



# 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](http://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...



www.dilbert.com scottadams@aol.com



1-11-07 ©2007 Scott Adams, Inc./Dist. by UFS, Inc.



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



www.dilbert.com scottadams@aol.com



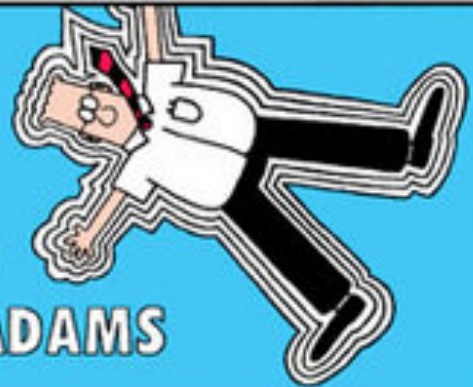
1-18-07 ©2007 Scott Adams, Inc./Dist. by UFS, Inc.



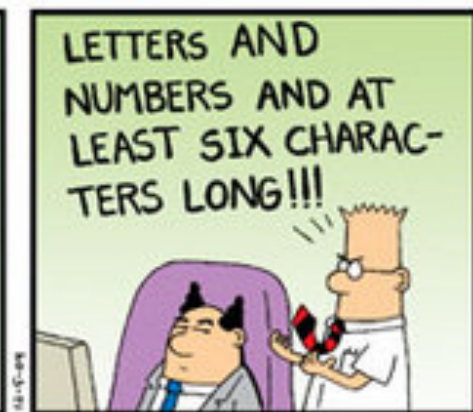
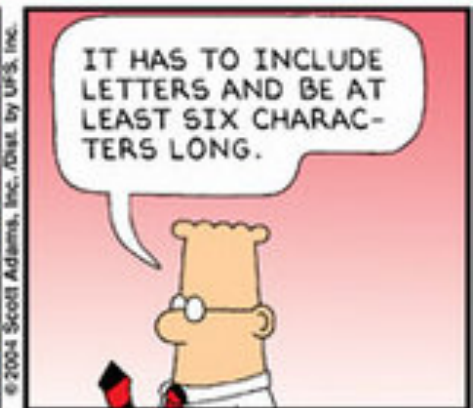
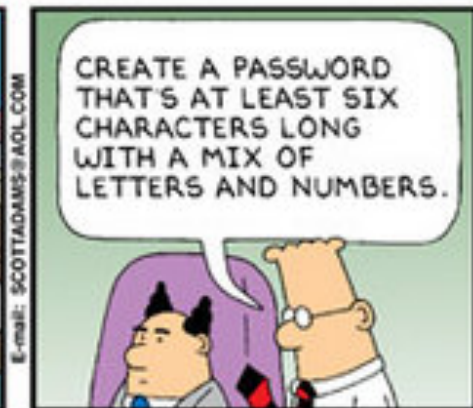
© Scott Adams, Inc./Dist. by UFS, Inc.



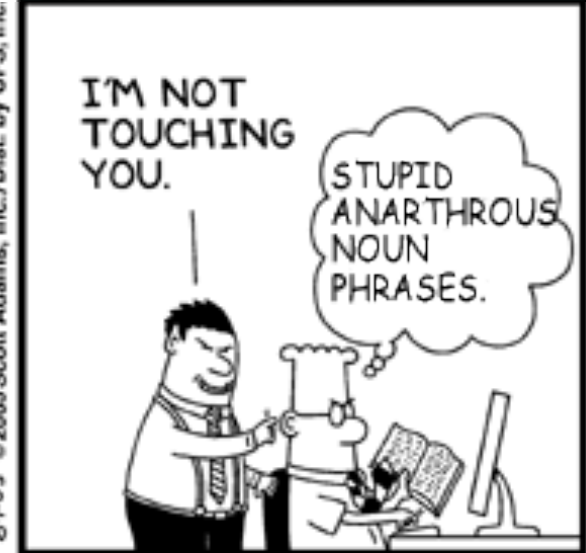
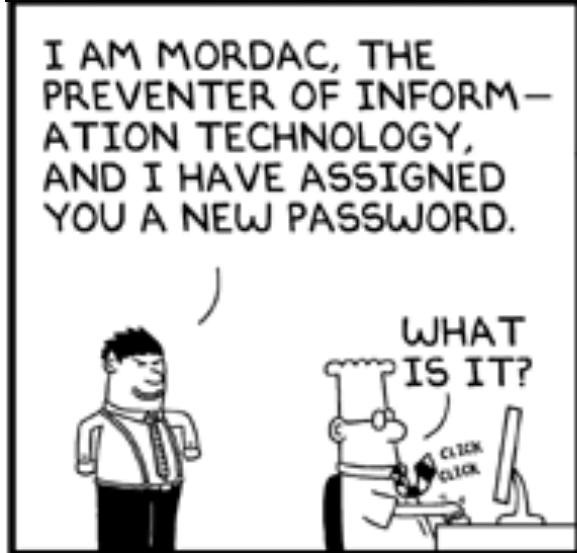
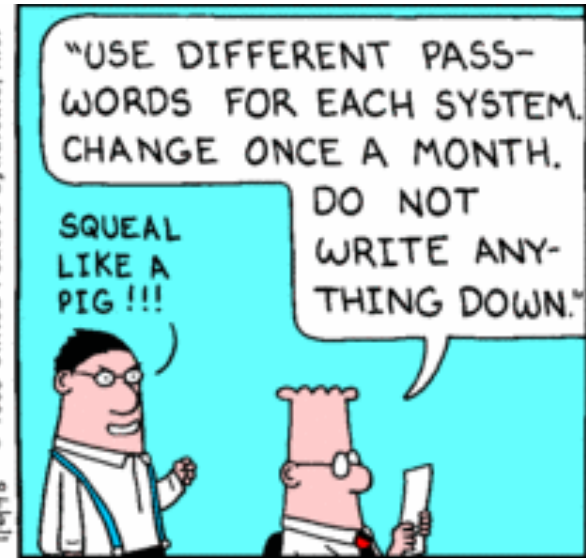
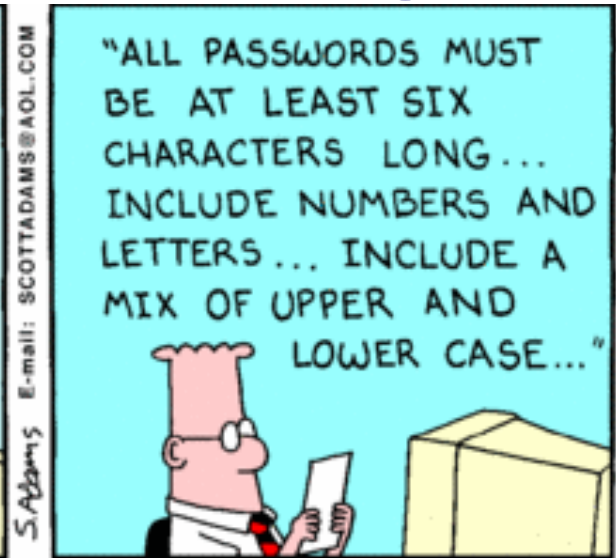
# DILBERT®



BY  
SCOTT ADAMS



# But are we asking too much?



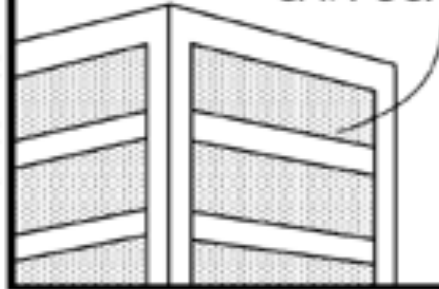
# Even biometrics can be painful...

I AM MORDAC, THE PREVENTER OF INFORMATION SERVICES, AND I BRING YOU MY NEWEST BIOMETRIC SCANNER.



www.dilbert.com scottadams@aol.com

INSTEAD OF A PASSWORD, I PUT THIS ON YOUR HEAD AND SQUEEZE UNTIL YOU SCREAM IN A WAY THAT ONLY YOU CAN SCREAM.



11-17-07 © 2007 Scott Adams, Inc./Dist. by UFS, Inc.

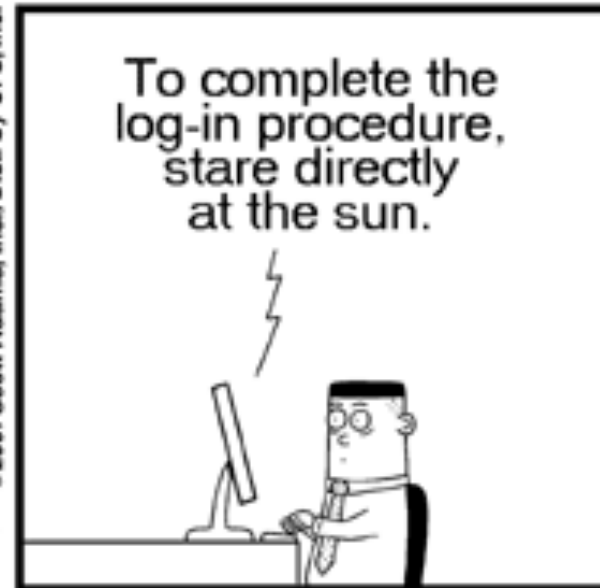
NO, THAT'S NOT YOU.

GAAA!  
GAAA!  
GAAA!



