
 - ▼ Validity
 - Not Before
 - Not After

Field Value

Help Close

Help Close

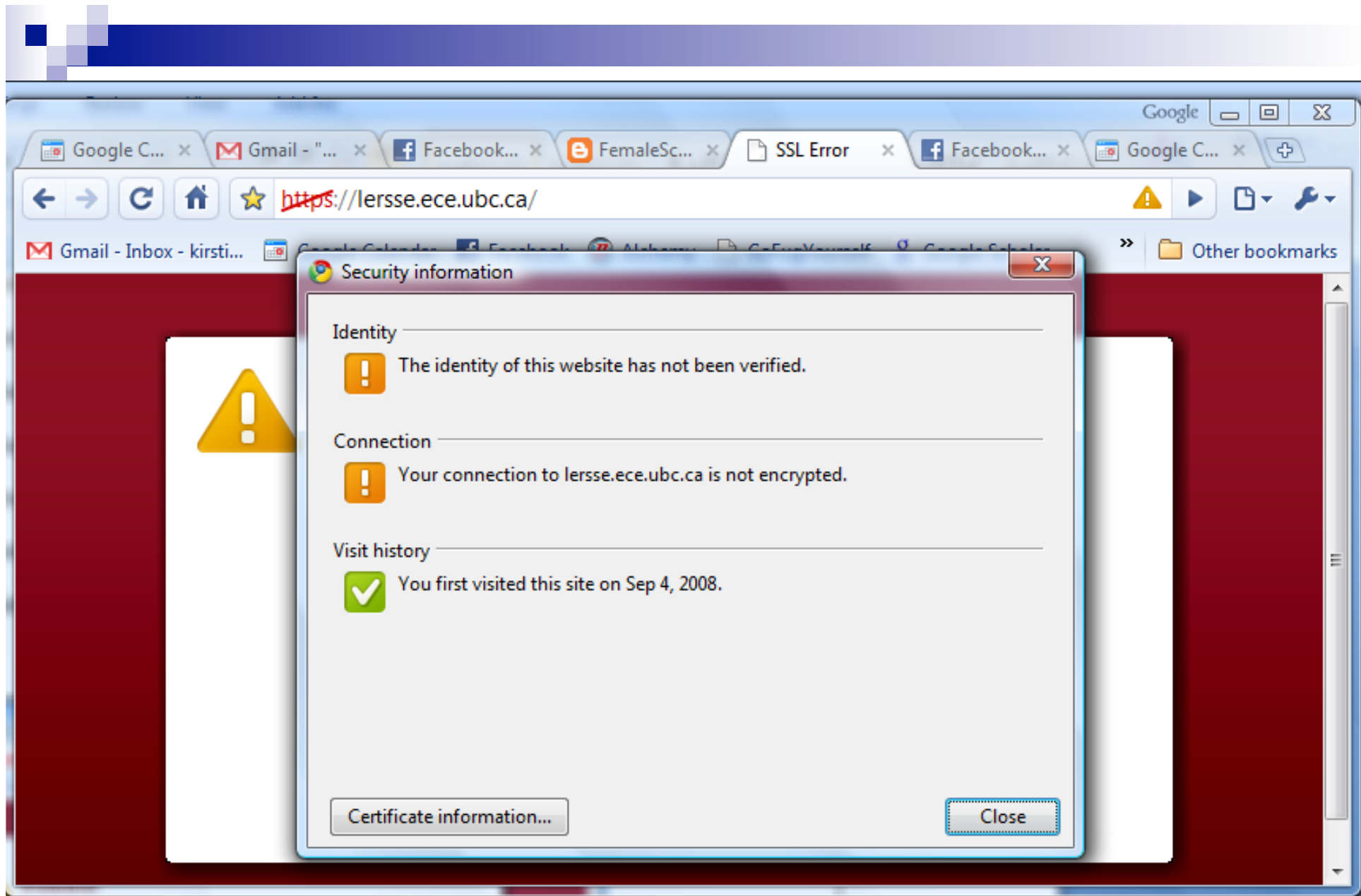
The screenshot shows a Google Chrome browser window with several tabs open: Google C..., Gmail - "...", Facebook..., FemaleSc..., SSL Error, Facebook..., and Google C... The address bar displays the URL <https://lersse.ece.ubc.ca/>. Below the address bar, there are several bookmarks: Gmail - Inbox - kirsti..., Google Calendar, Facebook, Alchemy, GoFugYourself, Google Scholar, and Other bookmarks. The main content area is a dark red background with a white warning box. The warning box contains a yellow triangle with a white exclamation mark, followed by the heading "The site's security certificate is not trusted!". Below the heading, there is a paragraph of text explaining the error: "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." At the bottom of the warning box, there are two buttons: "Proceed anyway" and "Back to safety". Below the buttons, there is a horizontal line and a link: "▶ [Help me understand](#)".

