Usable Security: Phishing

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 ‘s (ASU) talk from last year

Outline

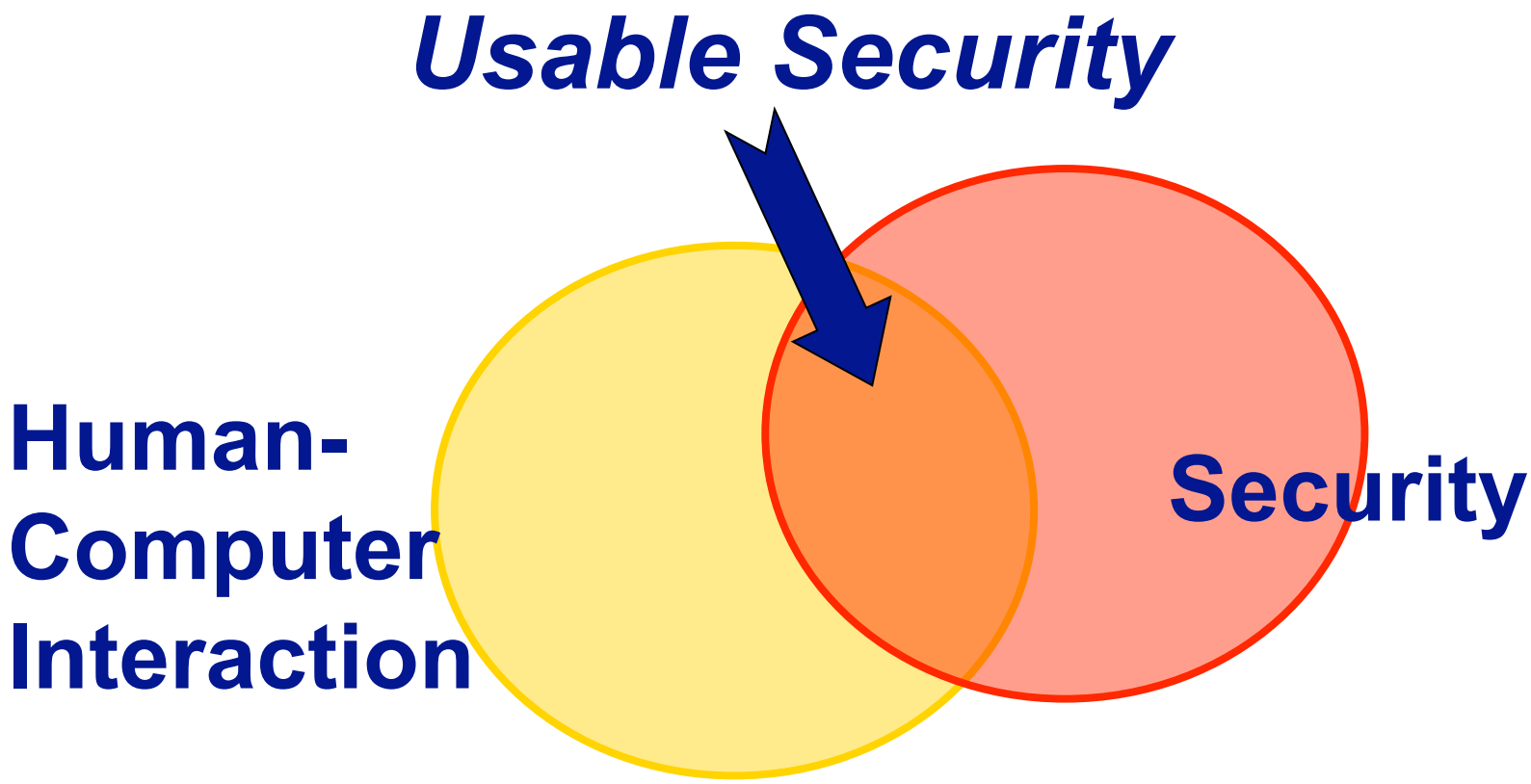
- Usable security
  - Challenges of humans in the loop
  - Usability guidelines
  - Heuristic evaluation
- Case study: Phishing

What you should learn?

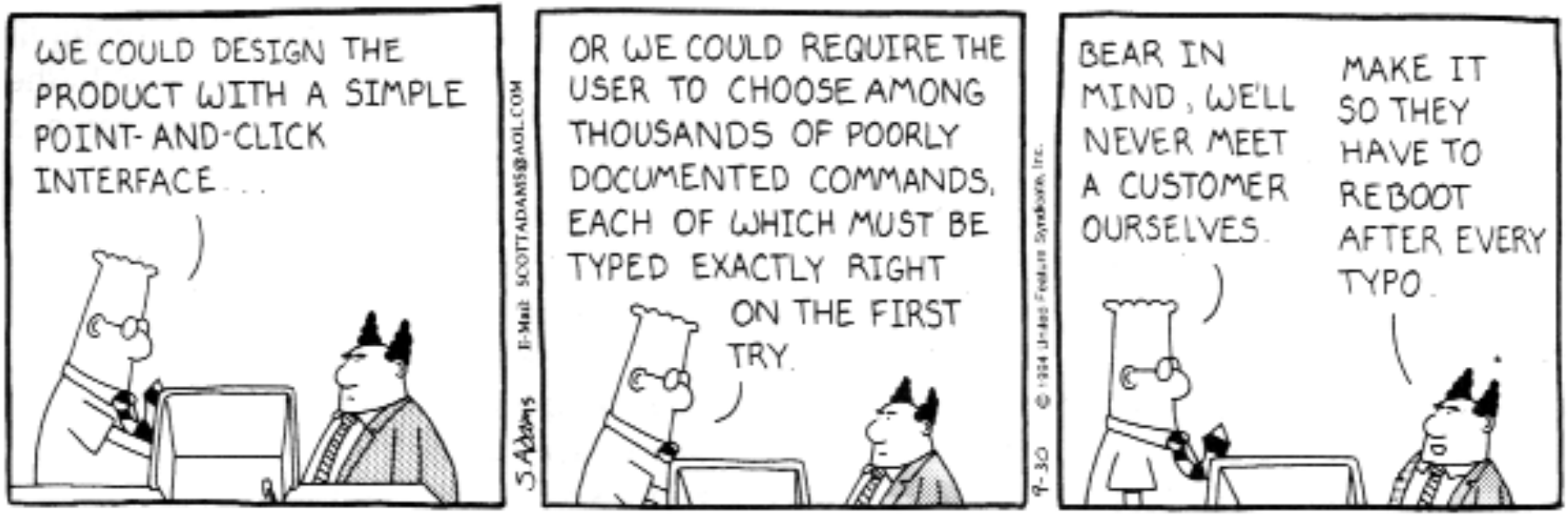
- Usable security challenges
- Usability guidelines
- How to apply them
- All about phishing (ok maybe not all)

Why should you learn this?

- Local reason: material will be on assignment and/or test
- Global reason: usable security is a hot topic in industry & academia


Usable Security
Human-Computer Interaction
Security

Usability


WE COULD DESIGN THE PRODUCT WITH A SIMPLE POINT-AND-CLICK INTERFACE...
OR WE COULD REQUIRE THE USER TO CHOOSE AMONG THOUSANDS OF POORLY DOCUMENTED COMMANDS, EACH OF WHICH MUST BE TYPED EXACTLY RIGHT ON THE FIRST TRY.
BEAR IN MIND, WE'LL NEVER MEET A CUSTOMER OURSELVES.
MAKE IT SO THEY HAVE TO REBOOT AFTER EVERY TYPO.