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

# Security as a barrier...



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

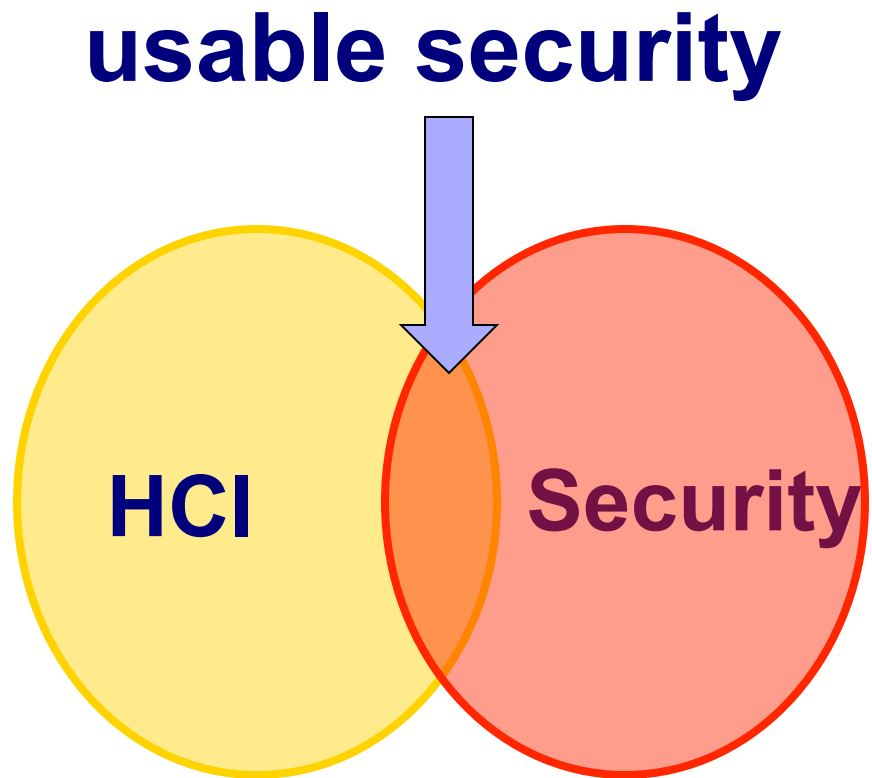


usability

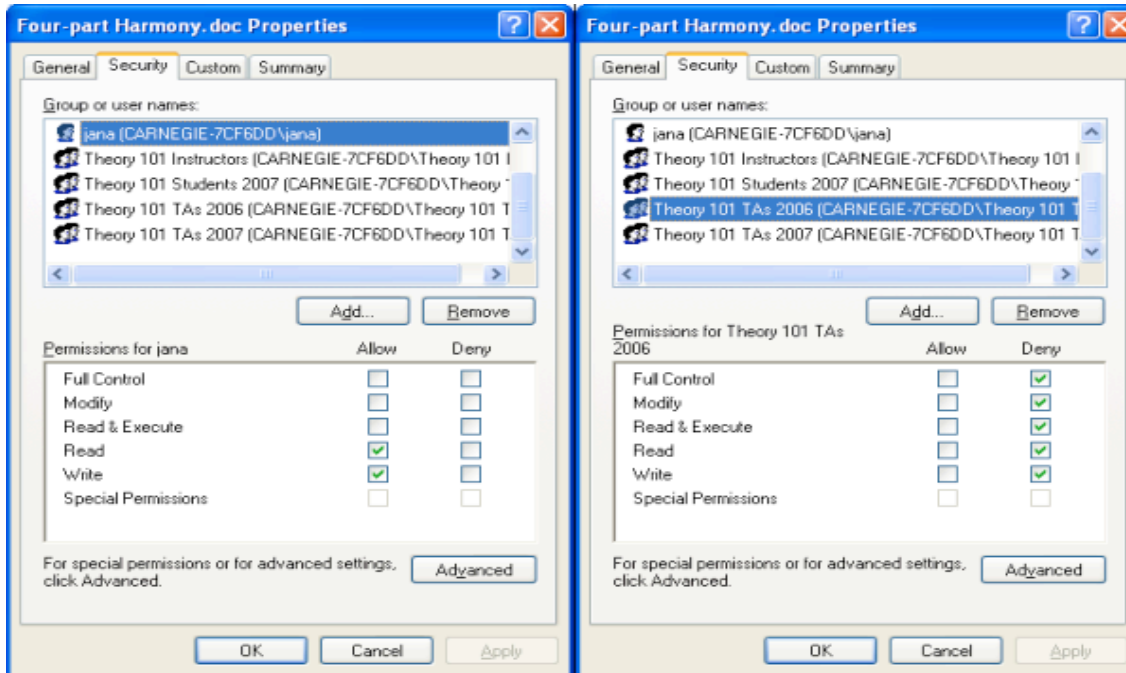
security

**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

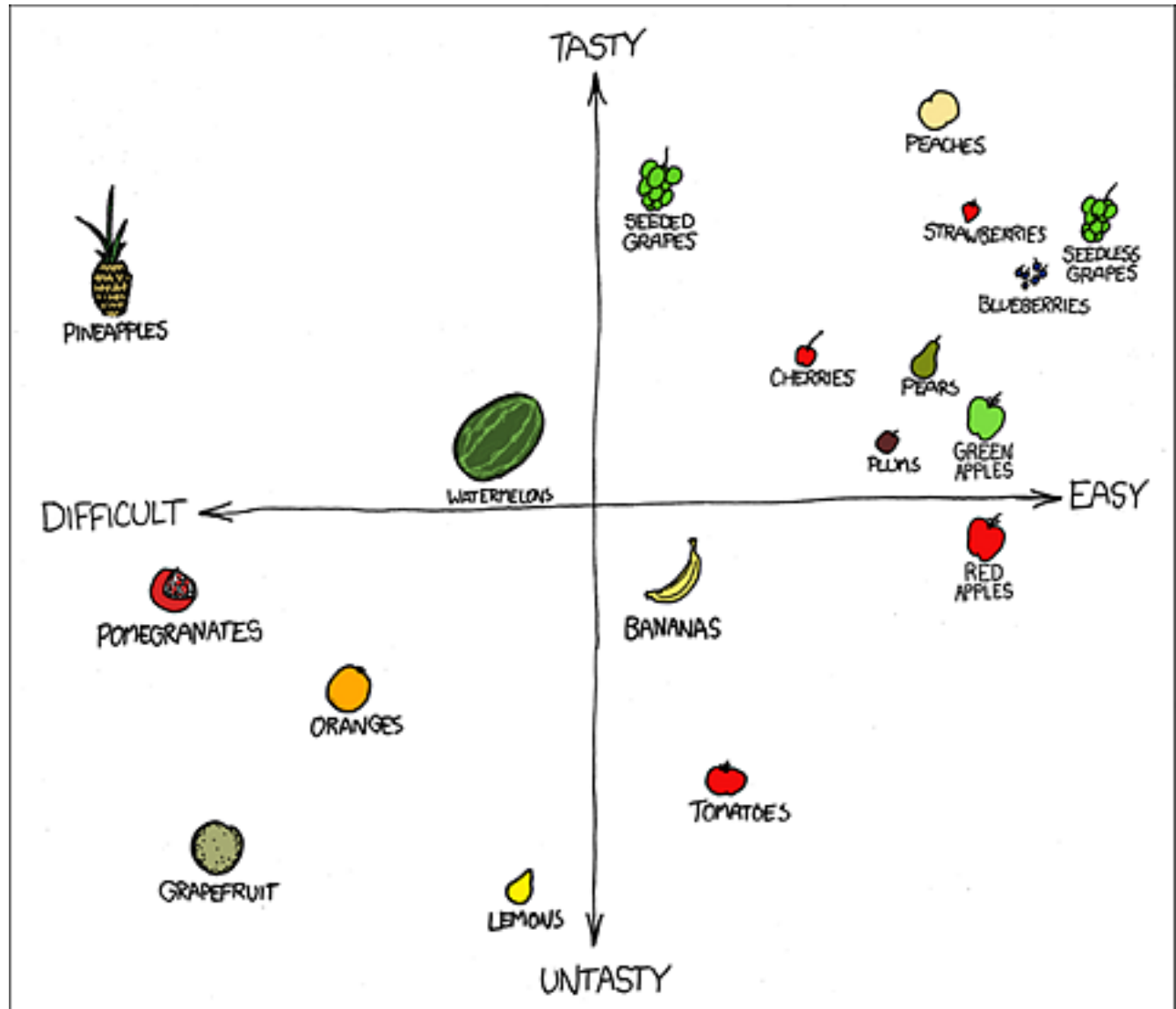
User-centred iterative approach

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

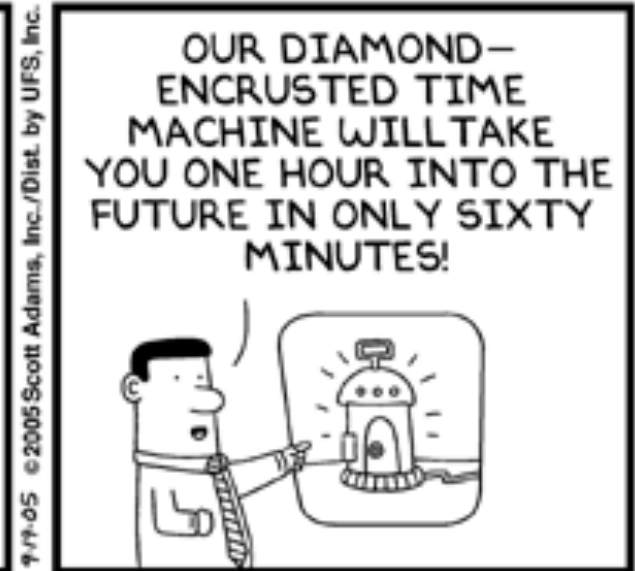


# Defining usability

## Usability of fruit



# Understand the user

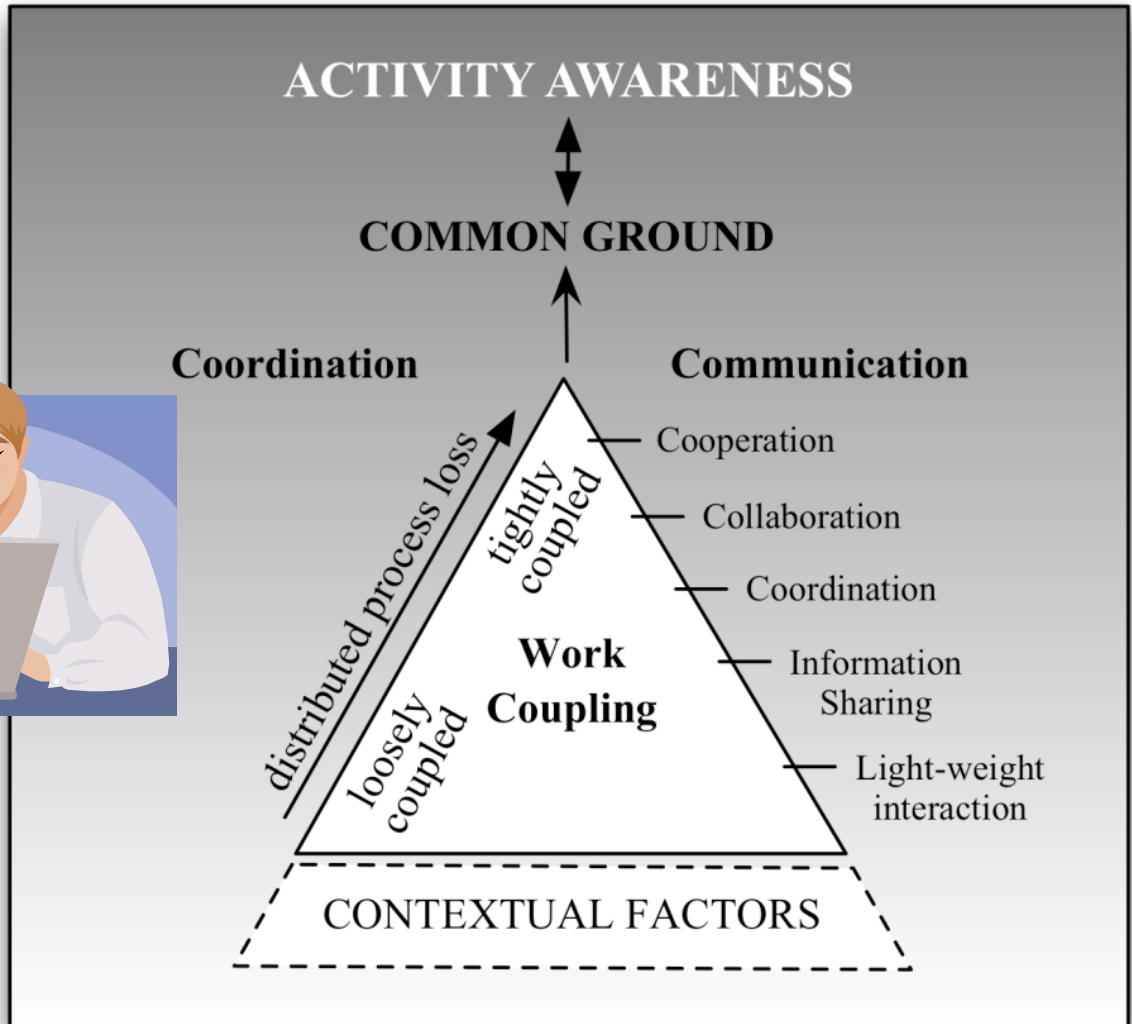


© Scott Adams, Inc./Dist. by UFS, Inc.



\$20,000 <http://www.mobilewhack.com>

# Understand the usage context



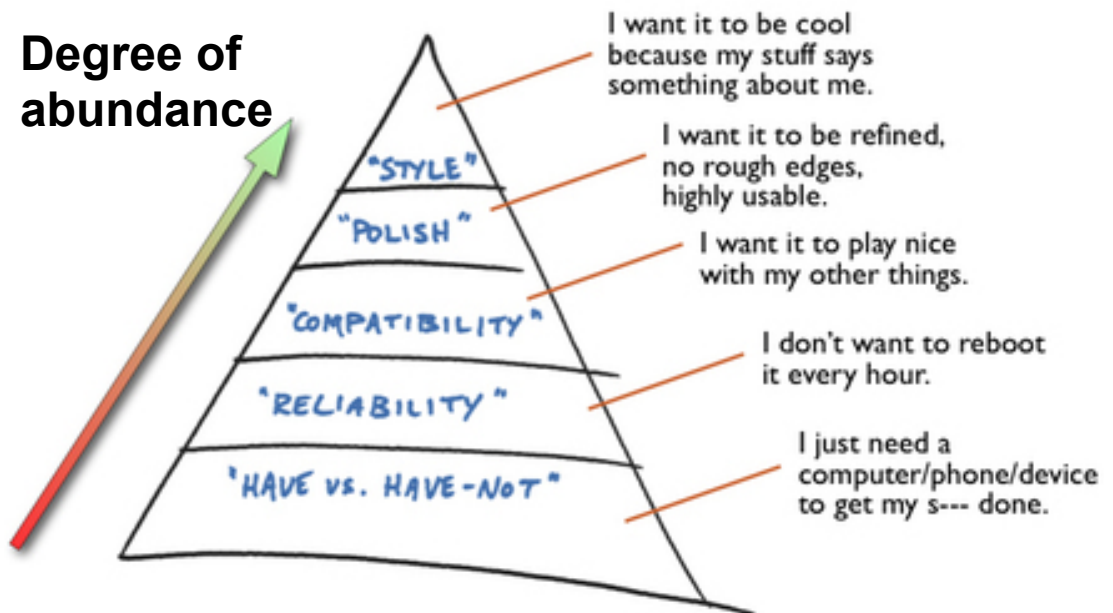
Neale, Carroll, Rosson. Evaluating computer-supported cooperative work: models and frameworks. In CSCW '04.