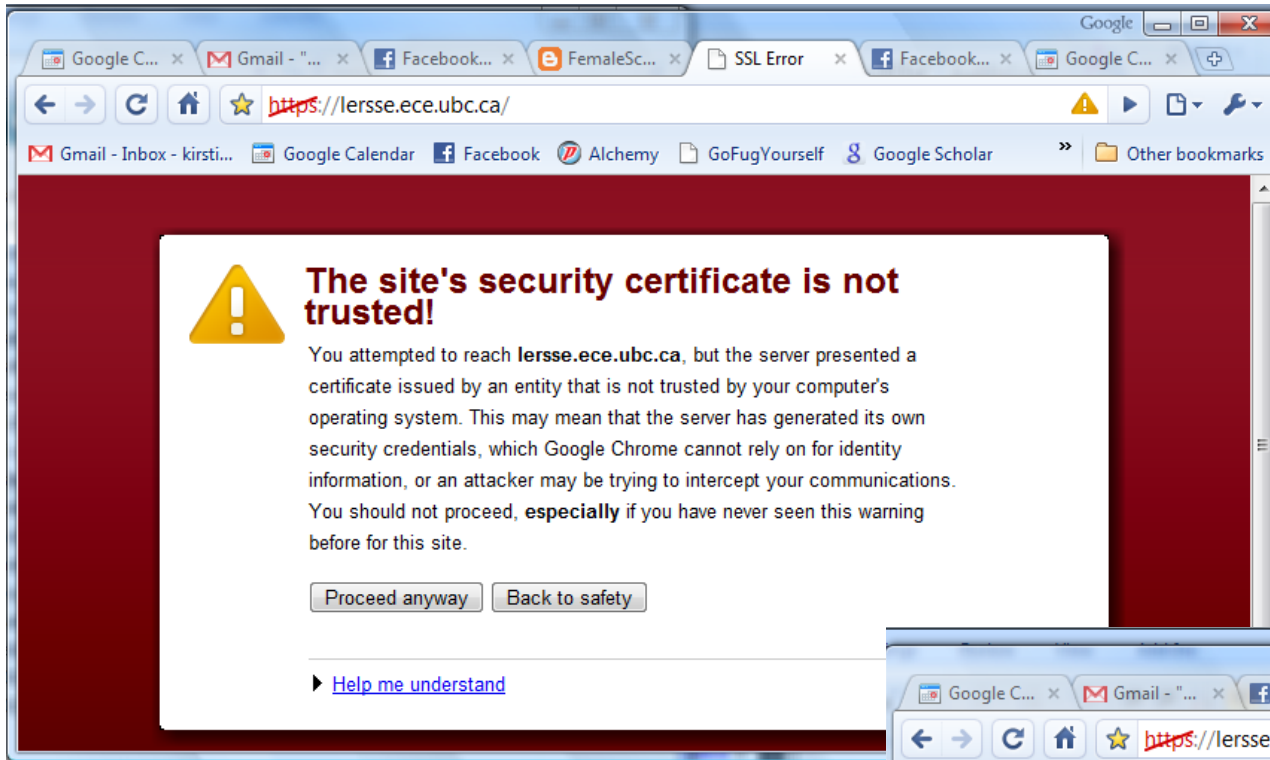
The site's security certificate is not trusted!

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](#)