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

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

Dealing with humans in the loop


PAL Spyware
webroot
Spy Sweeper
2004
Spyware
Eliminator
Anonymous Surfing
Privacy Protection That Defends Your Confidential Information
COOKIES
POP!
SPAM
Hormel
Norton
AntiVirus
2004
synantec.
OEM VERSION
Net Nanny
Encryption for Everyone
PGP
Pretty Good Privacy
HARDENED
PGP
O'Reilly & Associates, Inc.

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

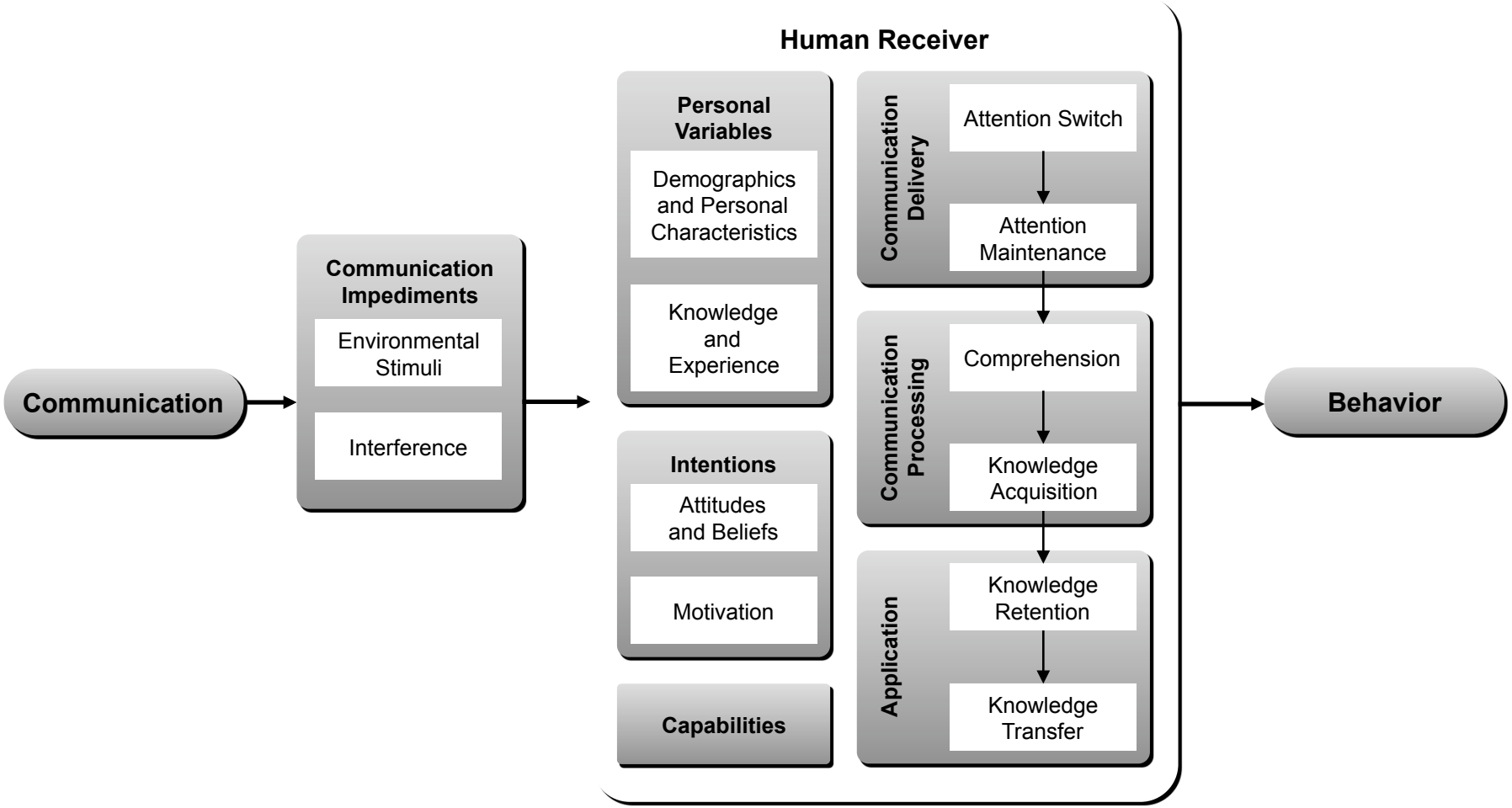
Approaches to usable security

- 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

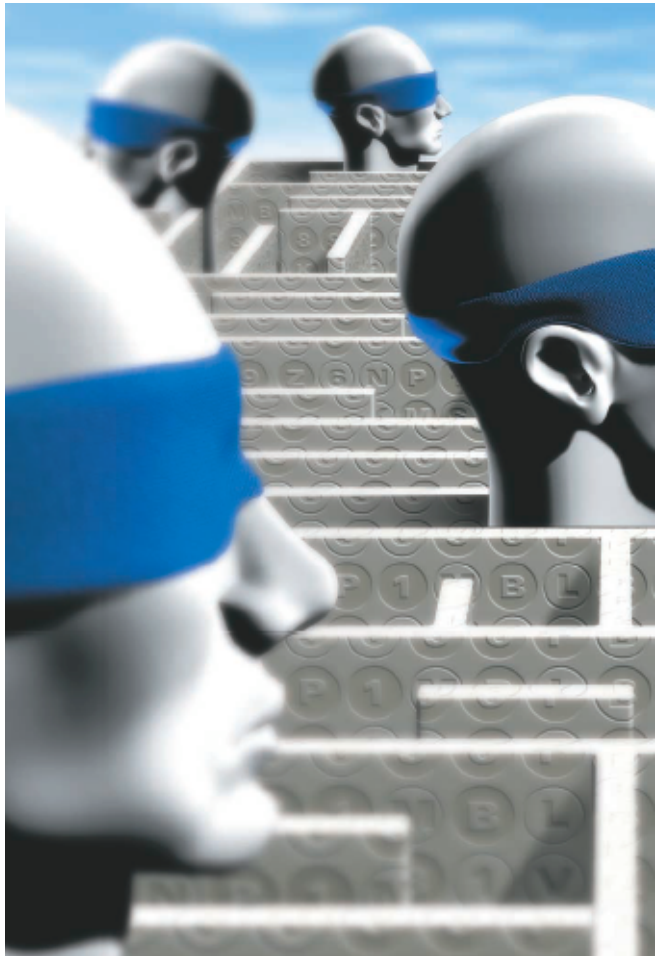
HCI: Understanding humans

- Do they know they are supposed to be doing something?
- Do they understand what they are supposed to do?
- Do they know how to do it?
- Are they motivated to do it?
- Are they capable of doing it?
- Will they actually do it?