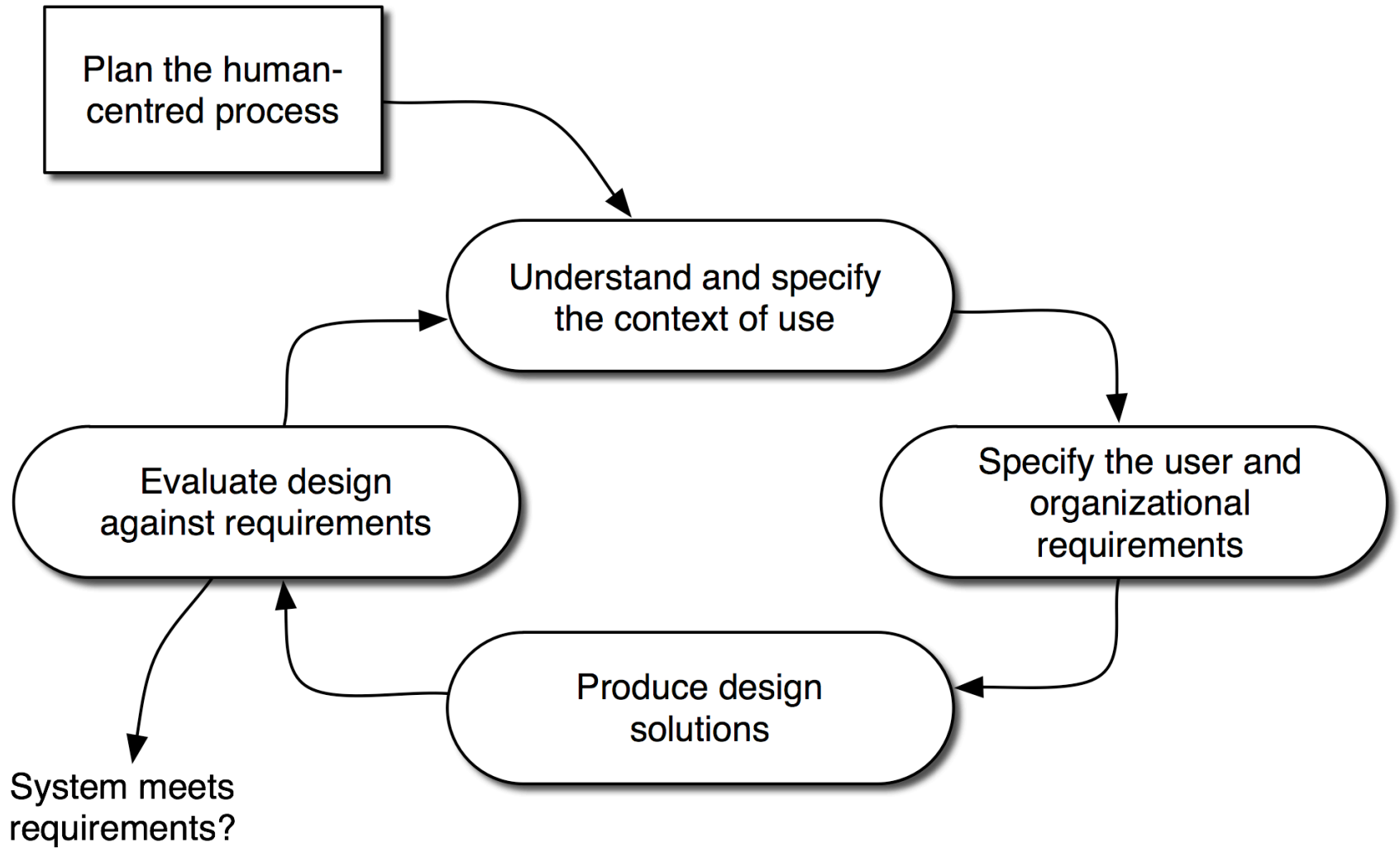
# Understand their expectations

- 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](http://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



Example

# **PRINCIPLE OF LEAST PRIVILEGE IN WINDOWS**

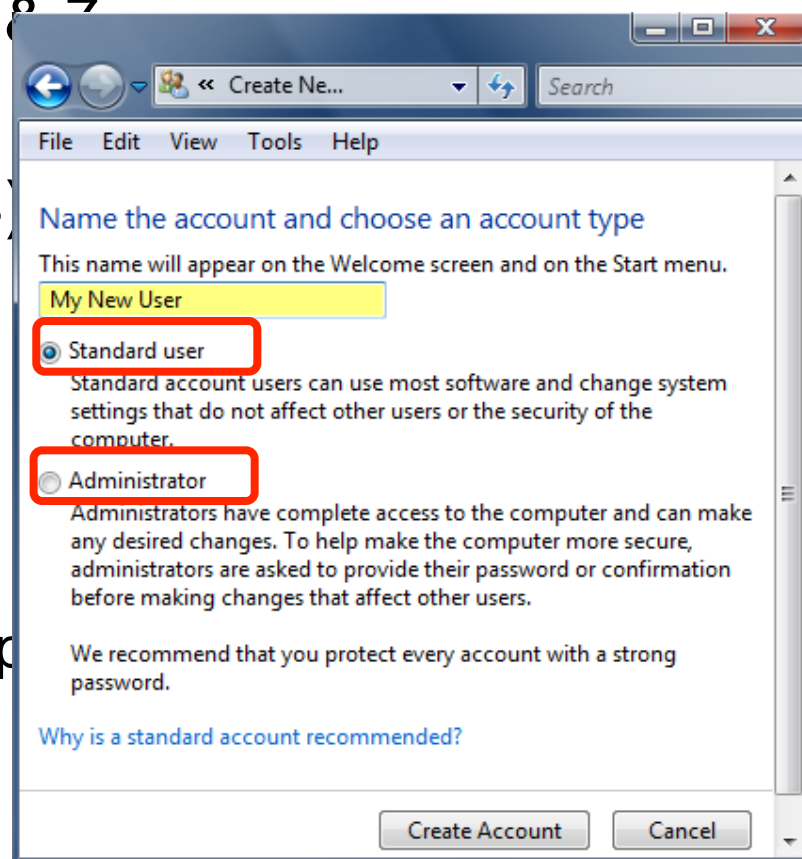


# User Account Usage

All 45 participants used **Administrator** user account on their laptops.

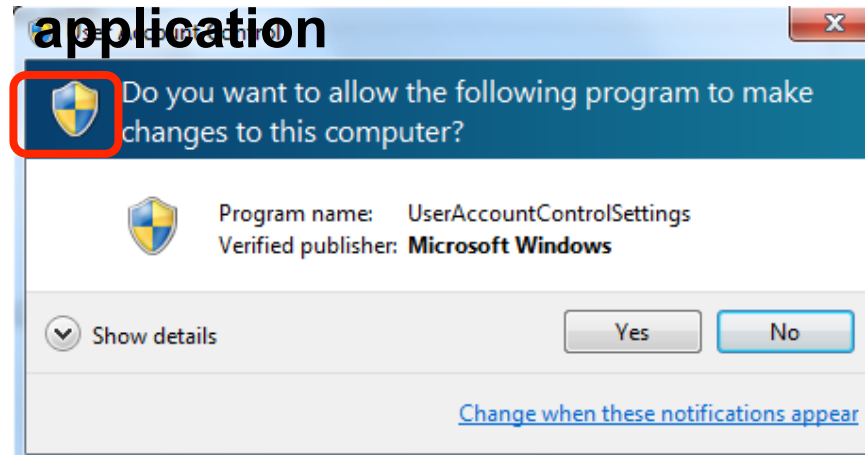
# User Account Control (UAC)

- 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 prompts

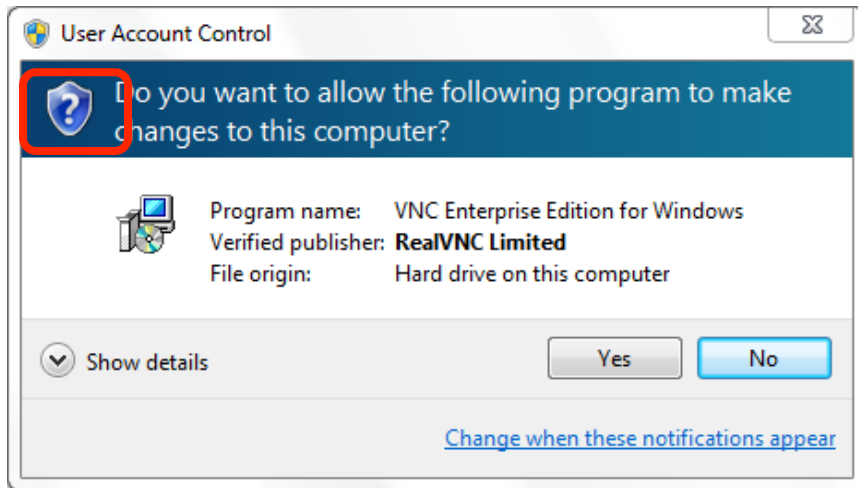




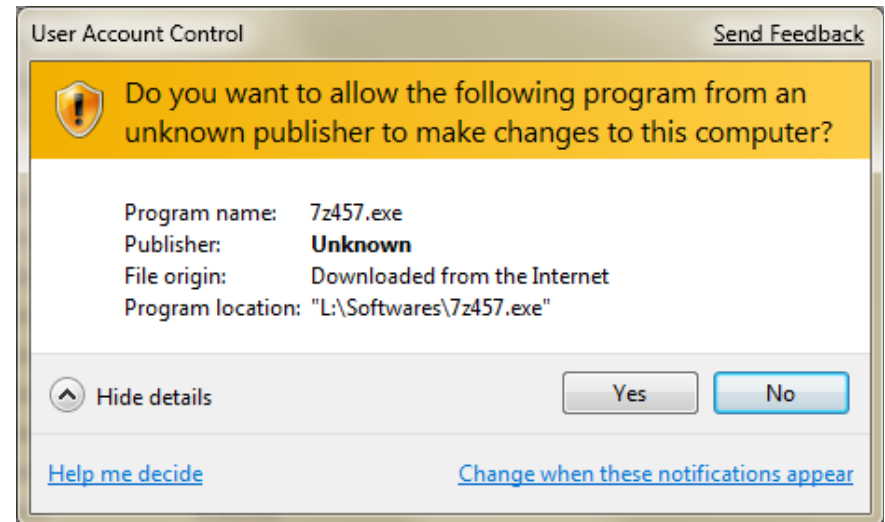
# Windows administrative application



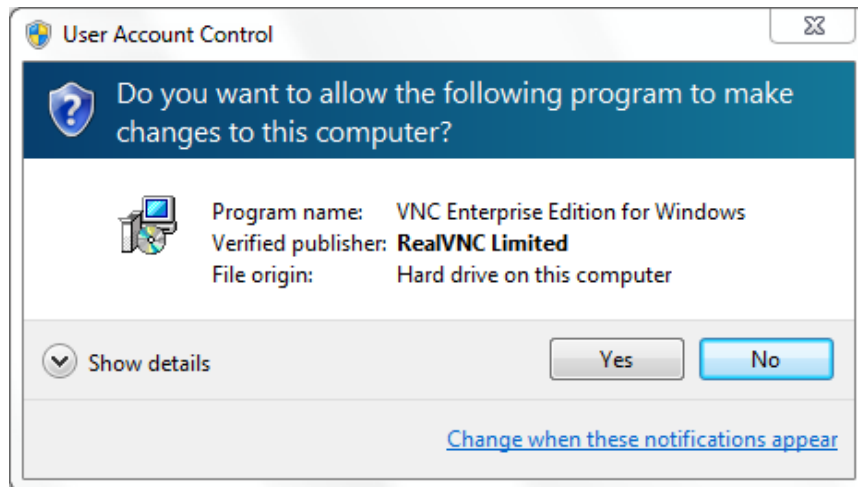
## Signed application



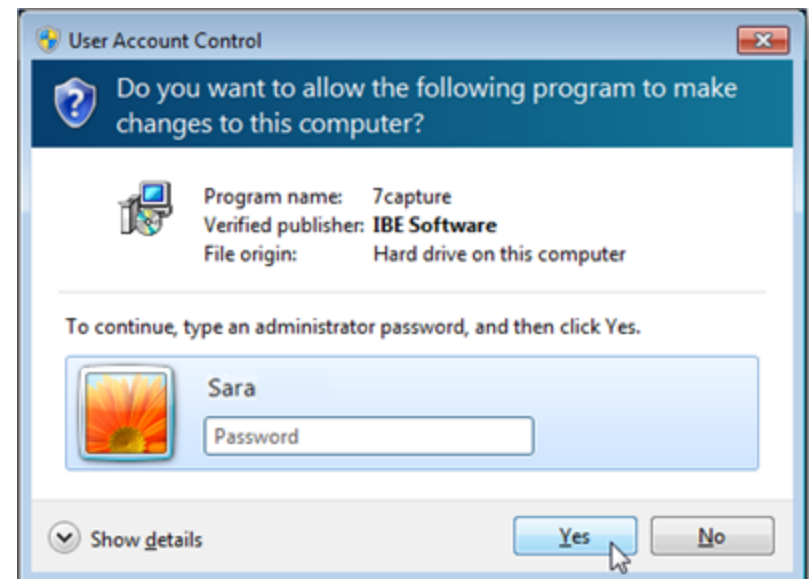
## Unsigned application




## UAC prompt for admin account



## UAC prompt for non-admin account





**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.**



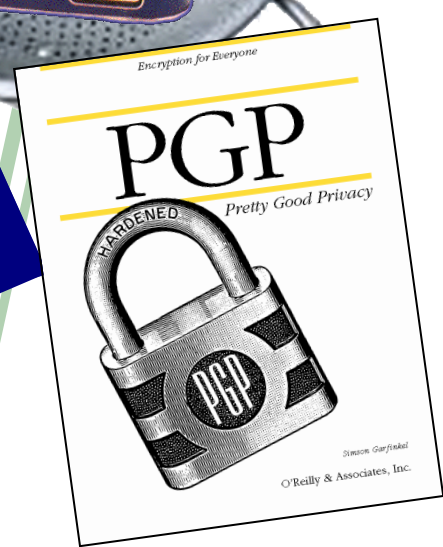
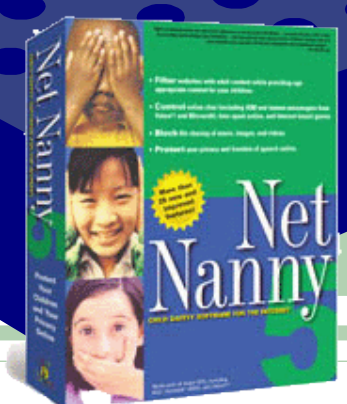
**When participants **initiated** an action that raised UAC prompts, most (95%) consented to these prompts.**