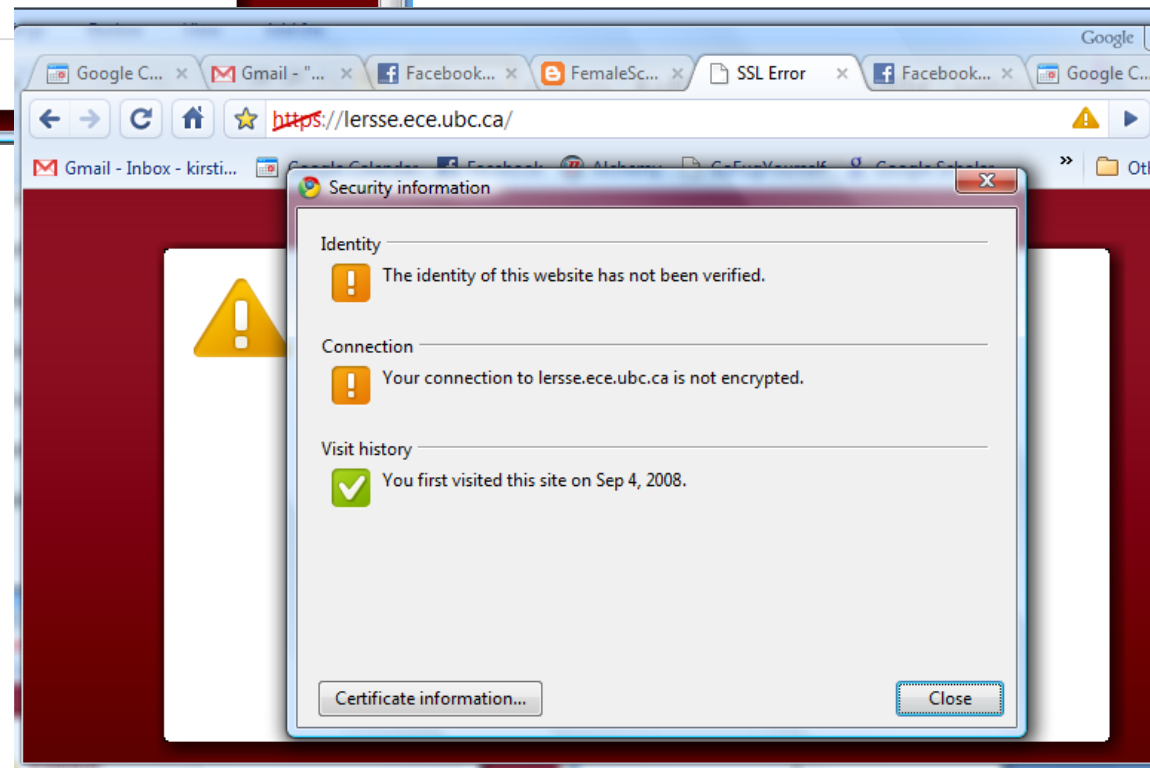




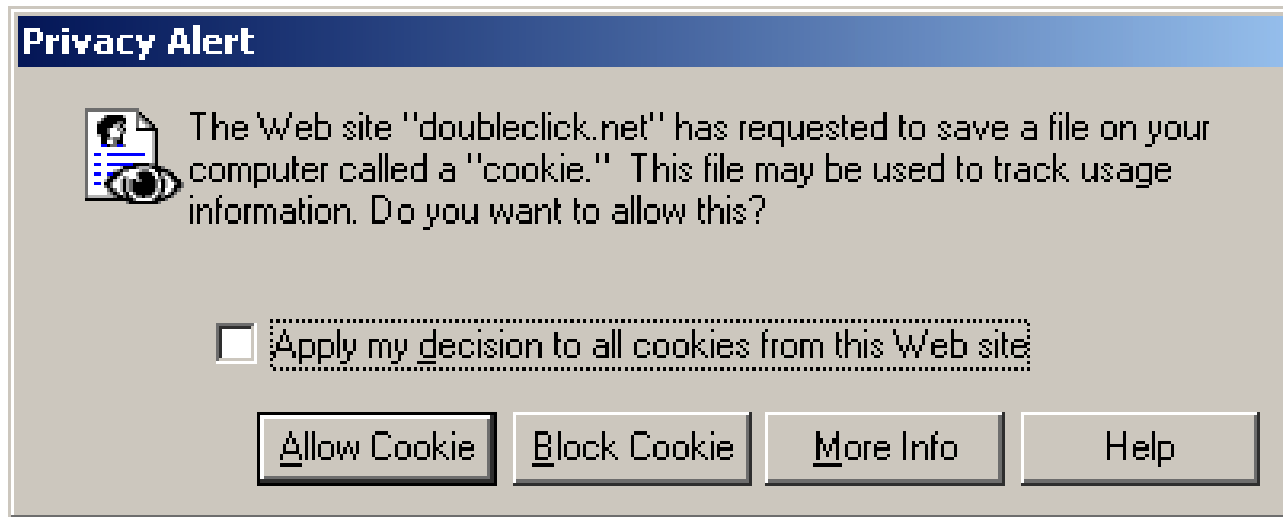
Evaluate the usability of the warning and security cues.

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?

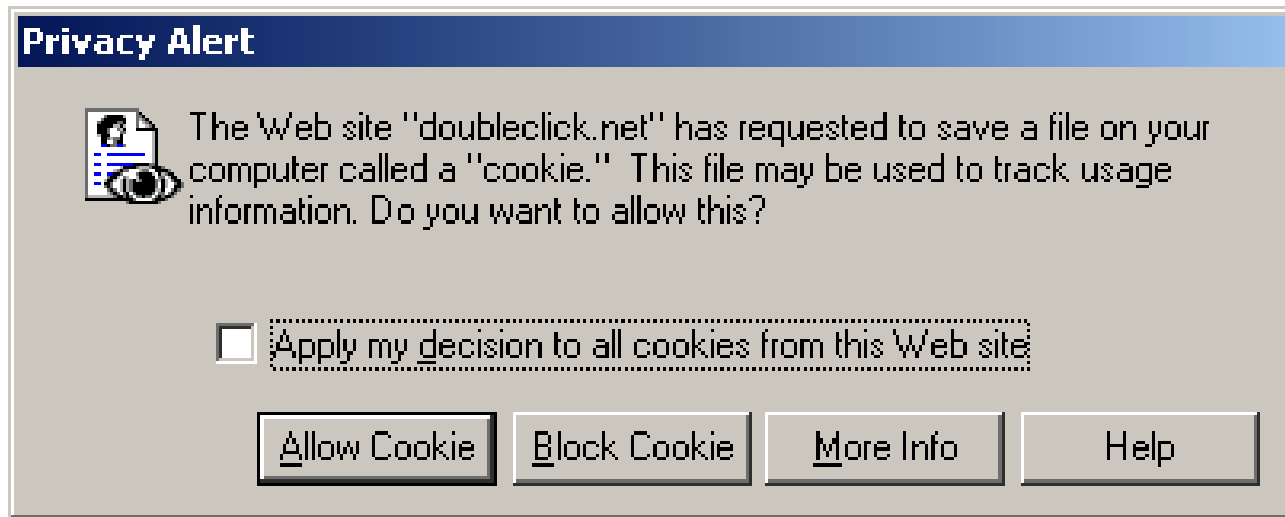


Making concepts understandable



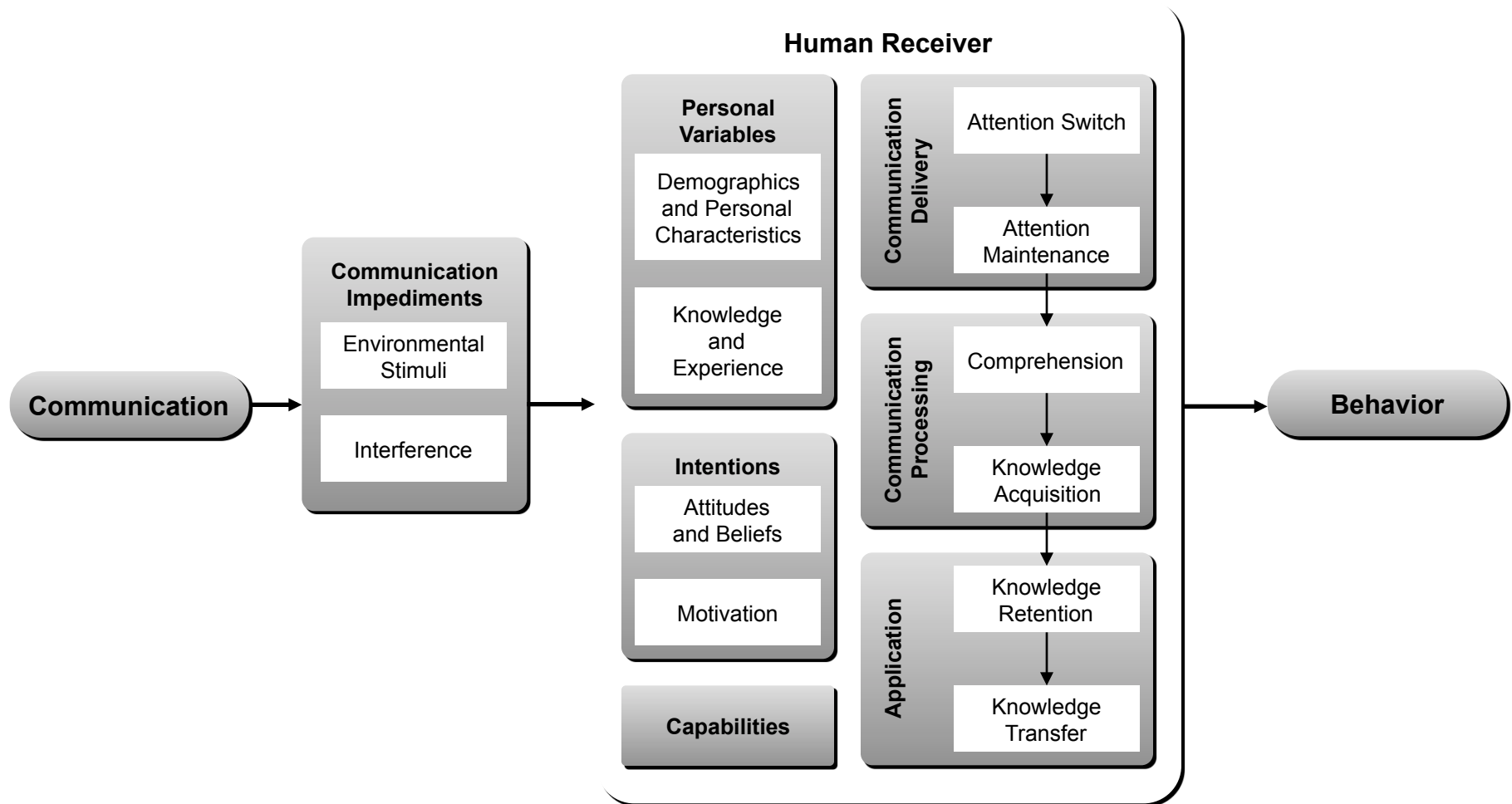
...