Cranor's Human in the Loop Security Framework

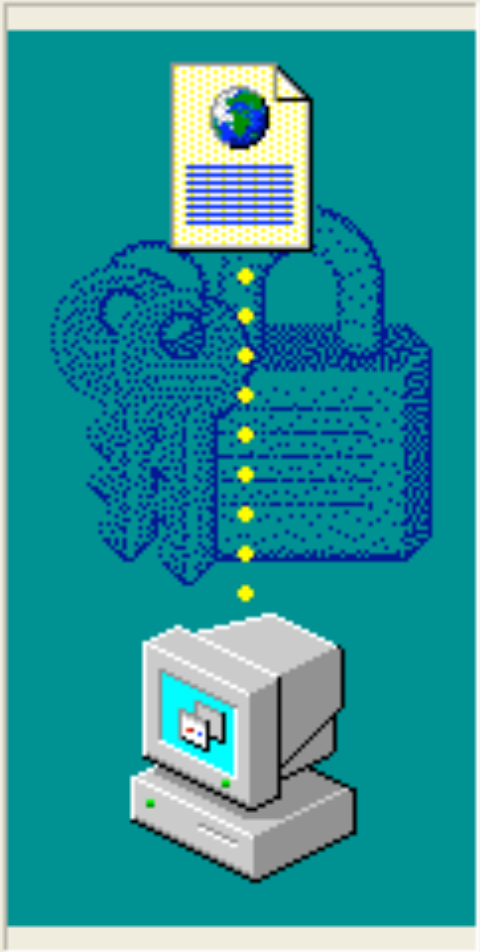


Help Users Make Decisions



- Developers should not expect users to make decisions they themselves can't make
- Present choices, not dilemmas

Security Warning



Do you want to install and run "MSN Chat Control 9.2.310.2401" signed on 10/27/2003 2:12 PM and distributed by:

Microsoft Corporation MSN

Publisher authenticity verified by Microsoft Code Signing PCA

Caution: Microsoft Corporation MSN asserts that this content is safe. You should only install/view this content if you trust Microsoft Corporation MSN to make that assertion.

☐ Always trust content from Microsoft Corporation MSN

Yes | No | More Info


Internet Explorer - Security Warning
Do you want to install this software?
Name: MSN Chat Control 9.2.310.2401
Publisher: Microsoft Corporation MSN
Always install software from "Microsoft Corporation MSN"
Never install software from "Microsoft Corporation MSN"
Ask me every time
Fewer options
Install
Don't Install
While files from the Internet can be useful, this file type can potentially harm your computer. Only install software from publishers you trust. What's the risk?


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:FA:54:CF
MD5 Fingerprint	AB:DB:89:FA:9E:B6:FA:8D:E5:DF:72:B5:0B:D5:DD:FE

Help | Close

General | Details

Certificate Hierarchy

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

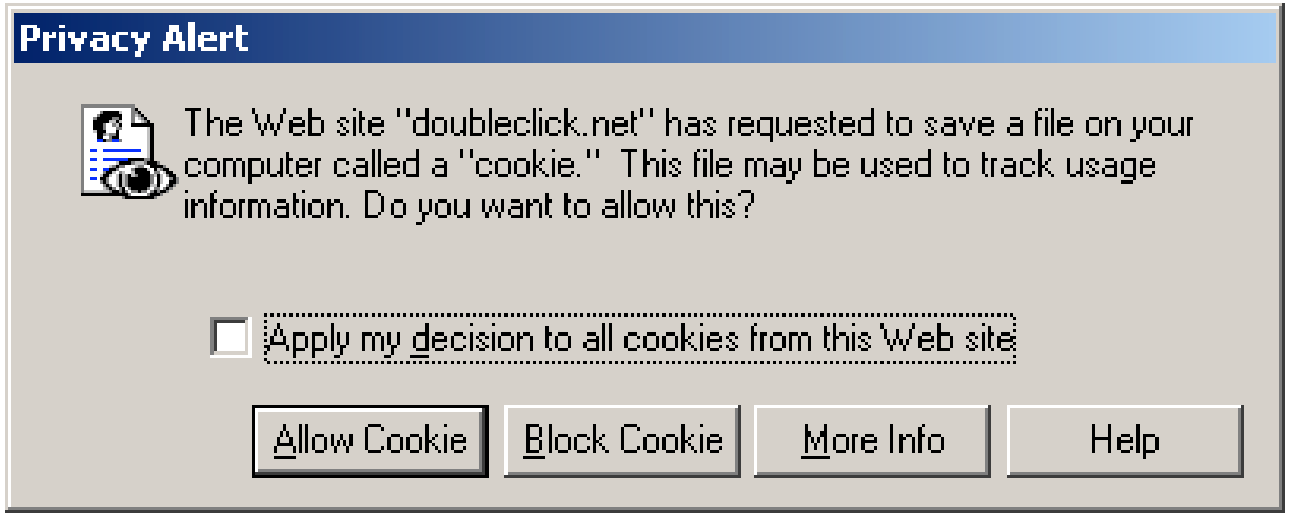
Certificate Fields

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

Field Value

Help | Close

Making concepts understandable



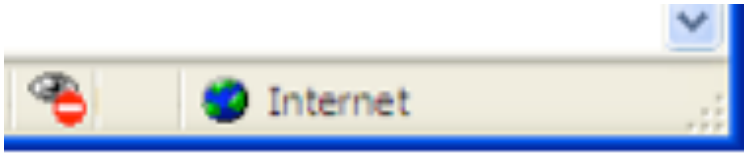
Making security and privacy visible

- Users could better manage online privacy and security if cues were more visible
- Cues must be understandable

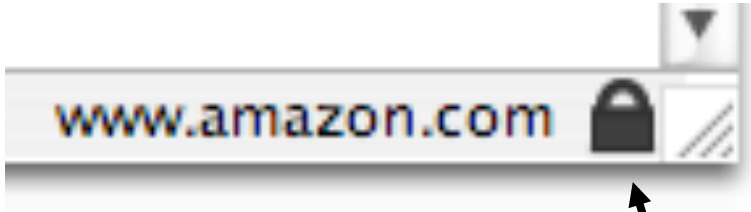
Symbols & Metaphors

Cookie flag

Netscape SSL icons



IE6 cookie flag



Firefox SSL icon

Privacy Bird Icons

Web site privacy policies

- Many posted, few read

Privacy policy *matches* user's privacy preferences

Privacy policy *does not match* user's privacy preferences

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?

Designing and Developing Usable and Secure Systems

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

Heuristic Evaluations

- Discount usability technique
- Experts adopt the role of target users
- Review the prototype and identify issues
  - Complete core scenarios developed from requirements gathering
  - Identify usability issues through the application of design guidelines

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

Yee's Principles for Secure Systems (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.
- **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

Heuristic evaluation

√ Pros:

- Quick & Dirty (do not need to design experiment, get users, etc)
- Good for finding obvious usability flaws

X Cons:

- Experts are not the “typical” user!

Next up:

- A class of security attacks that target end-users rather than computer systems themselves.
- Some slides are based on existing ones; credit on the bottom

A Recent Email…

usbank
Five Star Service Guaranteed

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.

Images from Anti-Phishing Working Group's Phishing Archive; Slide from "Pholproff Phishing Prevention" by B. Parno, C. Kuo, A Perrig

U.S. Bank Internet Banking - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back 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 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.

Welcome to Internet Banking

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.