# 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



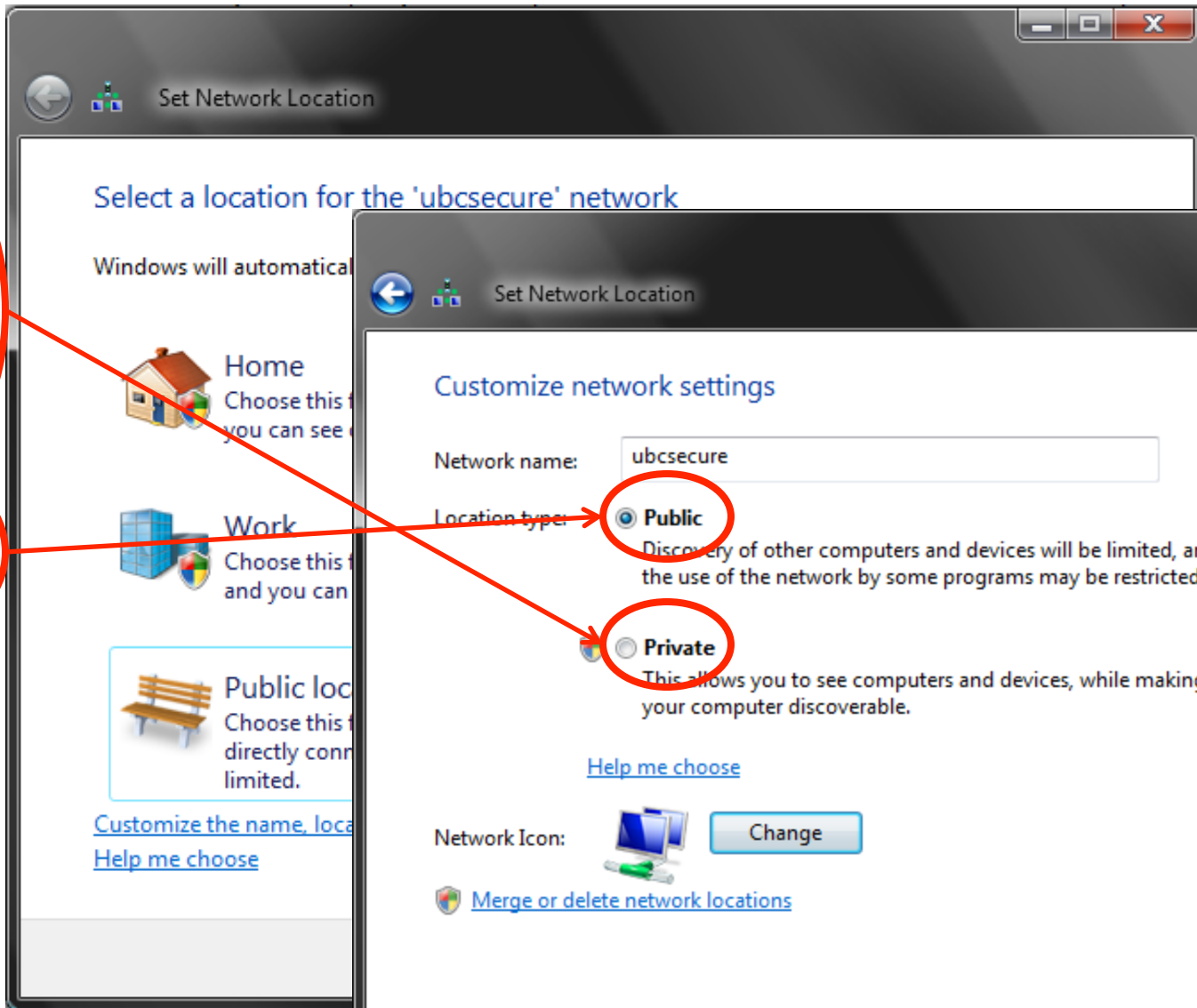
# Invisible Security

- 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)



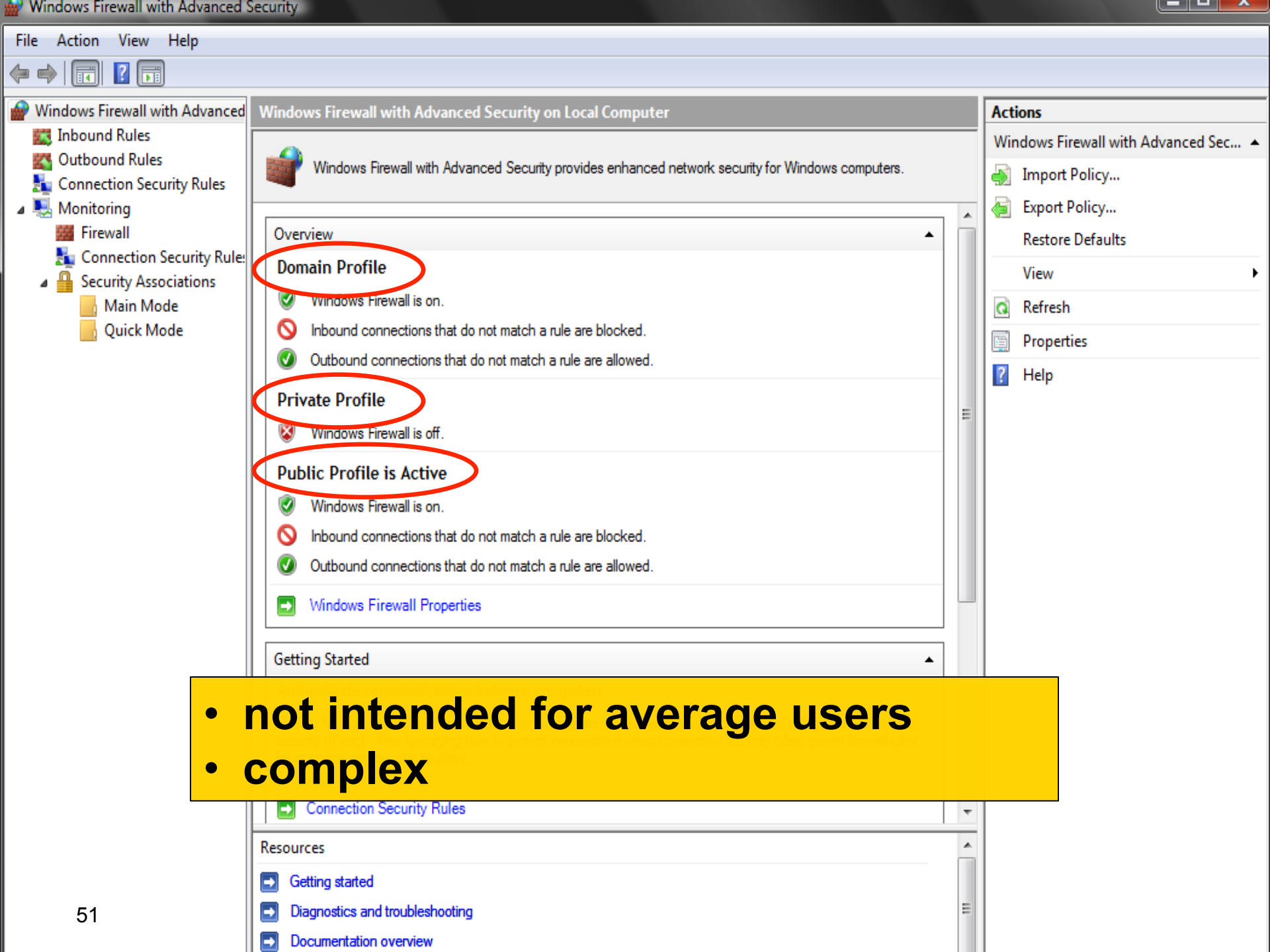


# Network Context in Vista Firewall

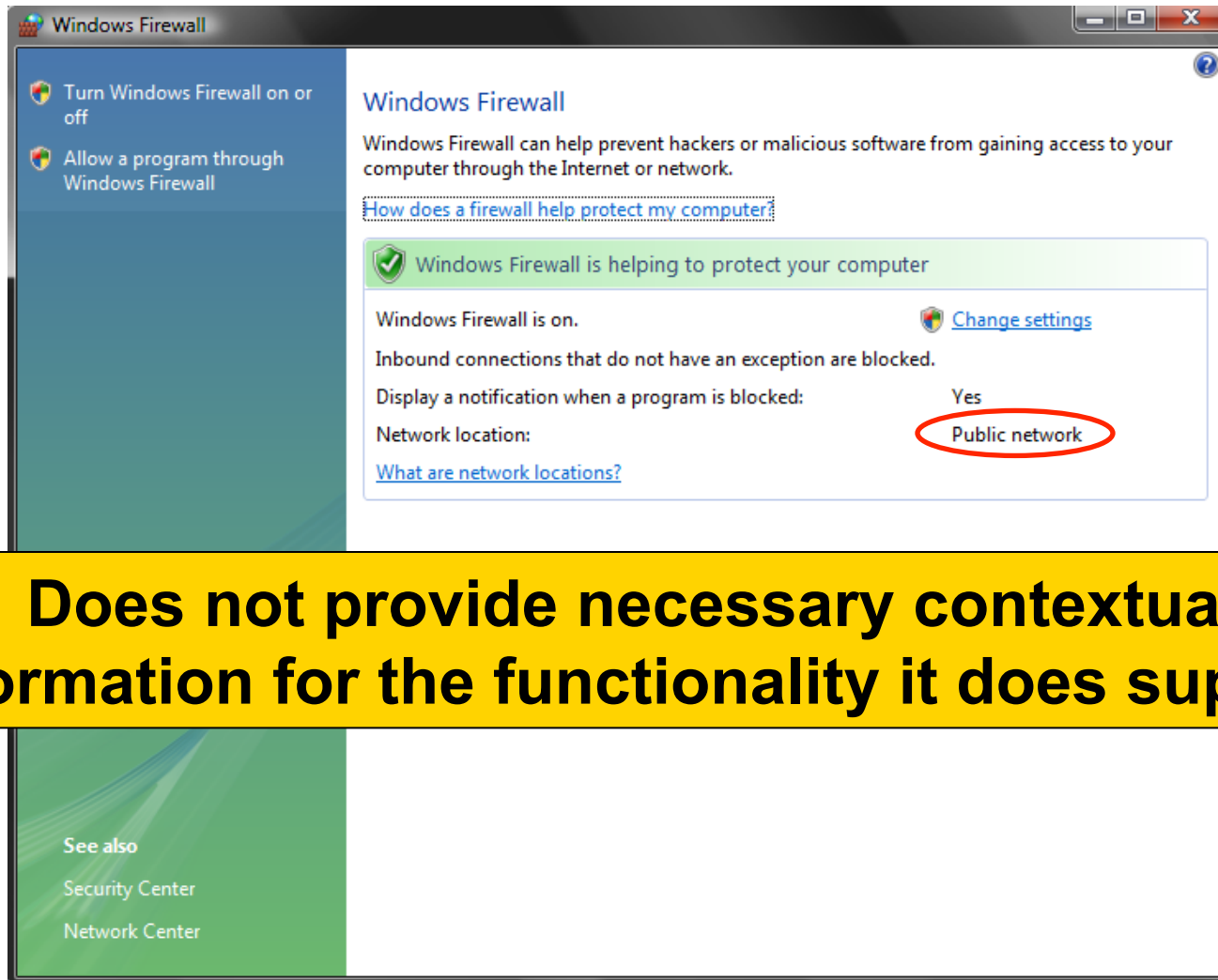
	Public Network Location 	Private Network Location 	Domain Network Location 
Wireless Network Connection 	On	Off	On
Local Area Connection 	On	Off	On
Bluetooth Network Connection 	Off	Off	Off



# **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

The image shows two overlapping windows from Windows Firewall. The background window is the 'Windows Firewall' status window, which displays a red error message: 'Your computer is not protected. Windows Firewall is off.' This message is circled in red. Below it, it says 'Network location:' and provides a link 'What are network locations?'. A yellow warning message below states 'Windows Firewall is not using settings to protect your computer. See recommended settings?'. The foreground window is the 'Windows Firewall Settings' dialog box, with the 'General' tab selected. It shows a green checkmark and the text 'Windows Firewall is helping to protect your computer'. Below this, it explains that Windows Firewall can help prevent hackers or malicious software from gaining access. There are three radio button options: 'On (recommended)' (selected), 'Block all incoming connections', and 'Off (not recommended)'. The 'On (recommended)' option is described as blocking all outside sources except for those unblocked on the Exceptions tab. The 'Block all incoming connections' option is described as being for less secure networks. The 'Off (not recommended)' option is described as making the computer more vulnerable. At the bottom of the dialog box are 'OK', 'Cancel', and 'Apply' buttons. A link 'Tell me more about these settings' is also present.