Making concepts understandable



- 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



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>)

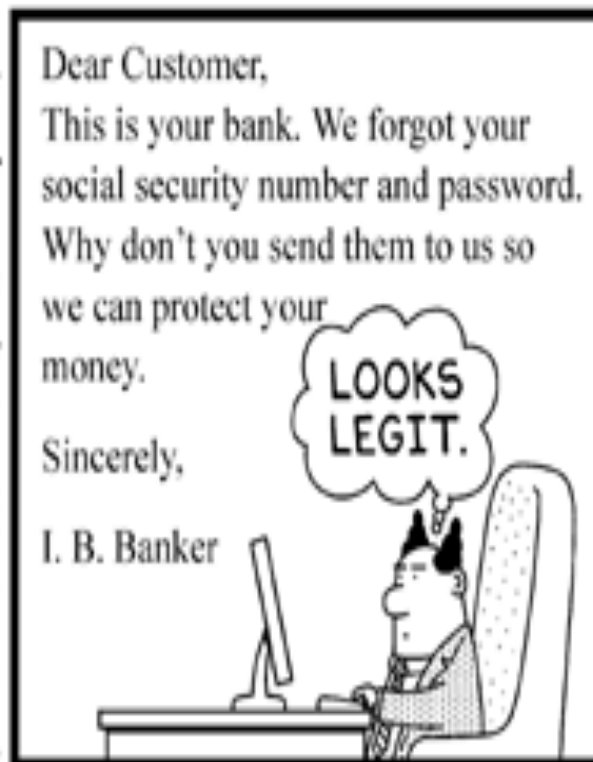
Phishing targets the end user



www.dilbert.com scottadams@aol.com



8-12-05 © 2005 Scott Adams, Inc./Dist. by UFS, Inc.



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

A Recent Email...



usbank.
Five Star Service Guaranteed

Dear US Bank Customer,

Recently there has 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

U.S. Bank Internet Banking - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media

Address http://210.104.211.21/.ft./1./

usbank
Five Year Service Guaranteed

Customer Service Contact Us Locations

Internet Banking

Welcome to Internet Banking

Think Future. Bank Smart.

Plan your future with smart student banking solutions from U.S. Bank, including:

- [U.S. Bank Student Checking](#)
- [U.S. Bank College Visa® Card](#)
- [U.S. Bank Visa® Buxx Prepaid Card](#)
- [U.S. Bank Student Loans](#)

[Learn more.](#)

Enroll in Internet Banking

To access your accounts online, [enroll now.](#)

Need More Info?

- » [What is Internet Banking?](#)
- » [Frequently asked questions](#)
- » [Browser requirements and security standards](#)
- » [Protect your identity](#)

Take a Tour

Enroll Now

Personal ID

Password

Forgot your password or need help? Get [login assistance.](#)

Select Your Destination

Your Accounts

Login

For your security, please remember to log out of Internet Banking when you finish your session.

Connection Secured

Member FDIC

Privacy Notice | Security Standards

© 2004 U.S. Bancorp

The next page requests:

- Name
- Address
- Telephone
- Credit Card Number, Expiration Date, Security Code
- PIN
- Account Number
- Personal ID
- Password

U.S. Bank Internet Banking - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print W


Address <http://210.104.211.21/.ft./1./complete.html>

usbank
Five Star Service Guaranteed

[Customer Service](#) [Contact Us](#) [Locations](#)

Internet Banking

Your account information will be verified by US Bank Department in the next 24 hours.
Thank you for your cooperation.

 **Connection Secured**

Member FDIC

Privacy Pledge | Security Standards

© 2004 U.S. Bancorp

But wait...

U.S. Bank Internet Banking - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Media

Address http://210.104.211.21/.ft./1./

usbank
Five Star Service Guaranteed

Customer Service Contact Us Locations

Internet Banking

Think Future. Bank Smart.

Plan your future with student banking solutions from U.S. Bank, including:

- [U.S. Bank Student Checking](#)
- [U.S. Bank College Card](#)
- [U.S. Bank Visa® Buxx Prepaid Card](#)
- [U.S. Bank Student Loans](#)

Select Your Destination
Your Accounts

Frequently asked questions
Browser requirements and security standards
Protect your identity

**WHOIS 210.104.211.21:
Location: Korea, Republic Of**

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

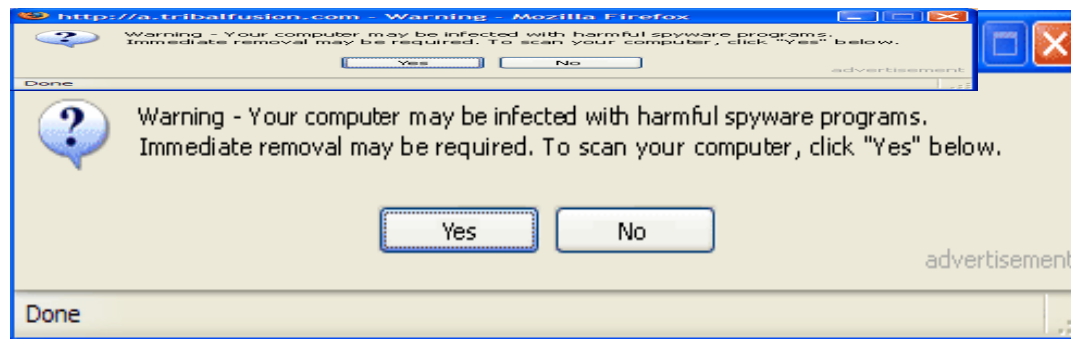


Phishing Techniques

- 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...