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

Connection Secured

Member FDIC

Privacy Pledge | Security Standards

© 2004 U.S. Bancorp

Images from Anti-Phishing Working Group's Phishing Archive; Slide from "Pholproff Phishing Prevention" by B. Parno, C. Kuo, A Perrig

The next page requests:

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

Slide from “Pholproff Phishing Prevention” by B. Parno, C. Kuo, A Perrig

U.S. Bank Internet Banking - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites Media

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

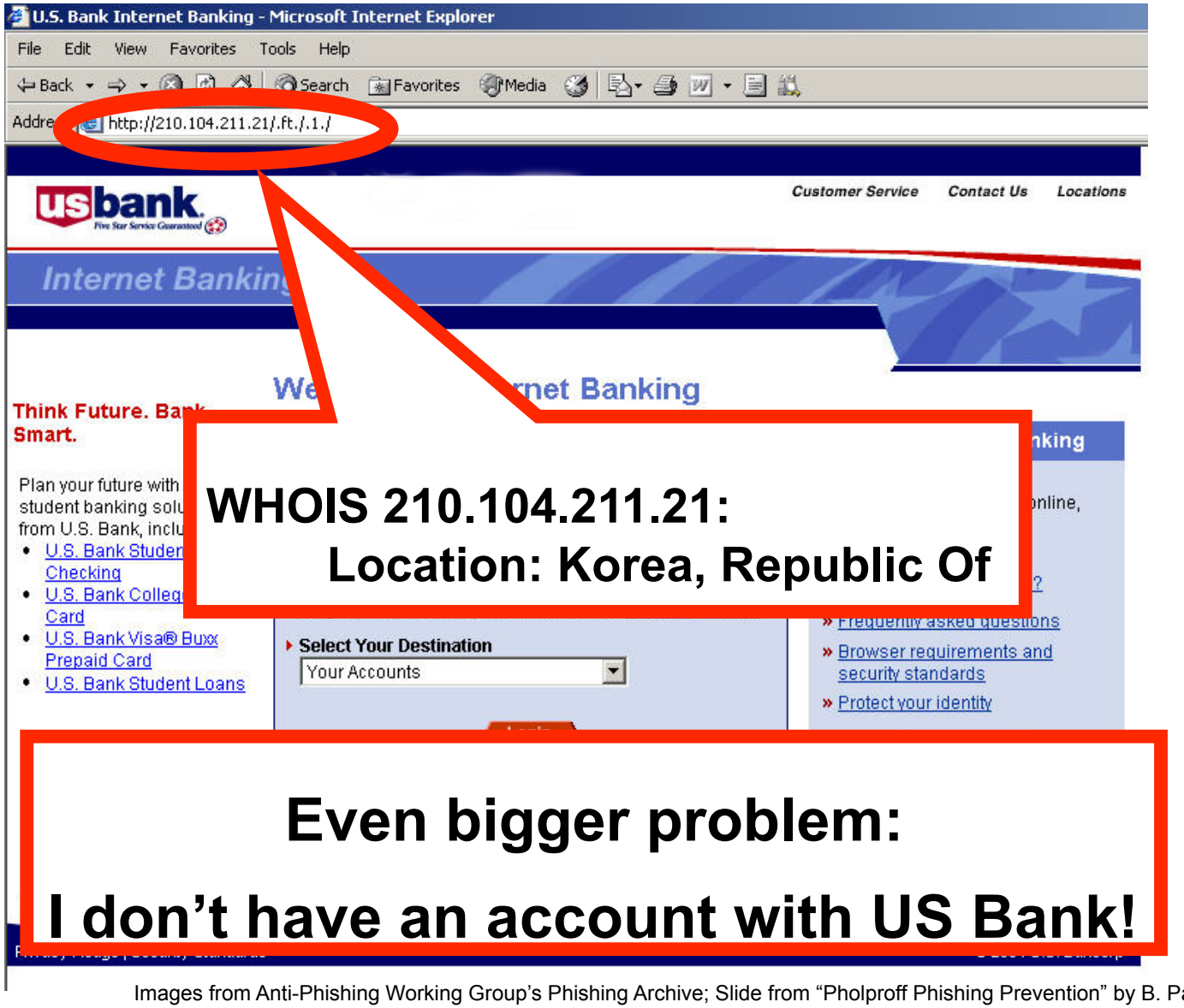
Member FDIC

Privacy Pledge | Security Standards

© 2004 U.S. Bancorp

Images from Anti-Phishing Working Group's Phishing Archive

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

They demand authentication from us… but do we also want authentication from ***<u>them</u>****?*

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)

Characteristics of a phishing attack

- **Social Engineering**. Phishing exploits individuals' vulnerabilities to dupe victims into acting against their own interests. (Lure)
- **Automation**. Computers are used to carry out phishing attacks on a massive scale.
- **Electronic Communication.** Phishers use electronic communications networks (primarily the Internet).
- **Impersonation**. A phishing attack requires perpetrators to impersonate a legitimate firm or government agency.

Phishing is NOT:

- Internet-based worms
- Virus-email
- Relatives stealing your wallet
- Spam

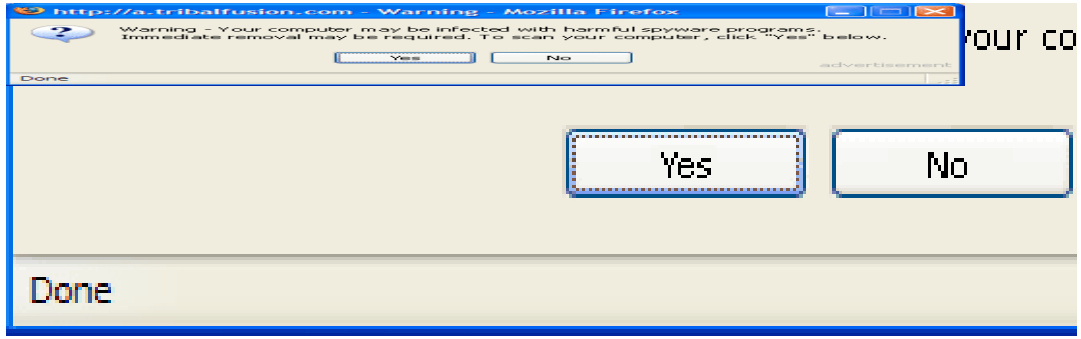
Slide from“A Leisurely Lunch Time Phishing Trip” by Patrick Cain

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



Slide based on one in “Pholproff Phishing Prevention” by B. Parno, C. Kuo, A Perrig

Impact of Phishing

- Hundreds of millions of $$$ cost to U.S. economy (e.g., 2.4 billion in fraud just for bank-related fraud)
- Affects 1+ million Internet users in U.S. alone
- What about privacy!
- The problem is growing… the number of phishing attacks doubled from 2004->2005 (from 16,000 to 32,000)

Slide based on one in "iTrustPage: Pretty Good Phishing Protection" S. Saroiu, T. Ronda, and A. Wolman

What can we do?

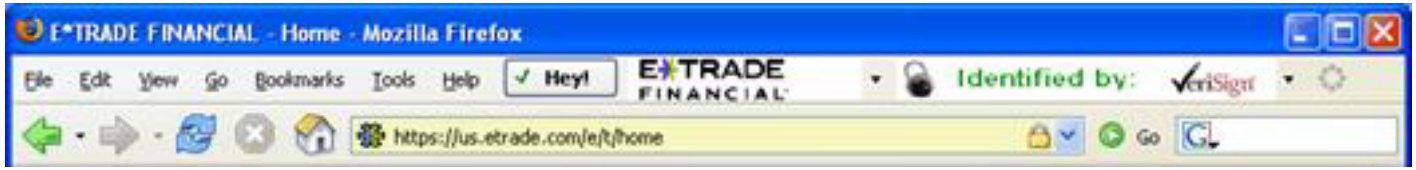
- Educate Users
- Good user interface design (usability guidelines)
- Help users make good decisions rather than presenting dilemmas

Slide based on one in “iTrustPage: Pretty Good Phishing Protection” S. Saroiu, T. Ronda, and A. Wolman