Windows Firewall

Turn Windows Firewall on or off

Allow a program through Windows Firewall

### Windows Firewall

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

[How does a firewall help protect my computer?](#)

**Windows Firewall is not using the recommended settings**

**Windows Firewall is on.** [Change settings](#)

Inbound connections that do not have an exception are blocked.

Display a notification when a program is blocked:  Yes

Network location: Public network

[What are network locations?](#)

**Windows Firewall is not using the recommended settings to protect your computer. [What are the recommended settings?](#)** [Update settings now](#)

Security Center

Network Center

**Simplified interface:**

- Hidden network context
- Automatic switching of firewall profiles

# 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**



Turn Windows Firewall on or off

Allow a program through Windows Firewall

### 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?

#### Windows Firewall network locations

[Change settings for...](#)

#### Public Network

Windows Firewall is on for B...

Inbound connections that d...

[Change Settings for...](#)

#### Private Network

Windows Firewall is on for V... connections.

Inbound connections that d...

[Change Settings for P...](#)

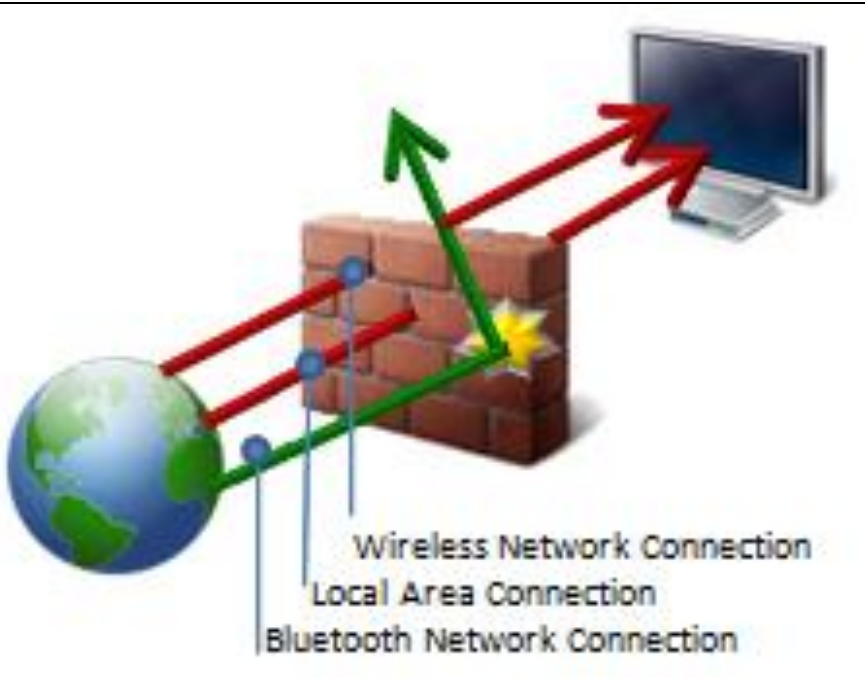
#### Domain Network

Windows Firewall is on for a...

Inbound connections that d...

[Change Settings for D...](#)

[What are network locations](#)



Bluetooth Connection	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off	<input type="checkbox"/> On <input checked="" type="checkbox"/> Off	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
----------------------	--	--	--