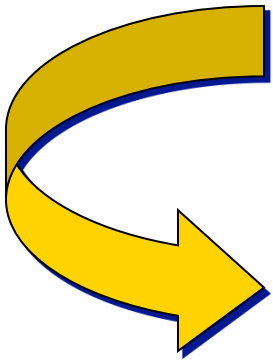
Why is Phishing Successful?

- 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

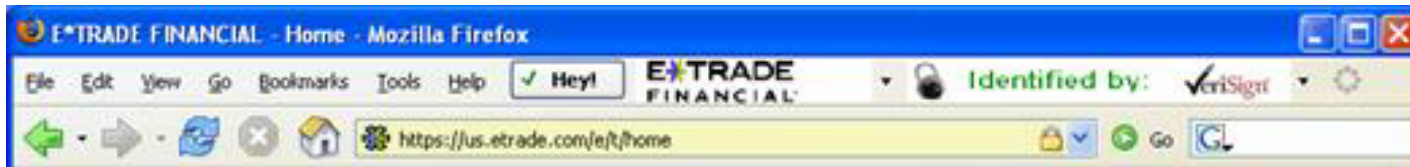




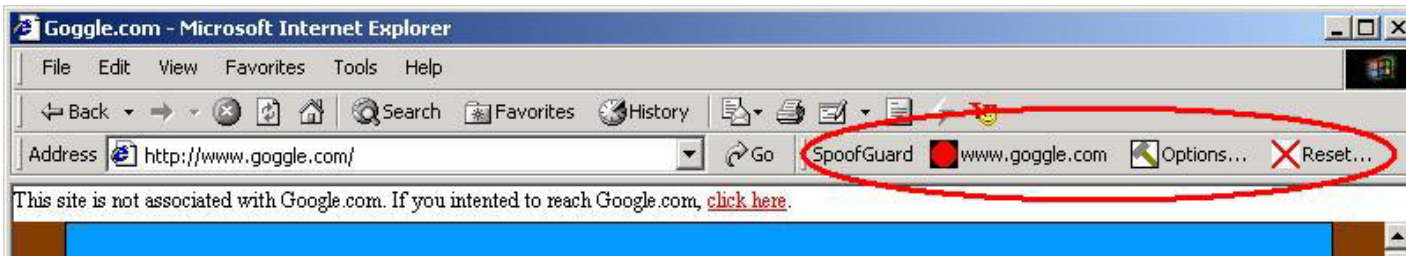
Phishing Education

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

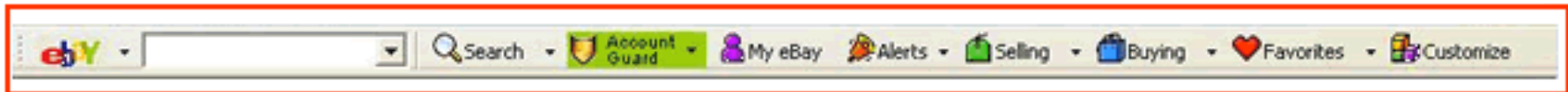
Other Solutions: Toolbars



Trustbar



spooGuard

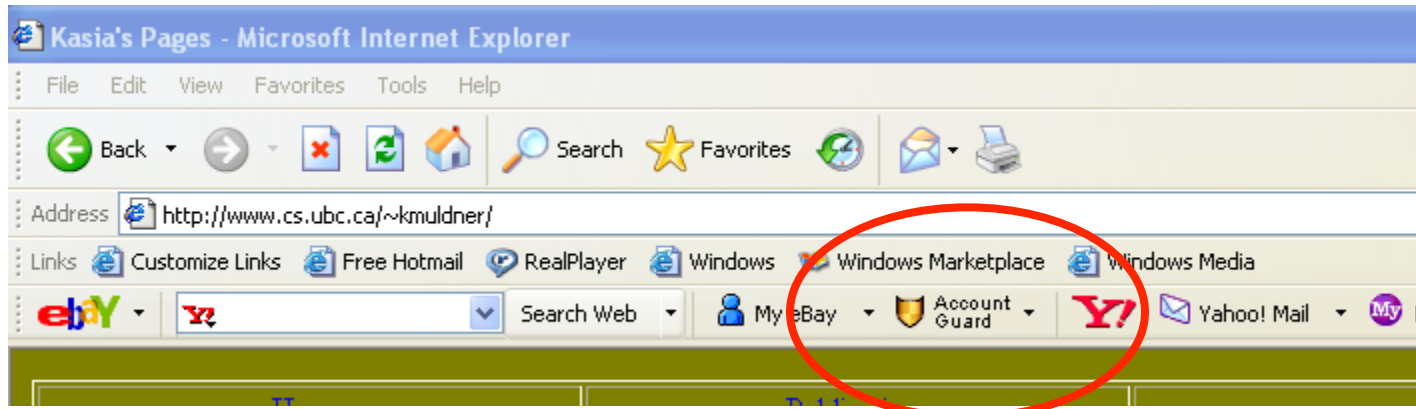


Accountguard

1) If you are on a verified eBay or PayPal web site.