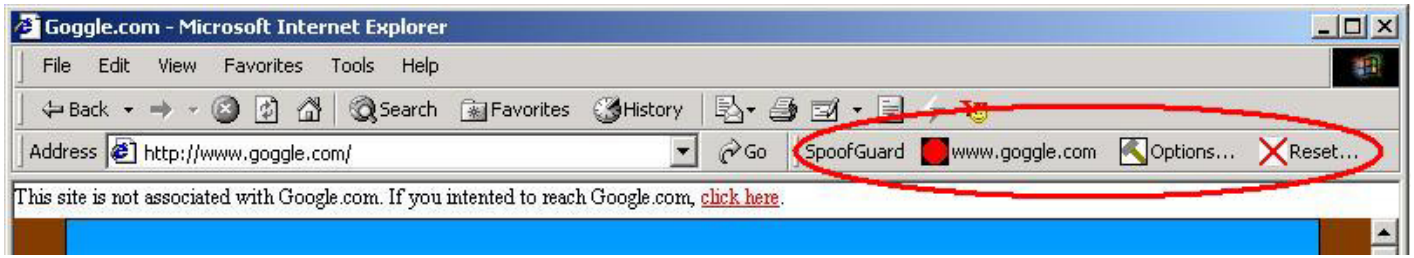
Phishing Education

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

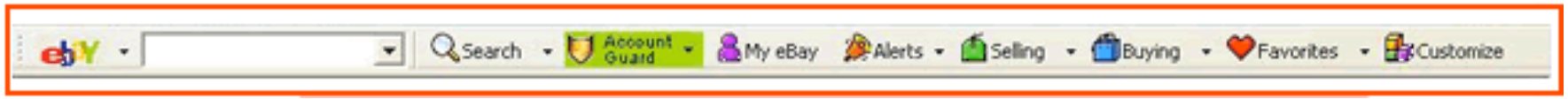
Other Solutions: Toolbars



Trustbar

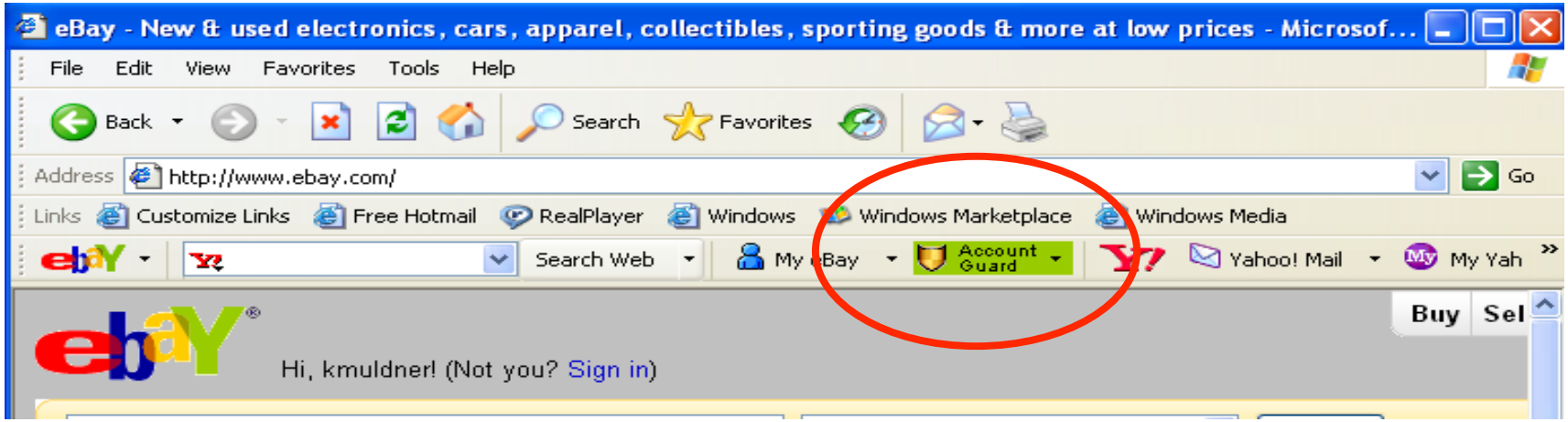


spoofguard

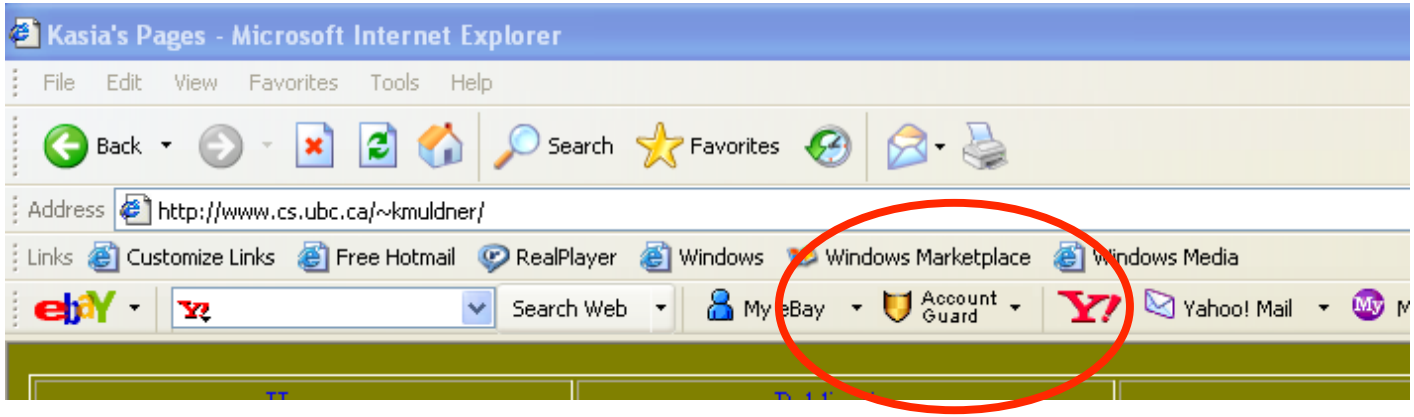


Accountguard

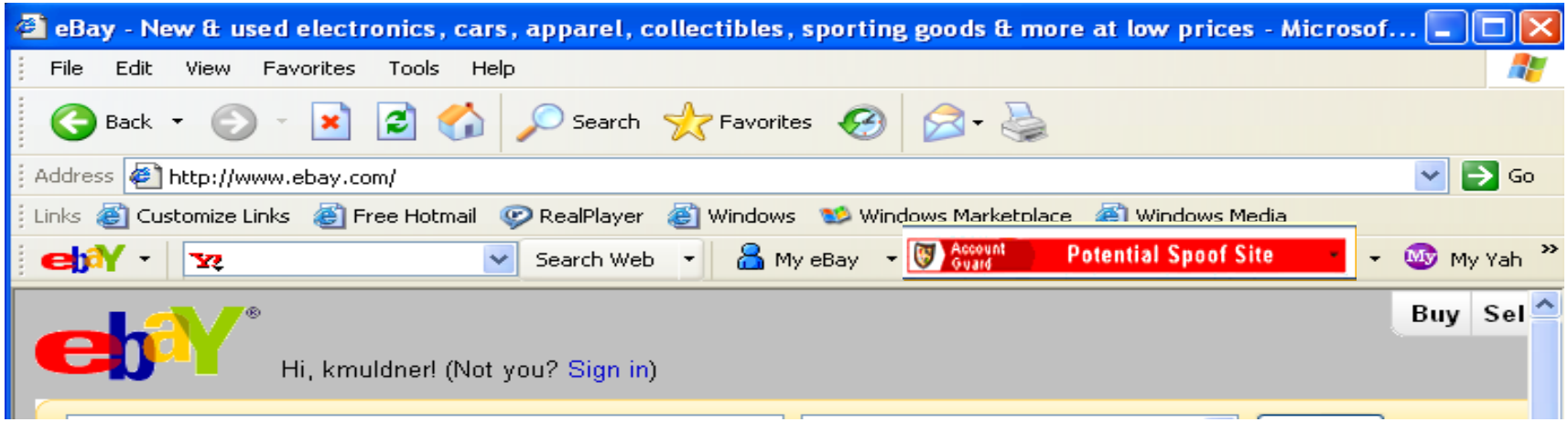
1) If you are on a verified eBay or PayPal web site.