[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

See also

Security Center

Network Center



# 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

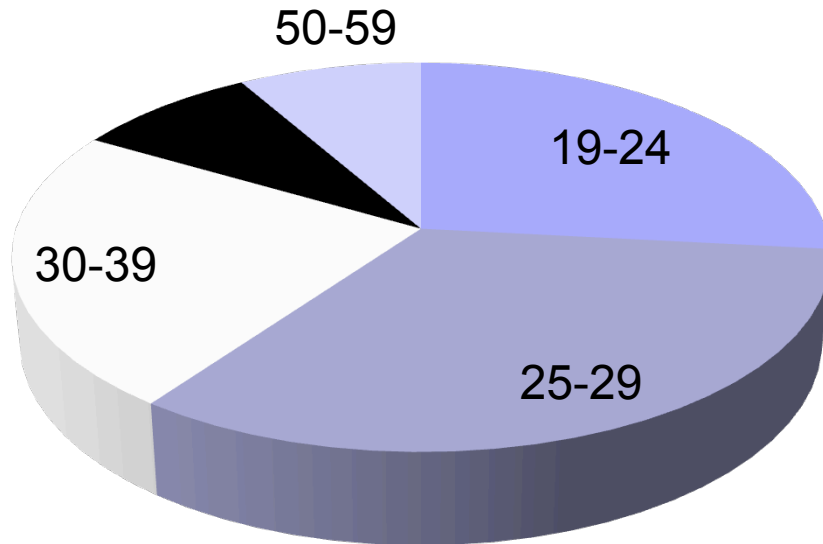


**30**

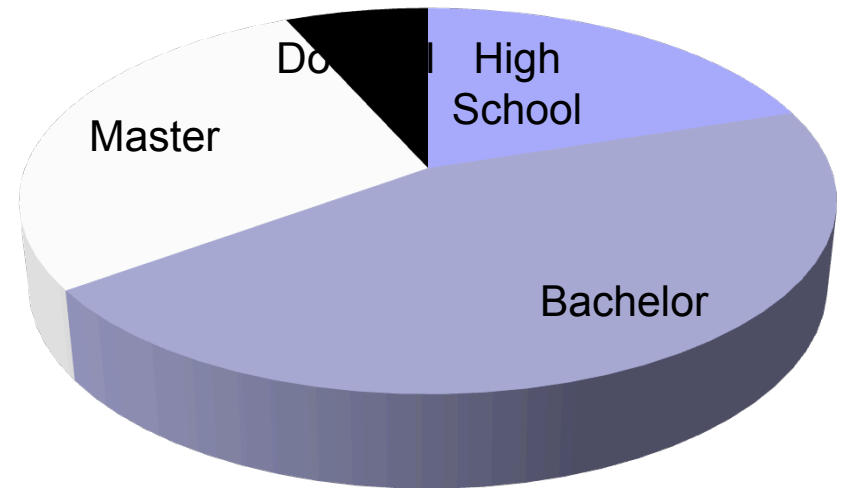


**30**

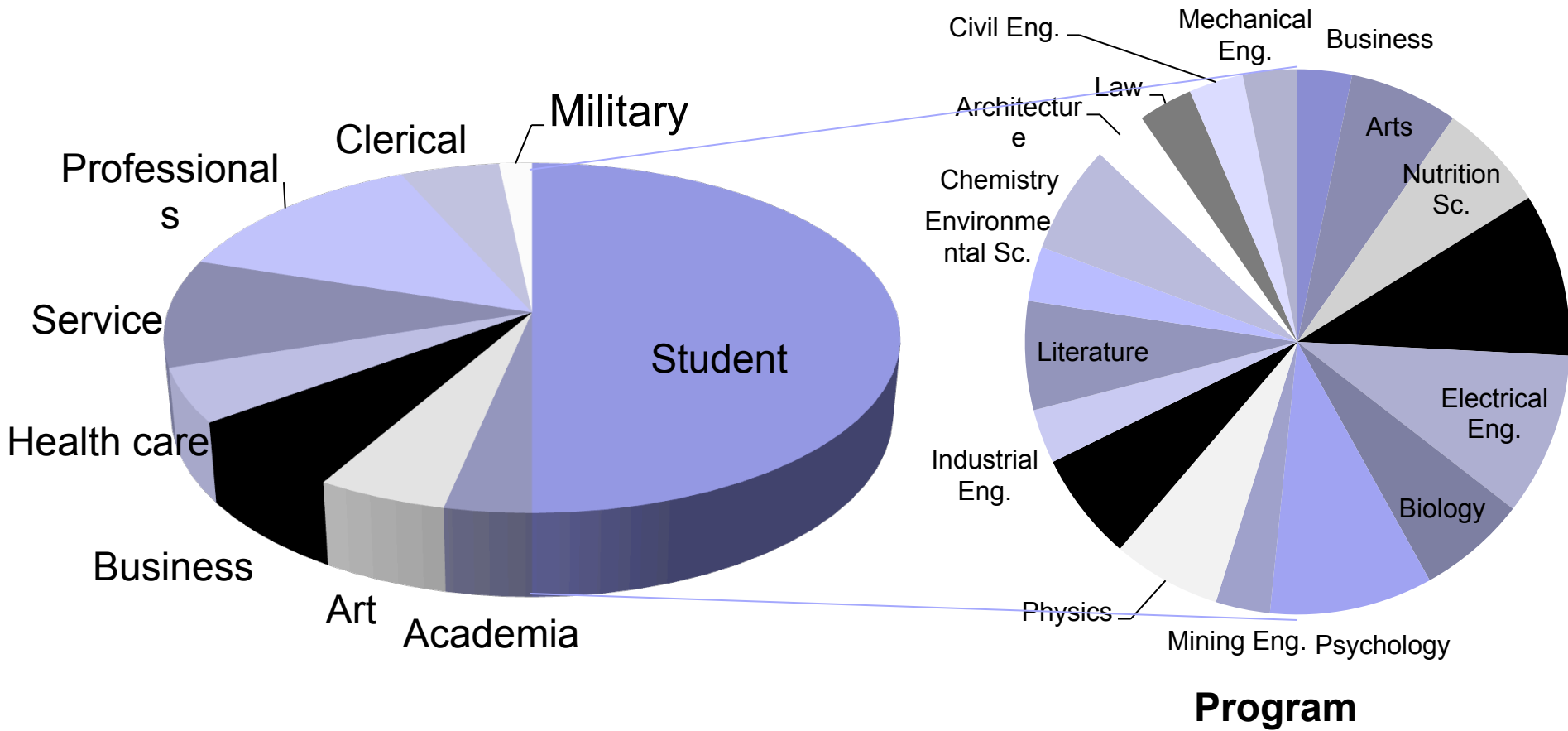
## Age



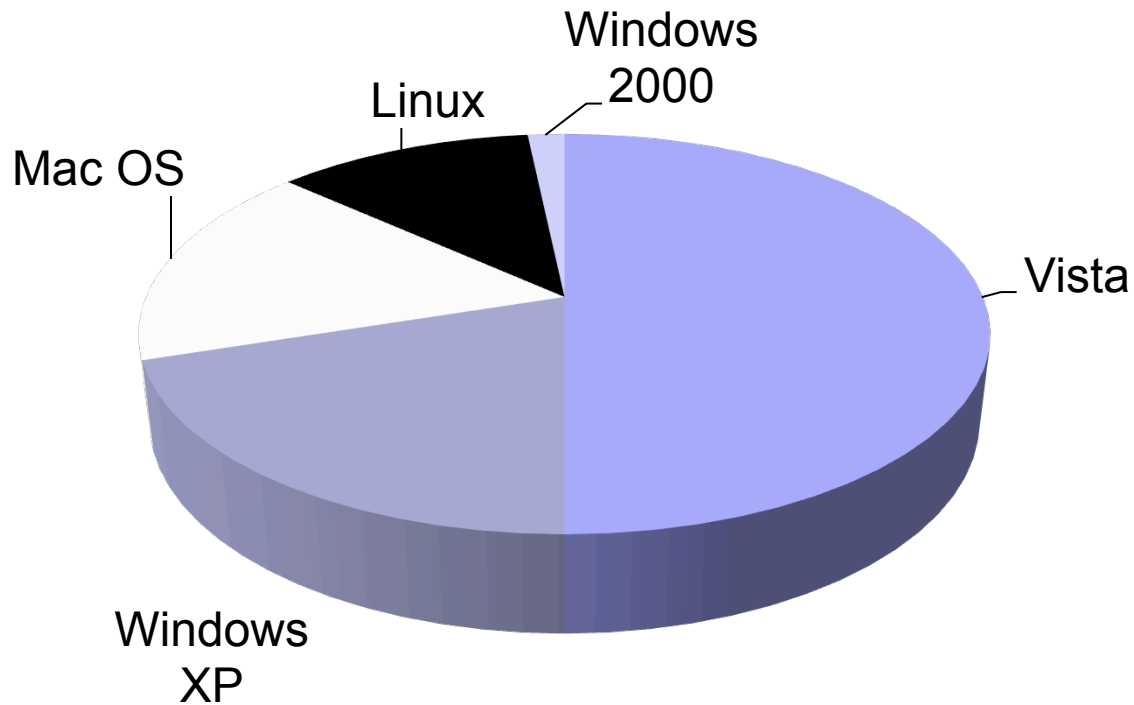
## Completed Education



# Occupation

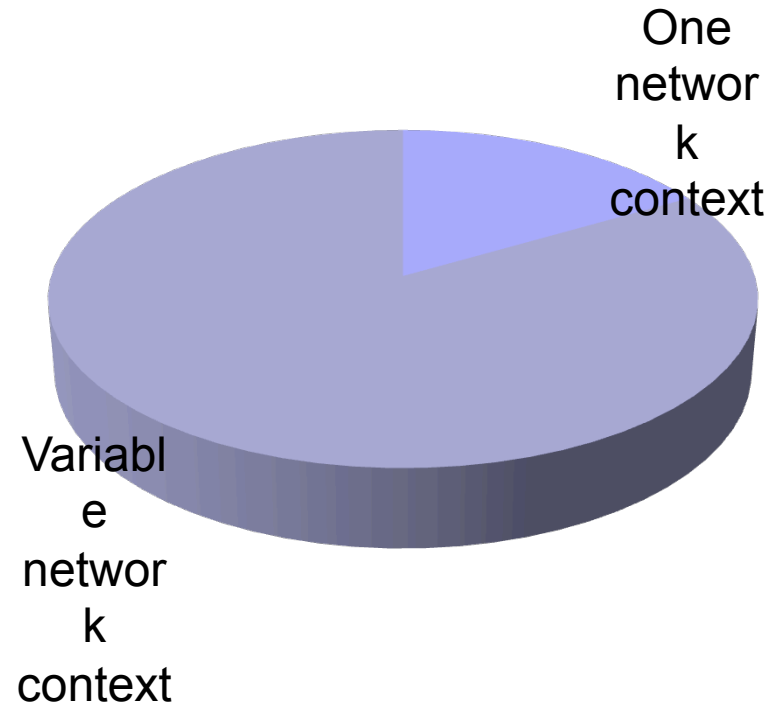
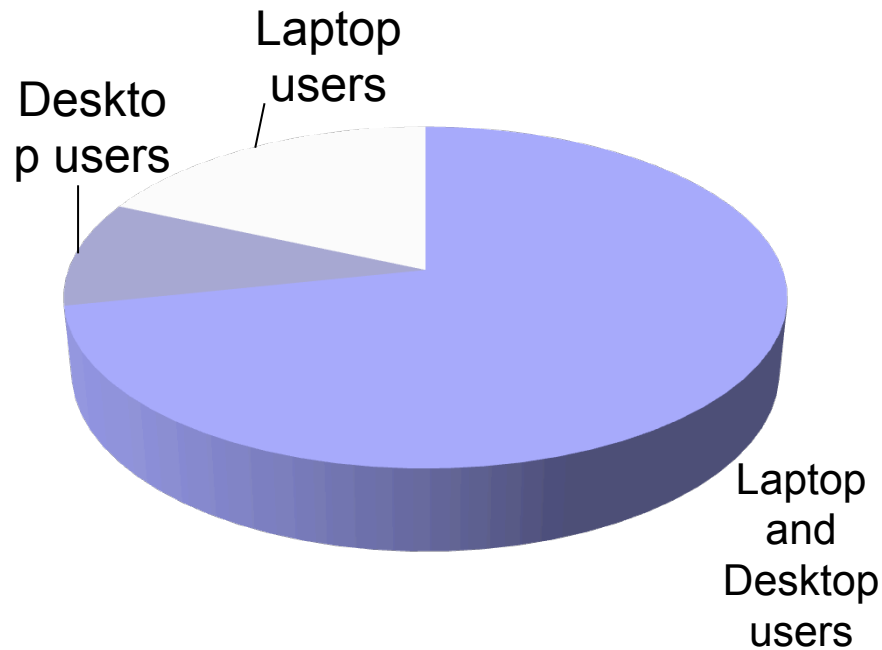


# All Daily Computer Users





# Context of Use



# Study Protocol

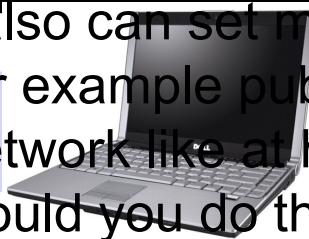
## Introduction to the Context



As you know we can use different network connections to connect to the Internet, like wireless or a cable. For this

### Tasks on the 1<sup>st</sup> Interface

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?



	Public Network Location	Private Network Location	Domain Network Location
Wireless Network Connection			
Local Area Connection			
Bluetooth Network Connection			



# Results

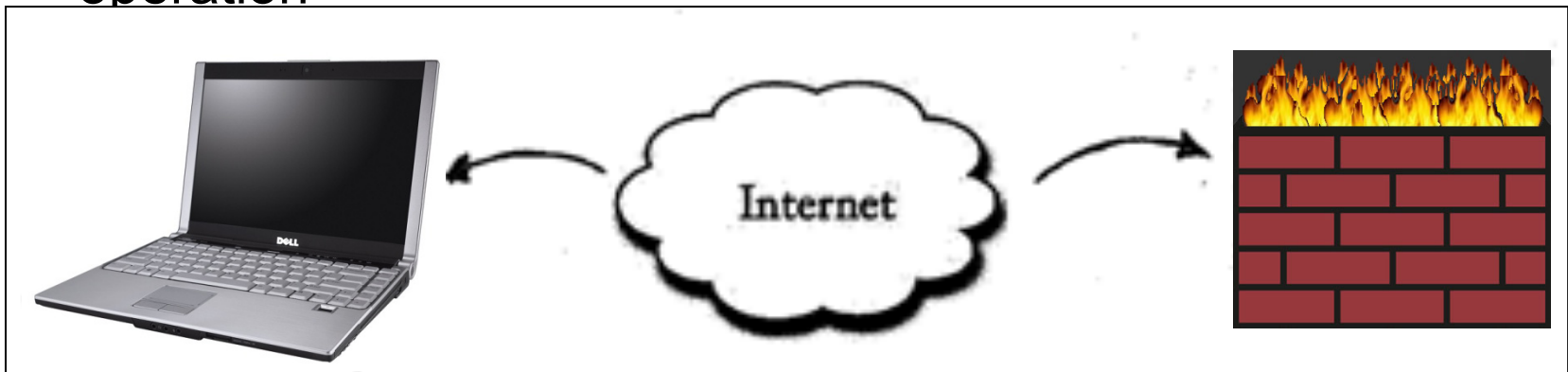


# Mental Models

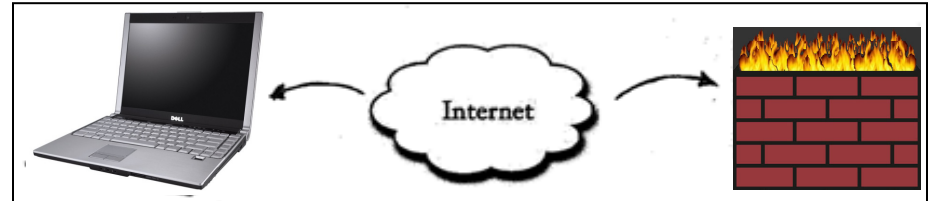
- Incorrect
- Incomplete
- Partially complete
- Complete

# Mental Models

- **Incorrect:** incorrect basic understanding of firewall operation

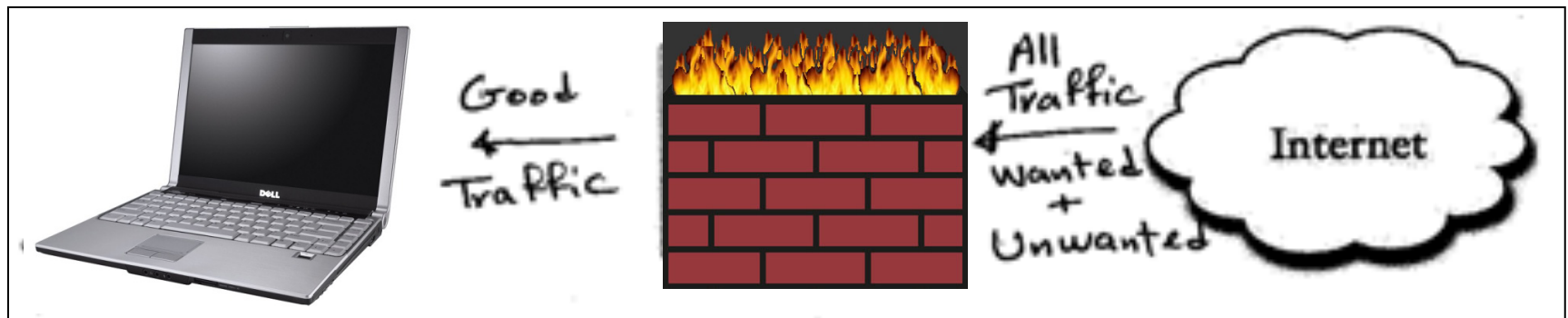


# Mental Models



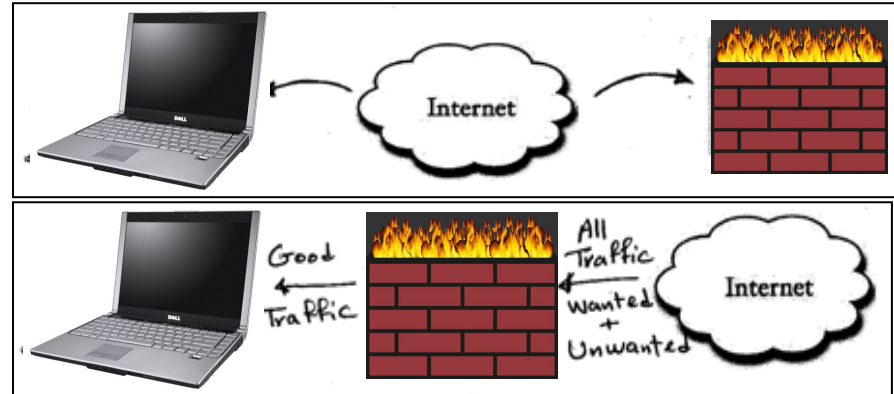
## ■ Incorrect

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

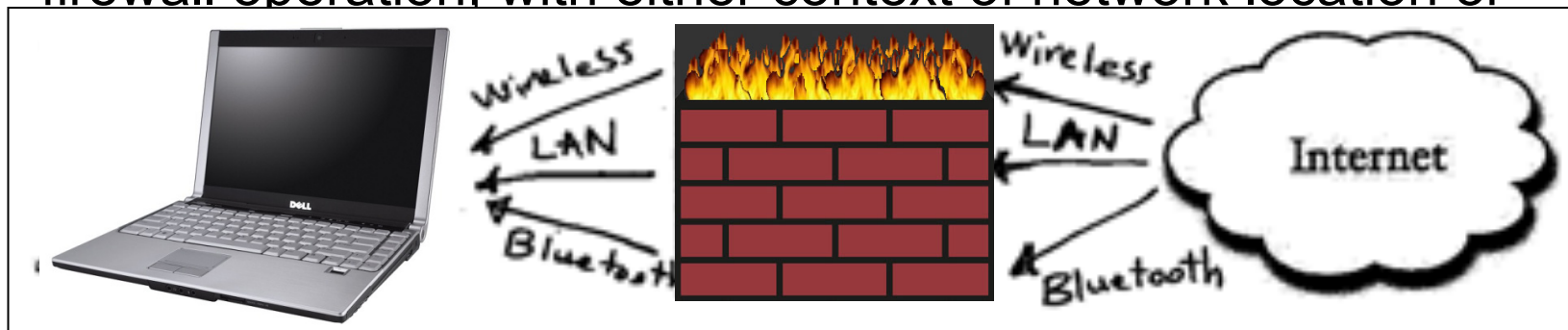


# Mental Models

- Incorrect
- Incomplete

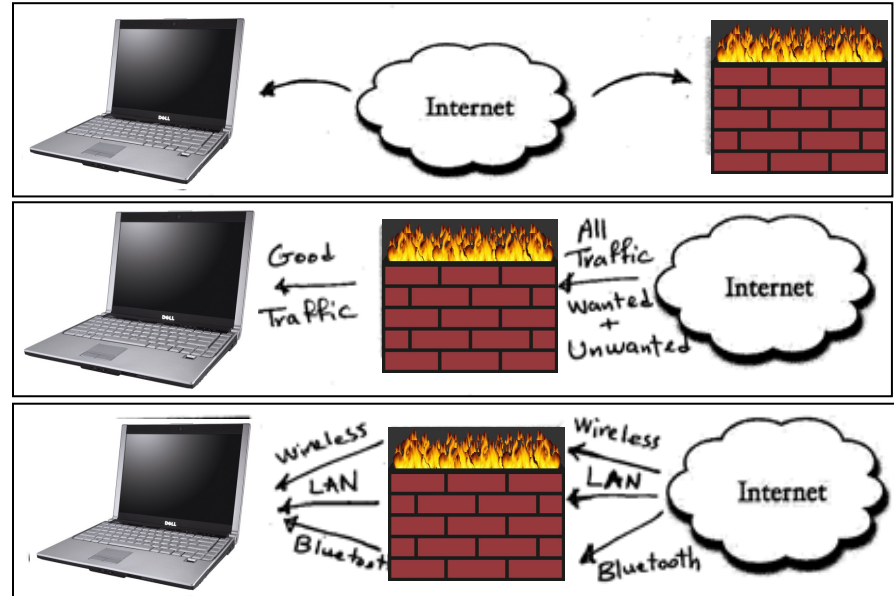


- **Partially complete:** correct basic understanding of firewall operation, with either context of network location or