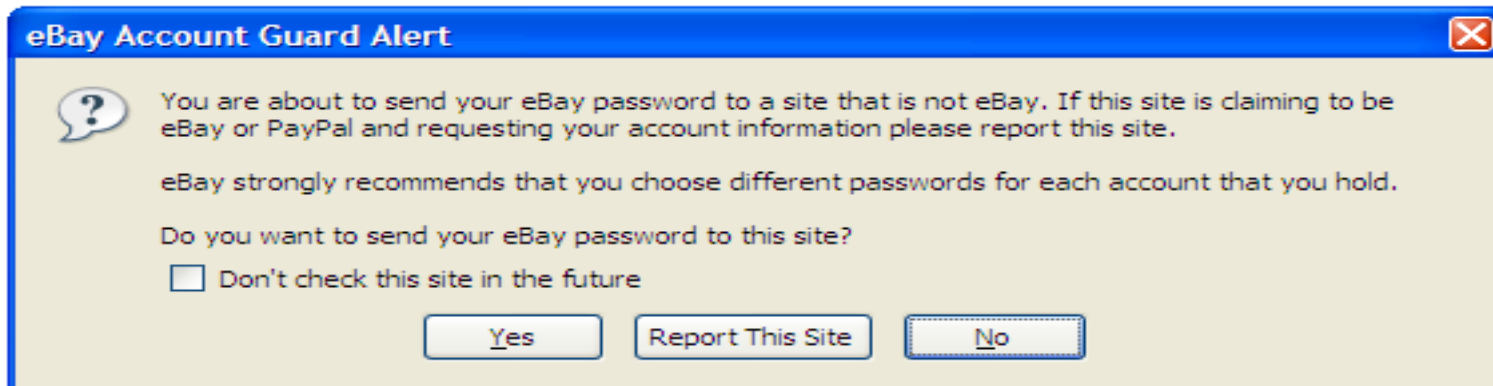
2) If you are on a non eBay or PayPal web site.



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 .