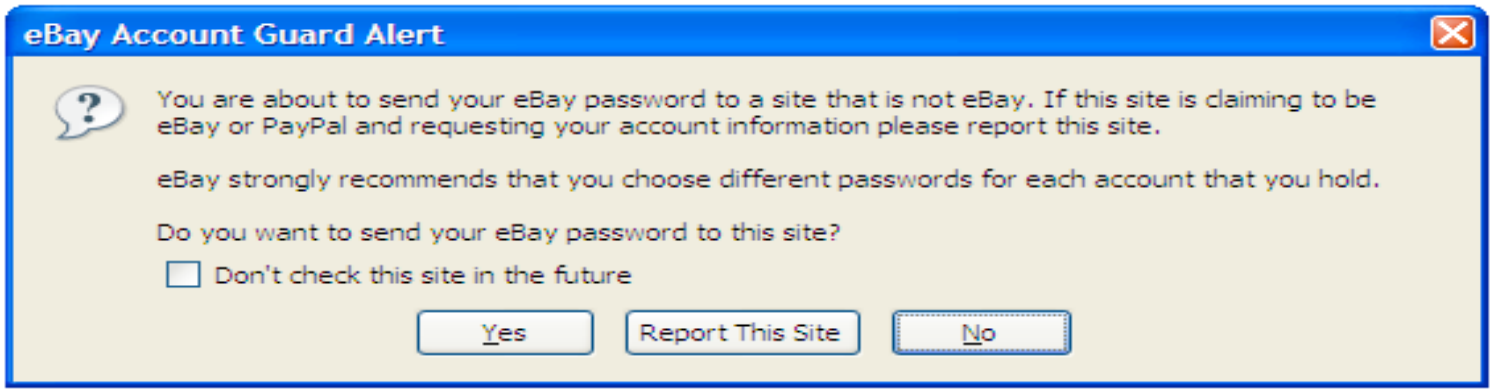
2) If you are on a non eBay or PayPal web site.



3) If you are on a potential spoof site, the icon turns red.



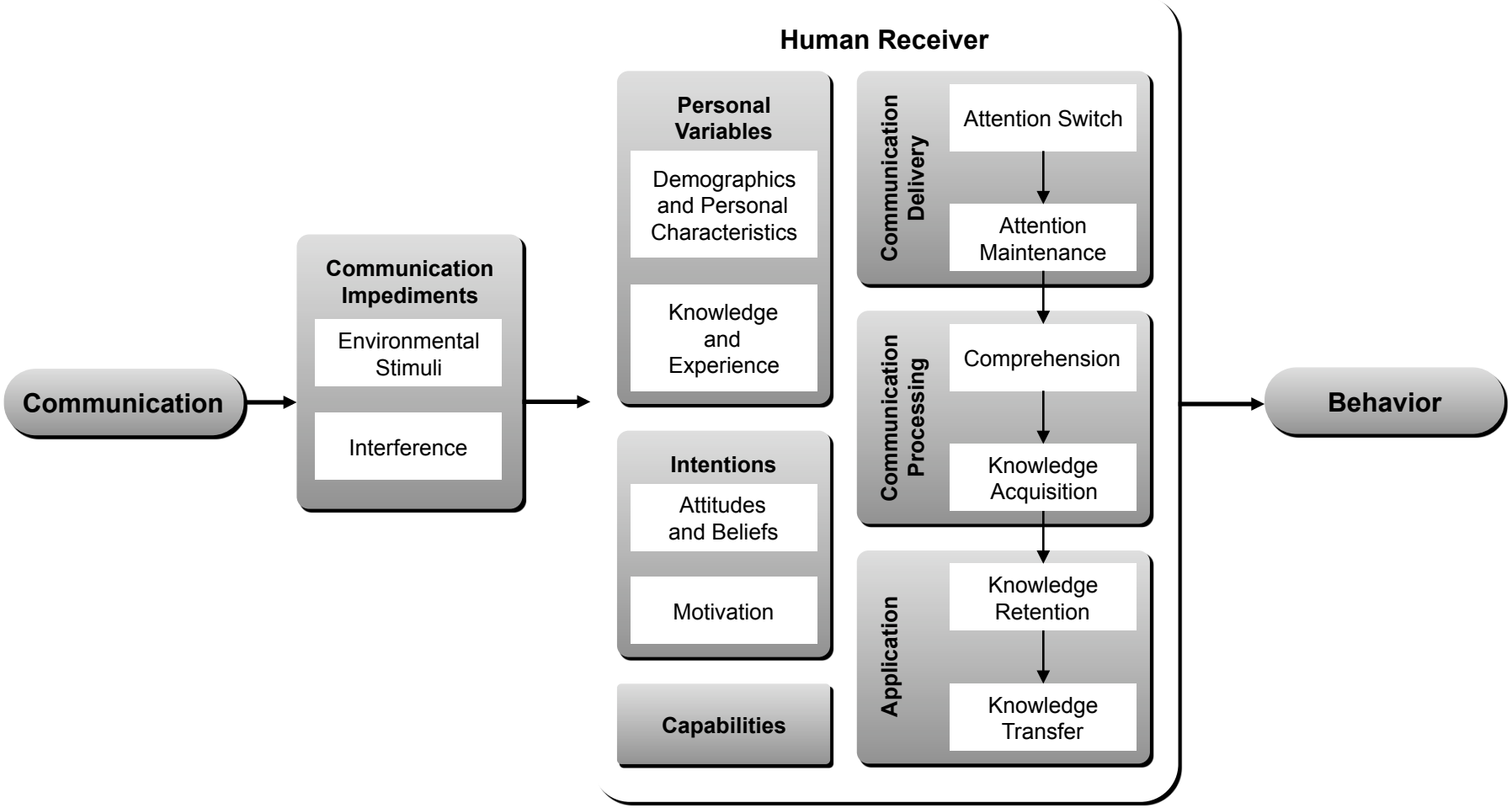
Will warn you when you are about to enter your eBay password into a non-eBay site .