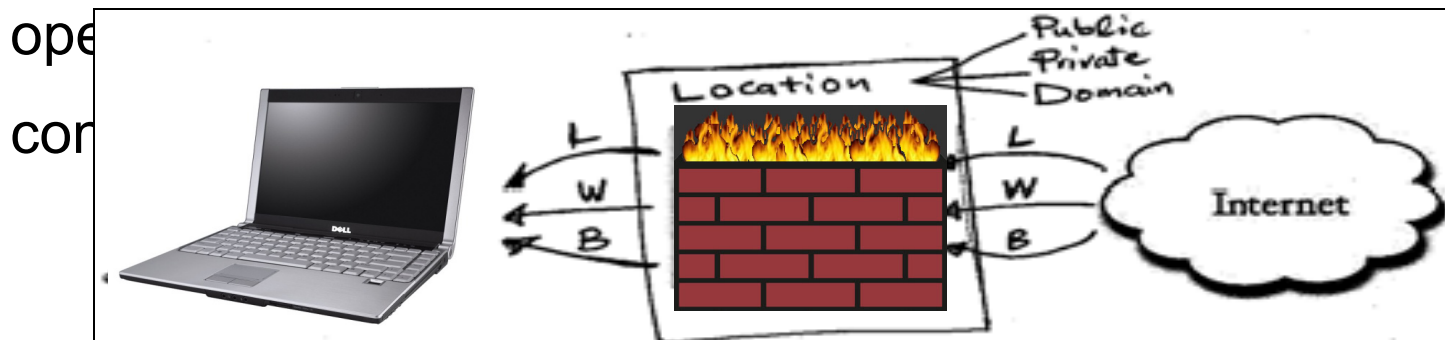


# Mental Models

- Incorrect
- Incomplete
- Partially complete

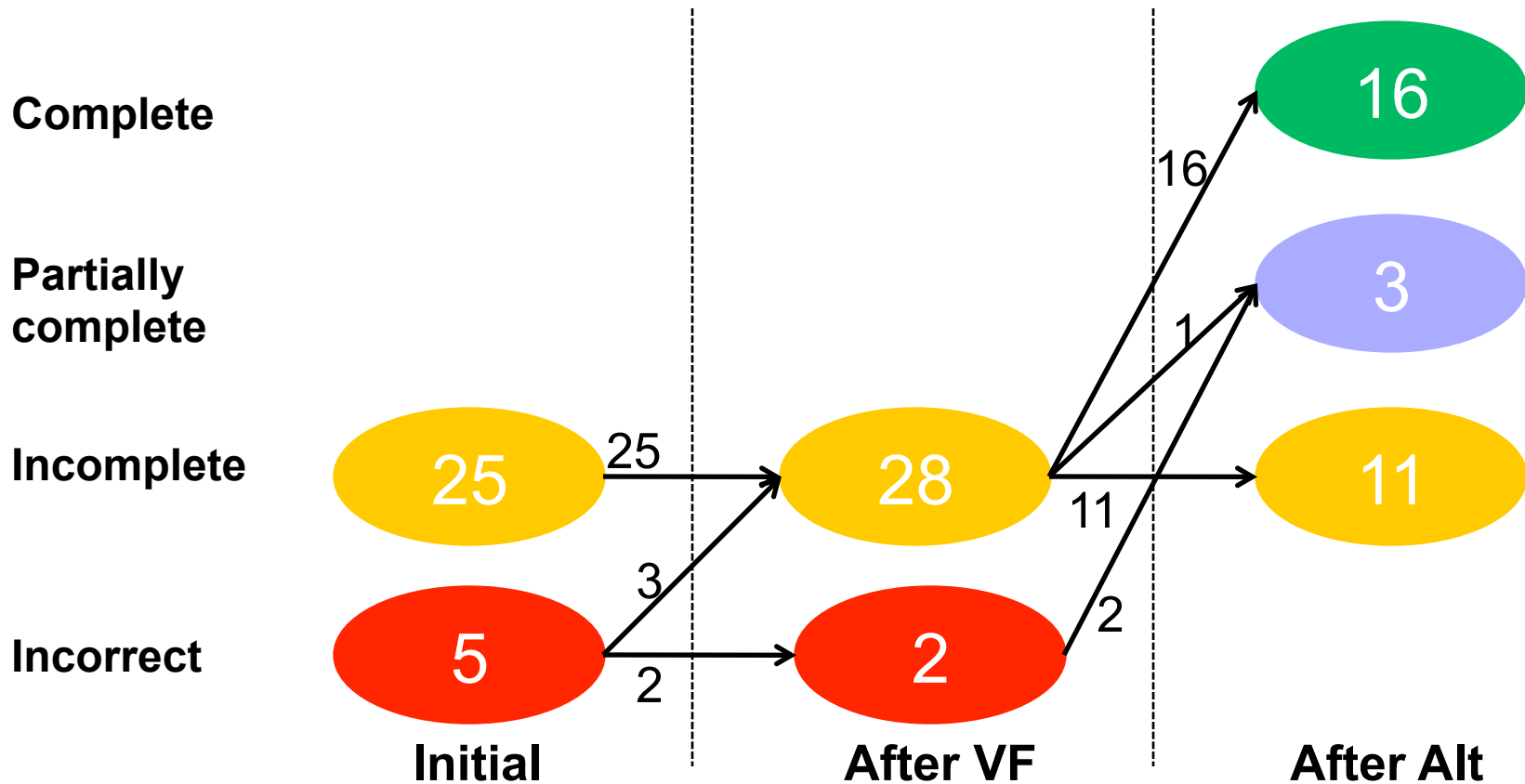


- **Complete:** correct basic understanding of firewall

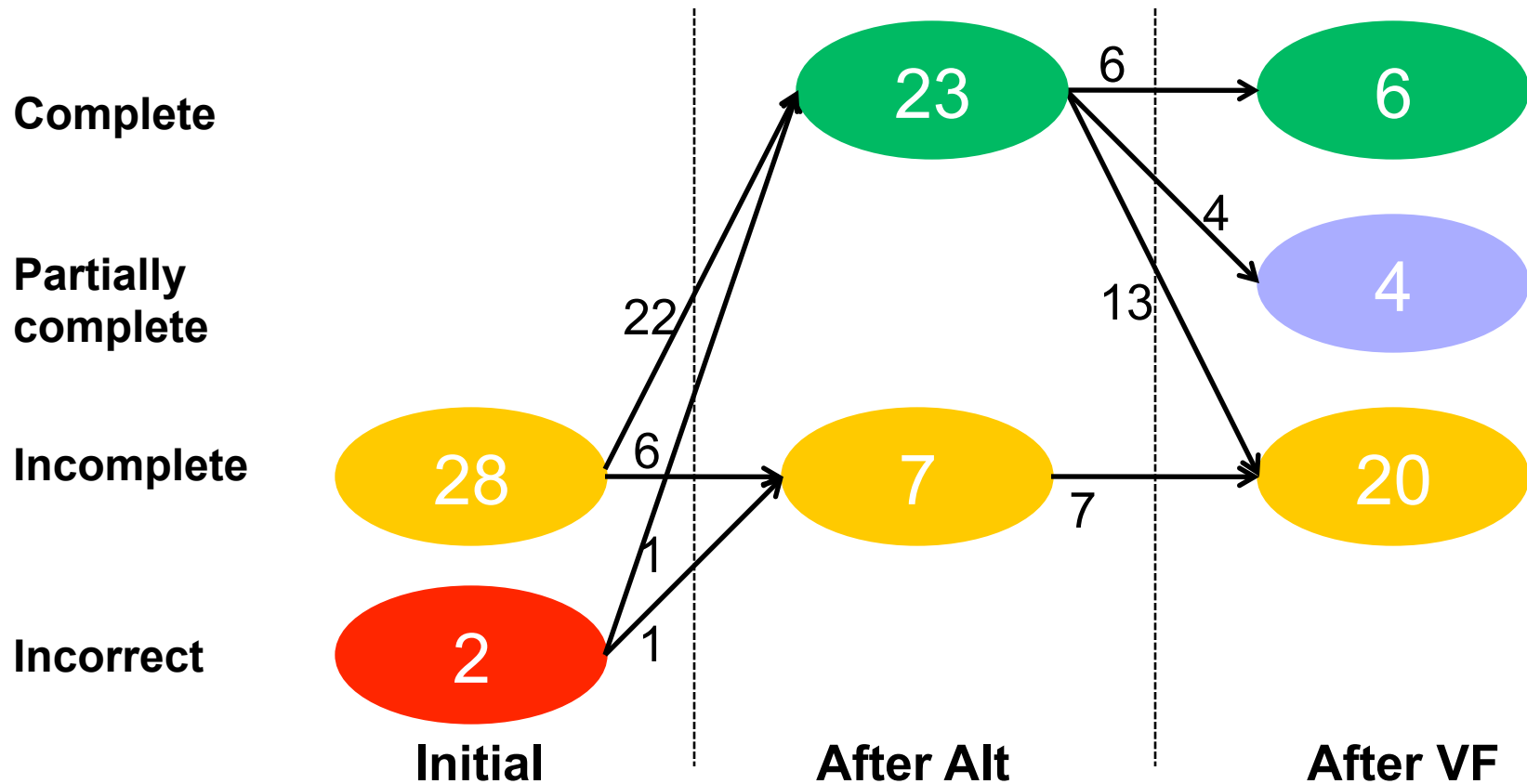




# First Vista Firewall Basic, then Alternative



# First Alternative, then Vista Firewall Basic

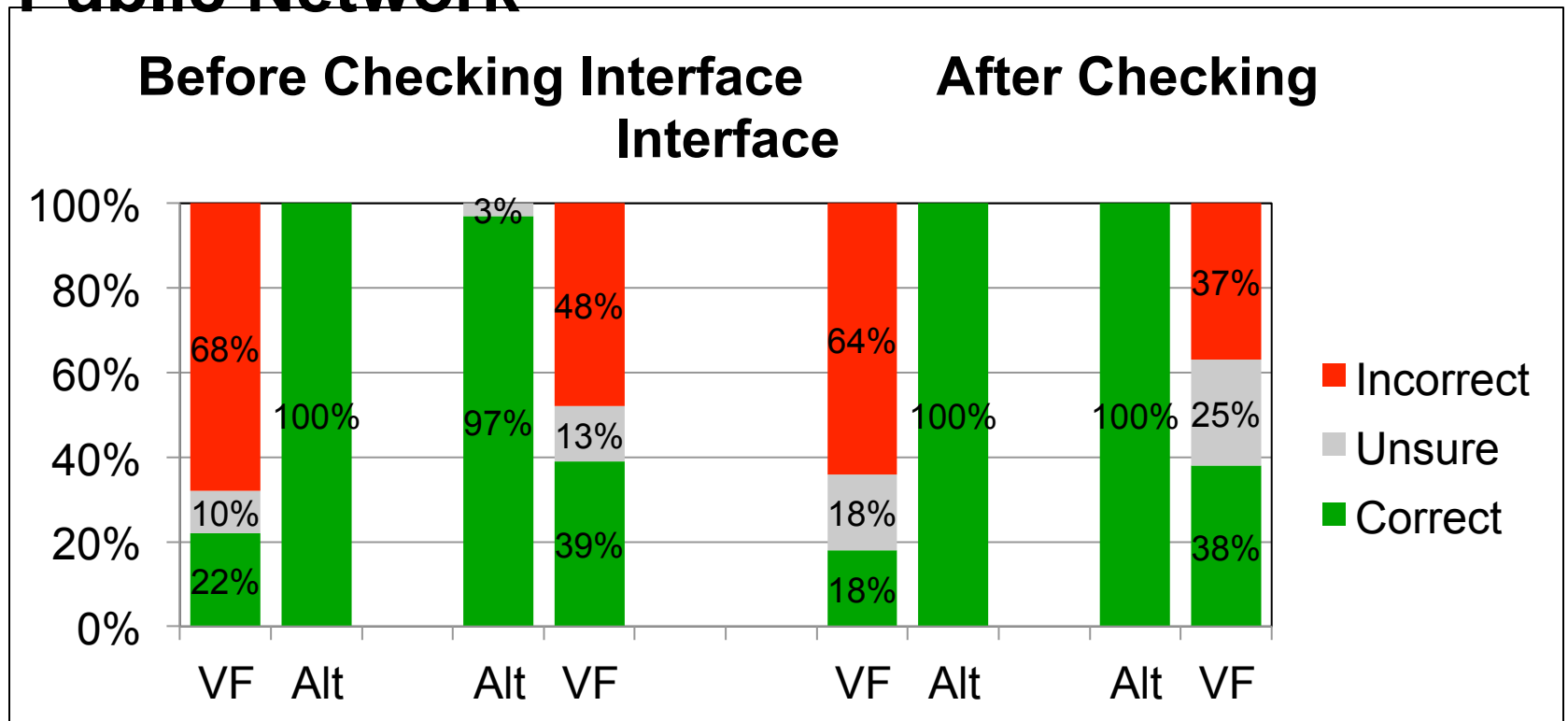


# Understanding Firewall

	Public Network Location	Private Network Location	Domain Network Location
Wireless Network Connection	On ✗	On ✗	Unsure
Local Area Connection	On ✗	Off	Unsure
Bluetooth Network Connection	On ✓	Unsure	Unsure

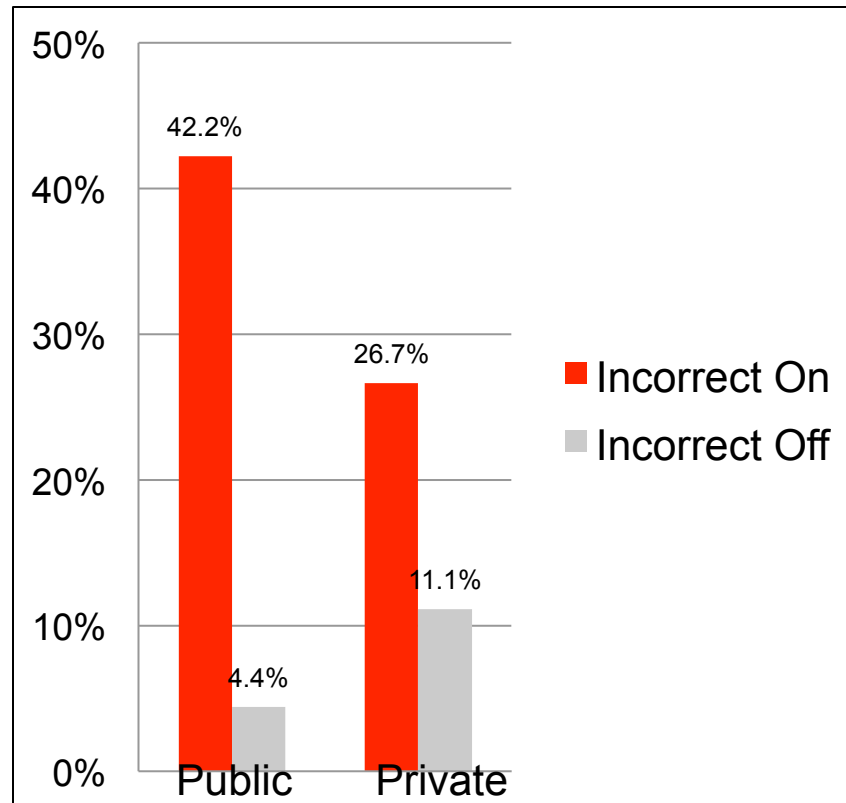
# Understanding Firewall Configuration

## Public Network



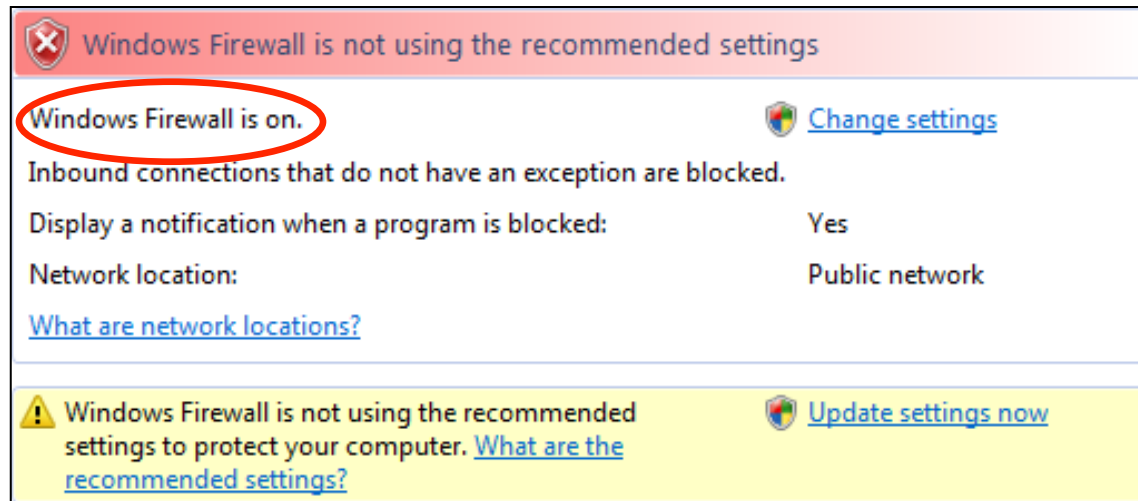
Vista-basic: large % of incorrect  
 Alternative interface: Understood config.