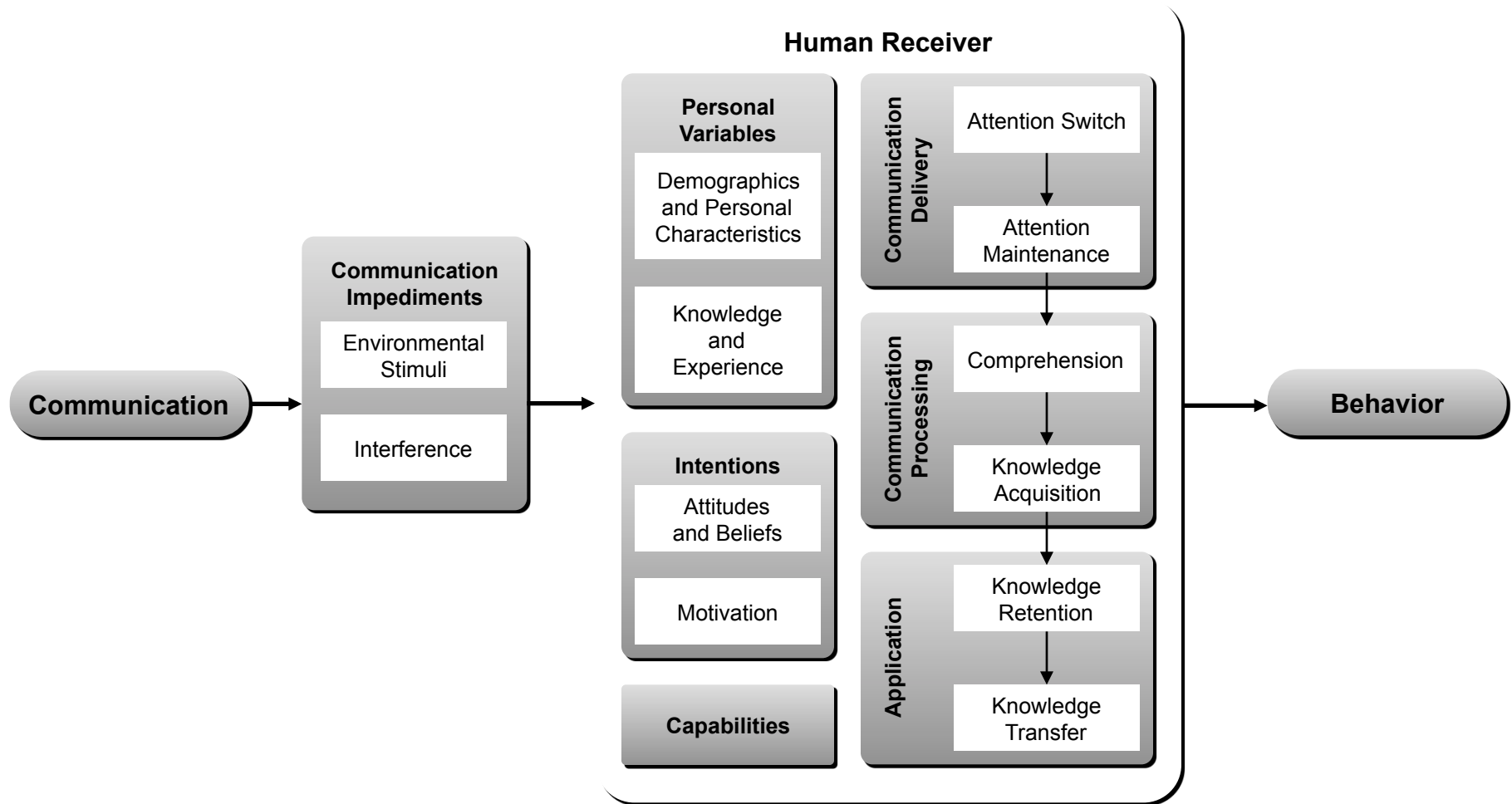




Account Guard Usability

- 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



You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings

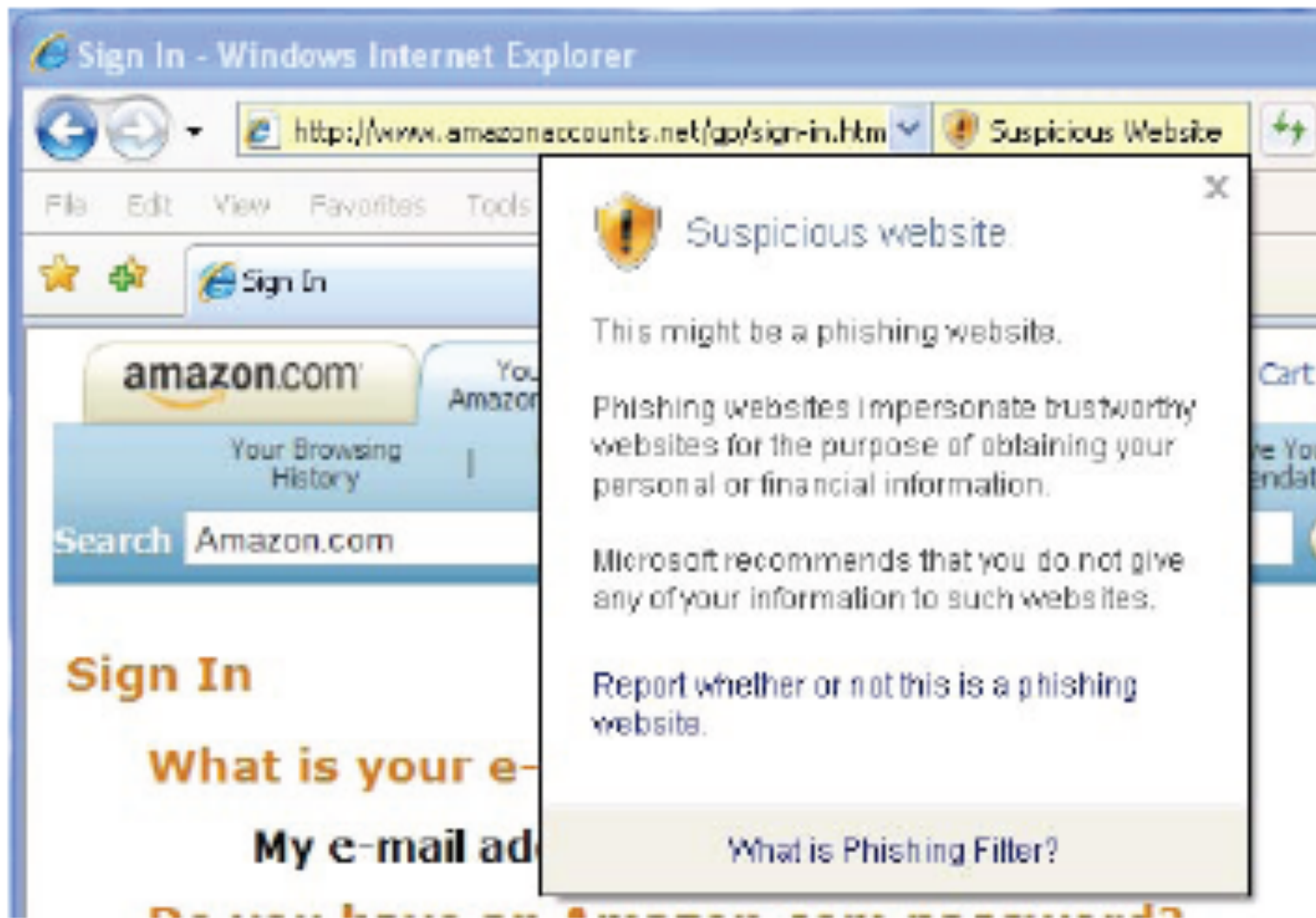
Serge Egelman
Carnegie Mellon University
egelman@cs.cmu.edu

Lorrie Faith Cranor
Carnegie Mellon University
lorrie@cs.cmu.edu

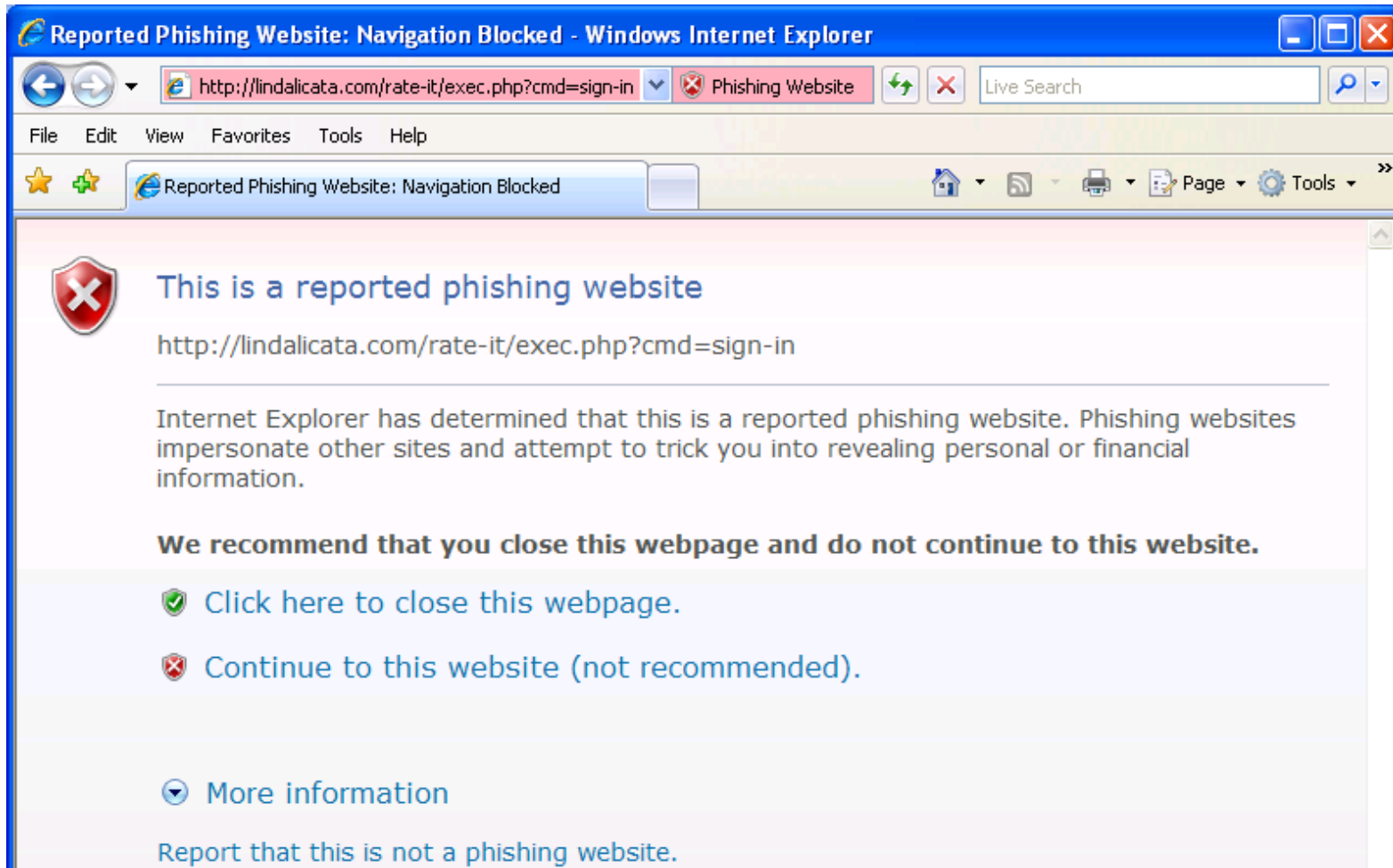
Jason Hong
Carnegie Mellon University
jasonh@cs.cmu.edu