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



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

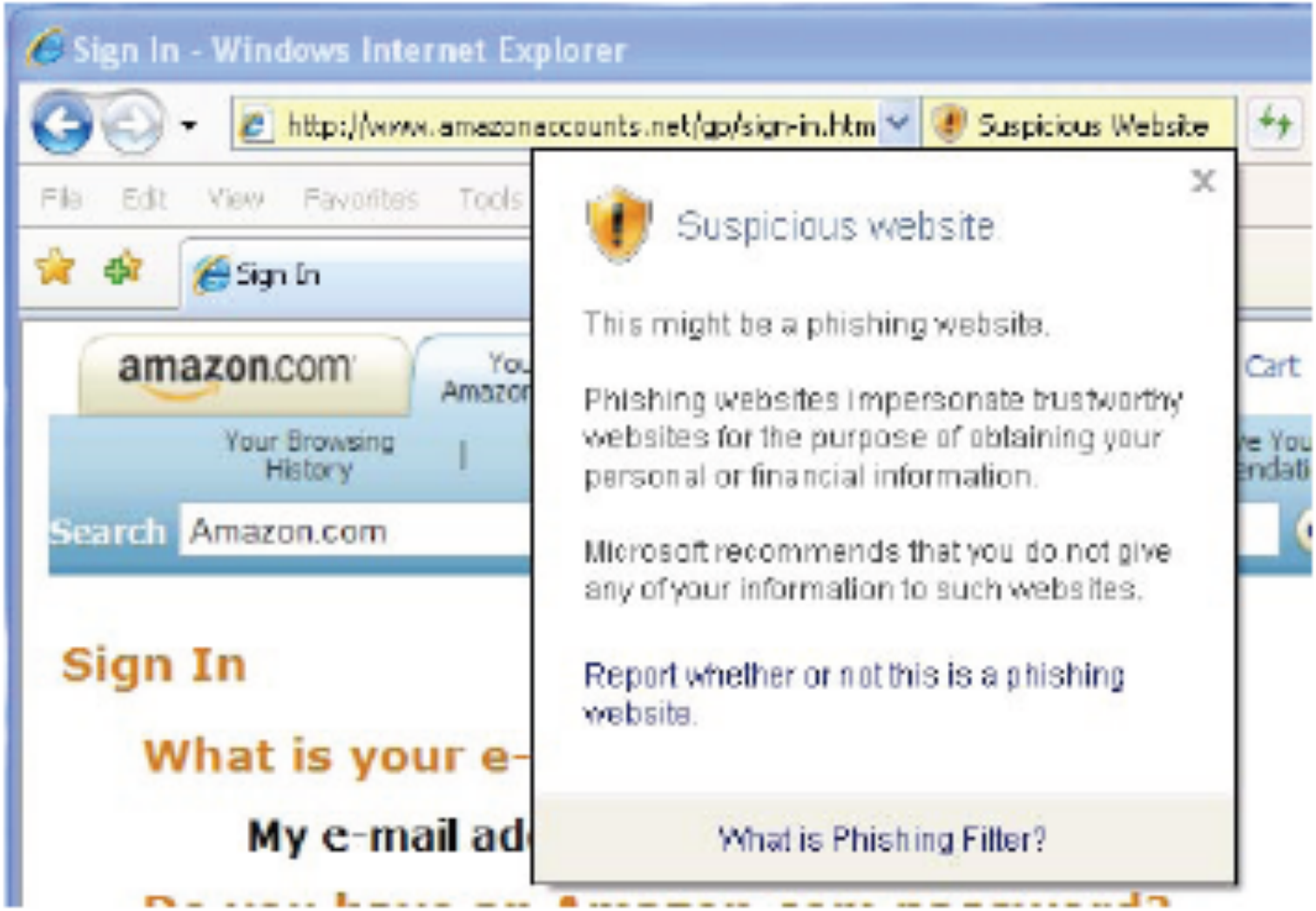
Serge Egelman
Carnegie Mellon University
egelman@cs.cmu.edu

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

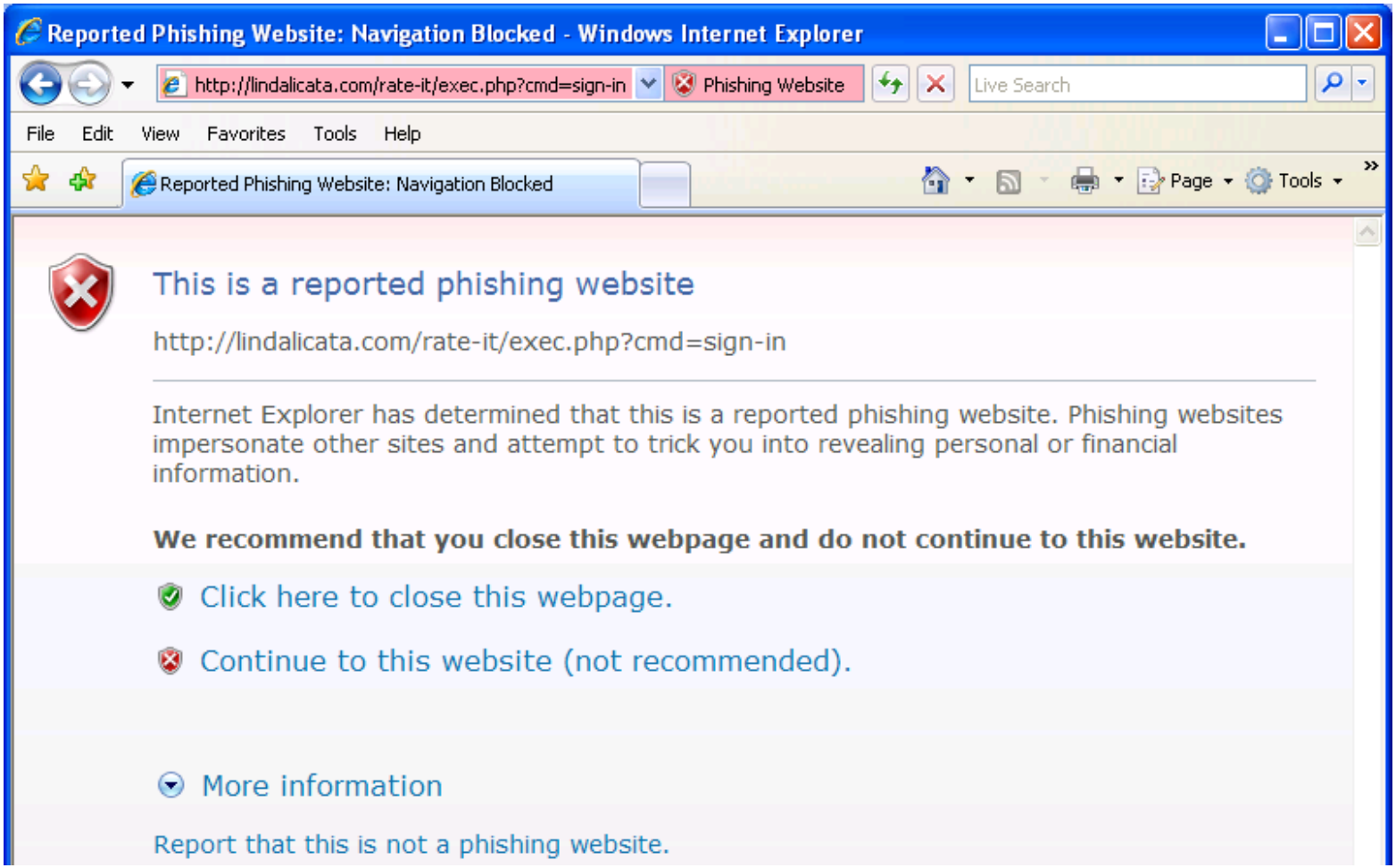
Jason Hong
Carnegie Mellon University
jasonh@cs.cmu.edu