- 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

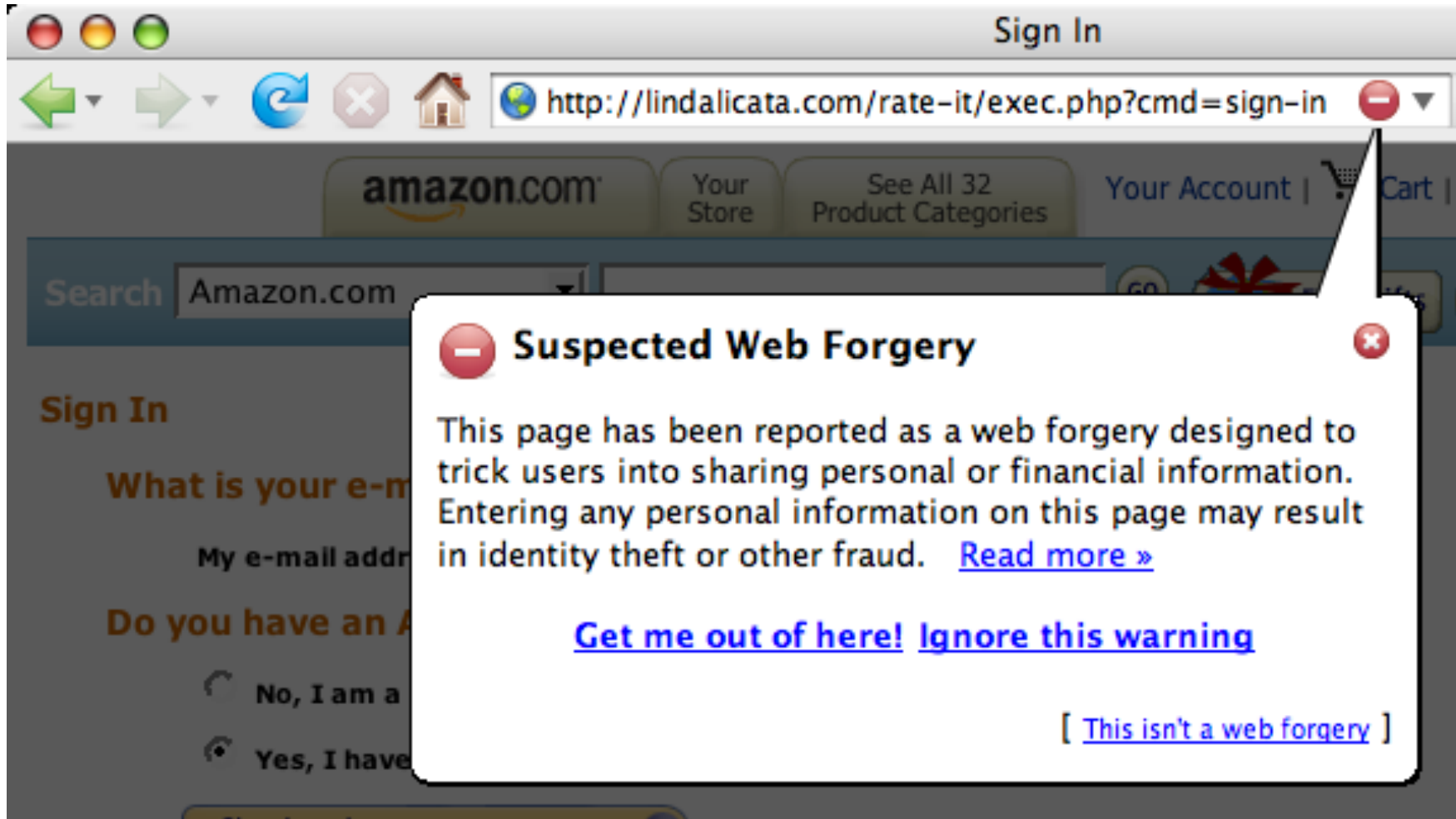
Passive IE Phishing Warning



Active IE Phishing Warning



Active Firefox Phishing Warning





How well do you think the phishing warnings work?

How well do the techniques work?

Condition Name	Size	Clicked	Phished
Firefox	20	20 (100%)	0 (0%)
Active IE	20	19 (95%)	9 (45%)
Passive IE	10	10 (100%)	9 (90%)
Control	10	9 (90%)	9 (90%)

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.

Condition Name	Sample Size	Saw Warning	Read Warning	Recognized Warning	Understood Meaning	Understood Choices
Firefox	20	20	13	4	17	19
Active IE	20	19	10	10	10	12
Passive IE	10	8	3	5	3	5

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