- 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

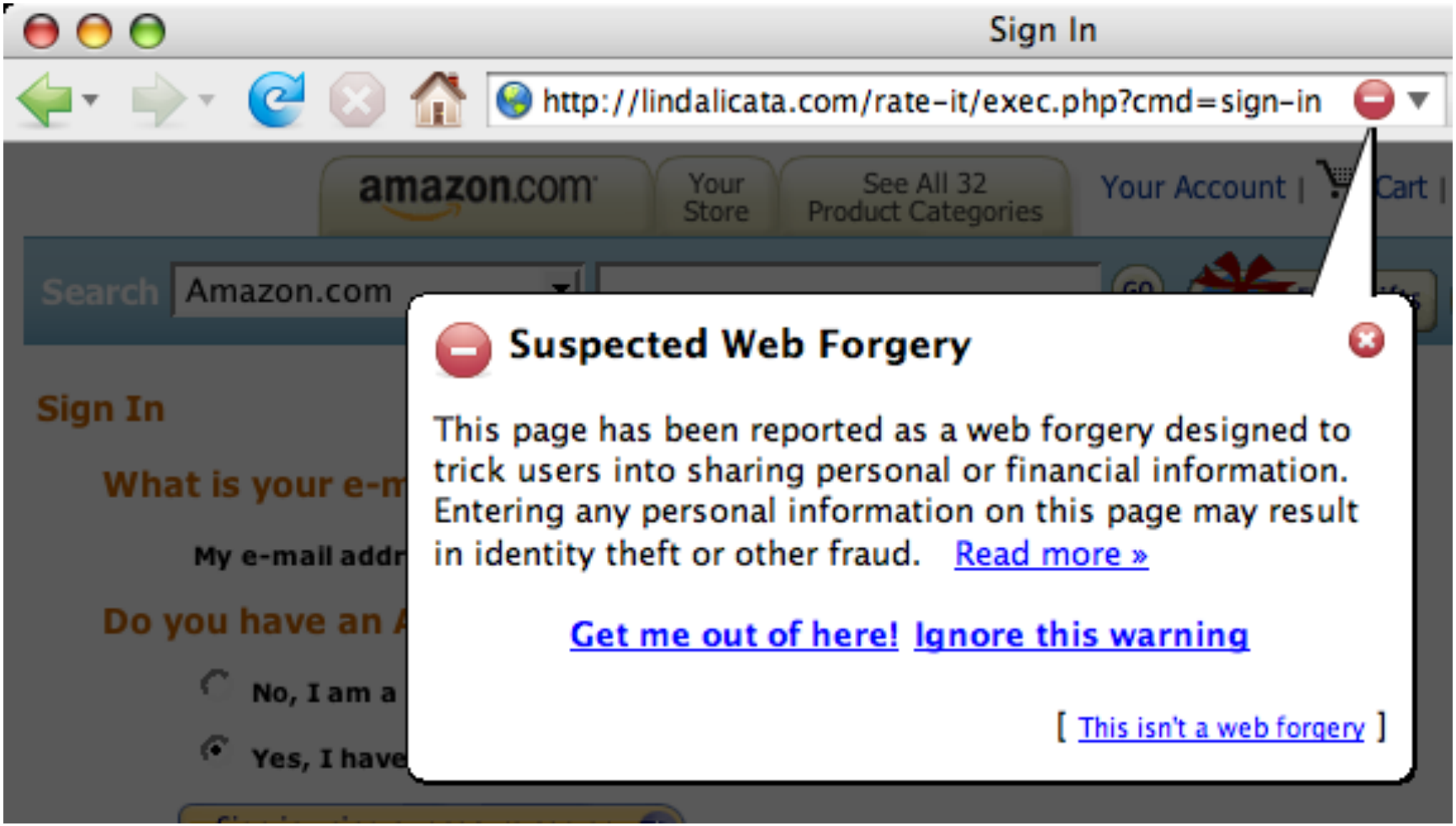
Passive IE Phishing Warning



Active IE Phishing Warning



Active Firefox Phishing Warning



How well do you think the phishing warnings work?

How well do the techniques work?

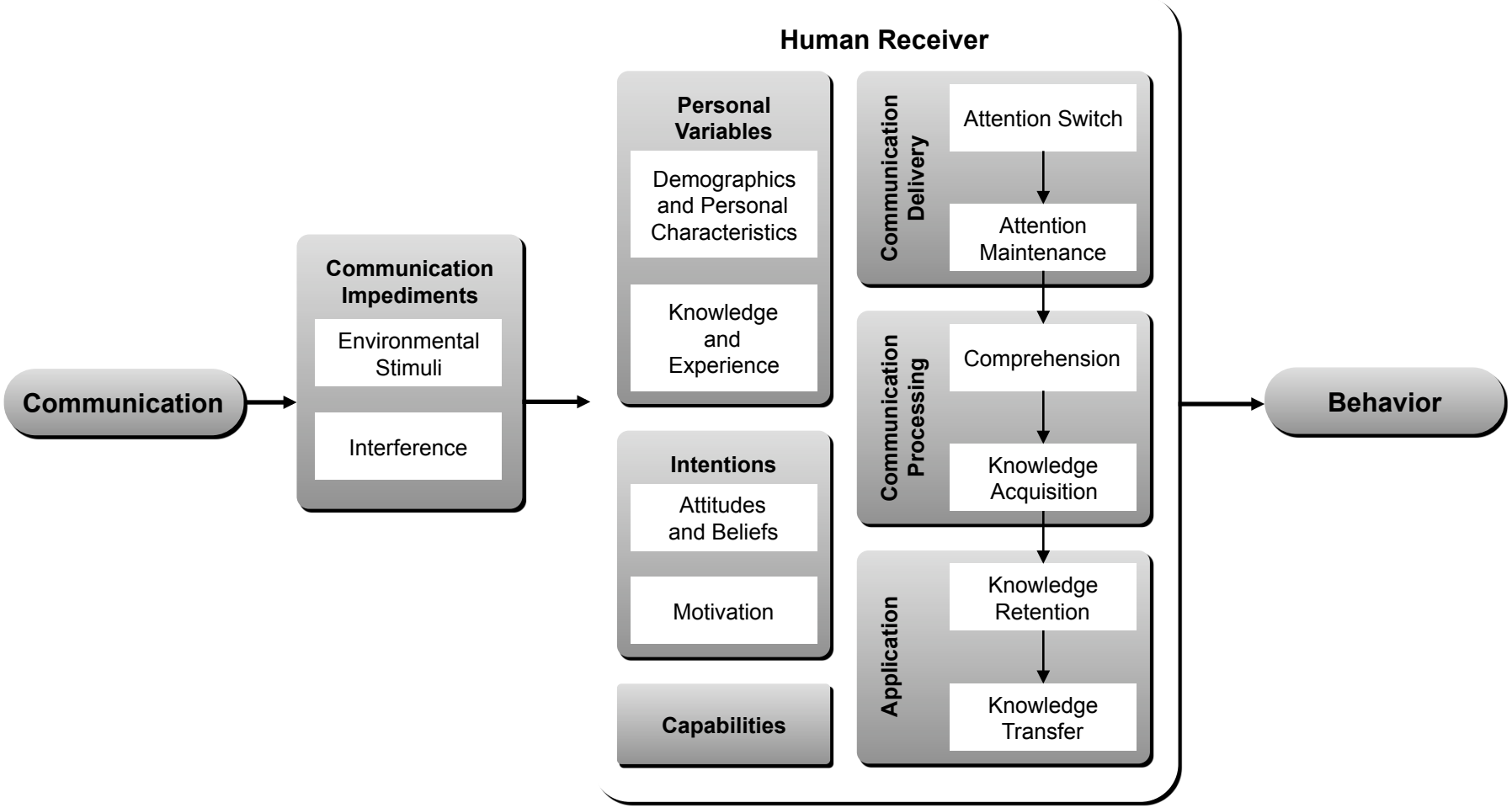
Condition Name	Size	Clicked	Phished
Firefox	20	20 (100%)	0 (0%)
Active IE	20	19 (95%)	9 (45%)
Passive IE	10	10 (100%)	9 (90%)
Control	10	9 (90%)	9 (90%)

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



Wrap-up

Revising "*What you should learn*"…

- Usable security challenges
- Usability guidelines
- How to apply them
- All about phishing (ok maybe not all)

Thank-you for your attention!