# 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.”*

# Feedback on Alternative Interface

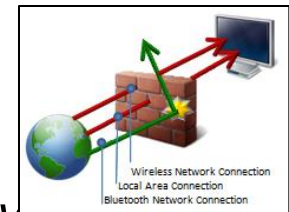
- 56 (93%) participants liked images, fine-grained control  
*“The second interface is much better. The pictures are very instructive. I have more control on it and that is nice.”*

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



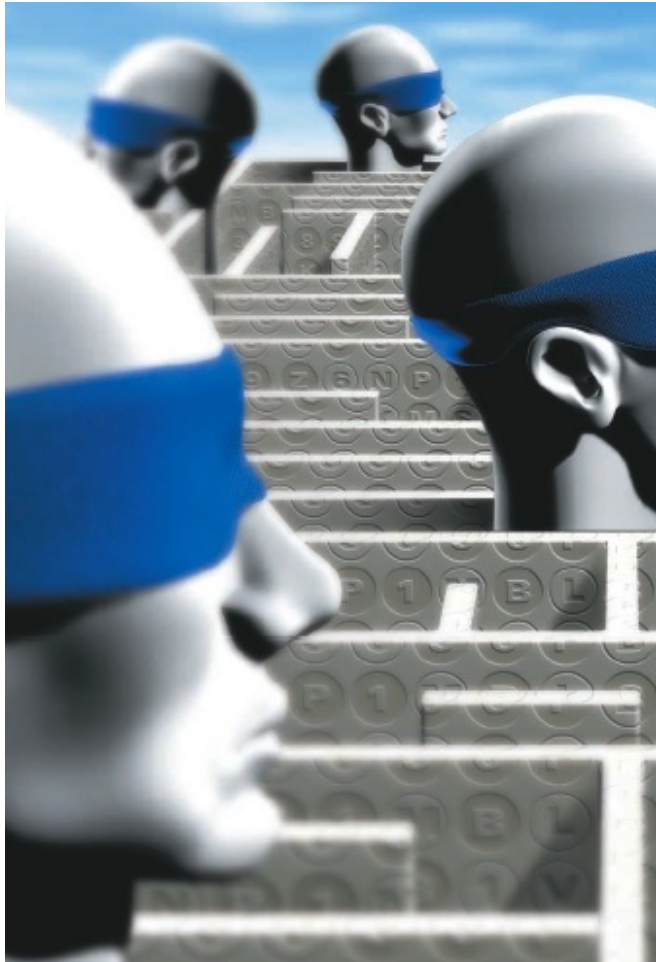
# Privacy Bird Icons



**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

## 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/

MDS 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 site's security certificate is not trusted!

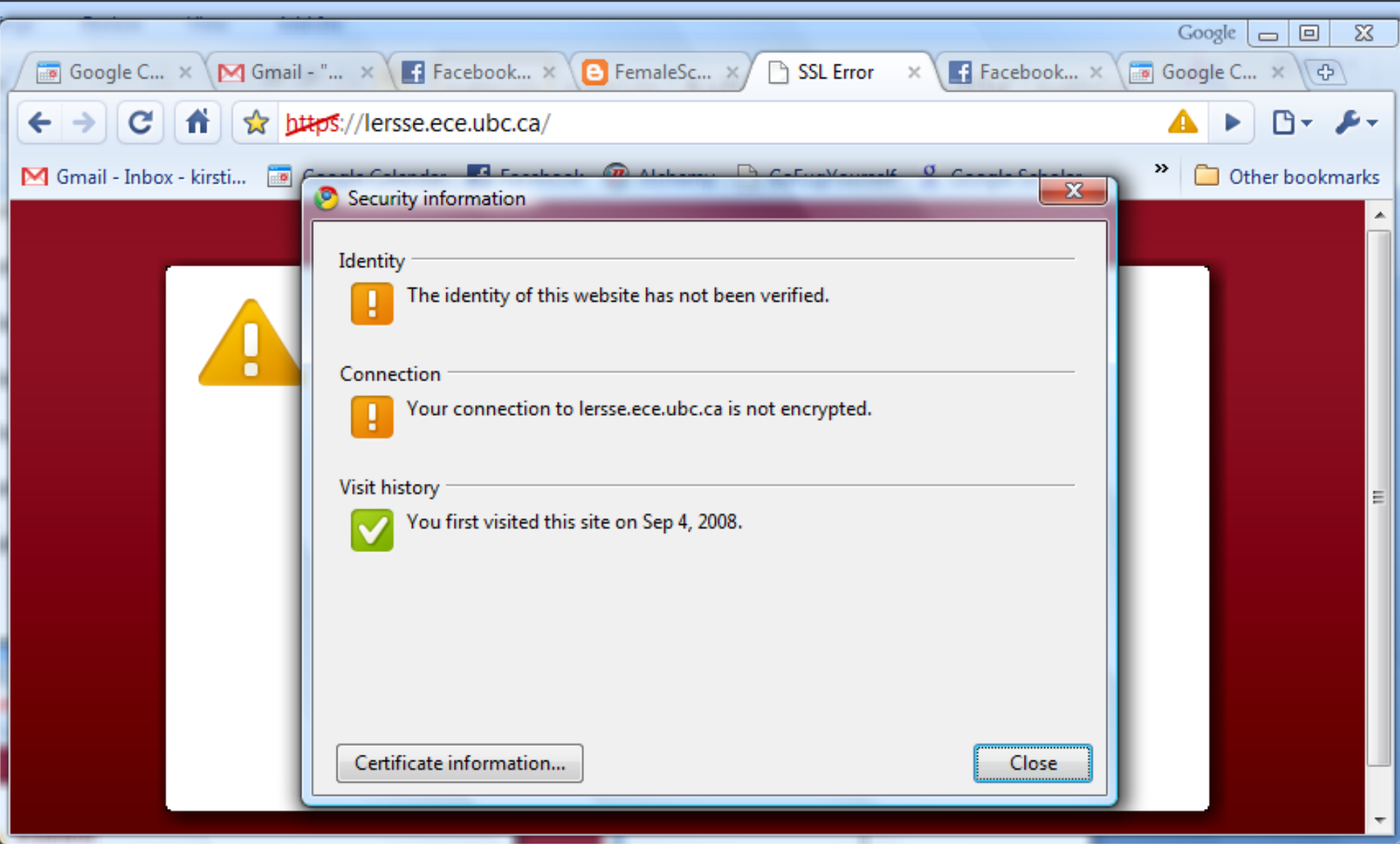
You attempted to reach **lersse.ece.ubc.ca**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Google Chrome cannot rely on for identity information, or an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

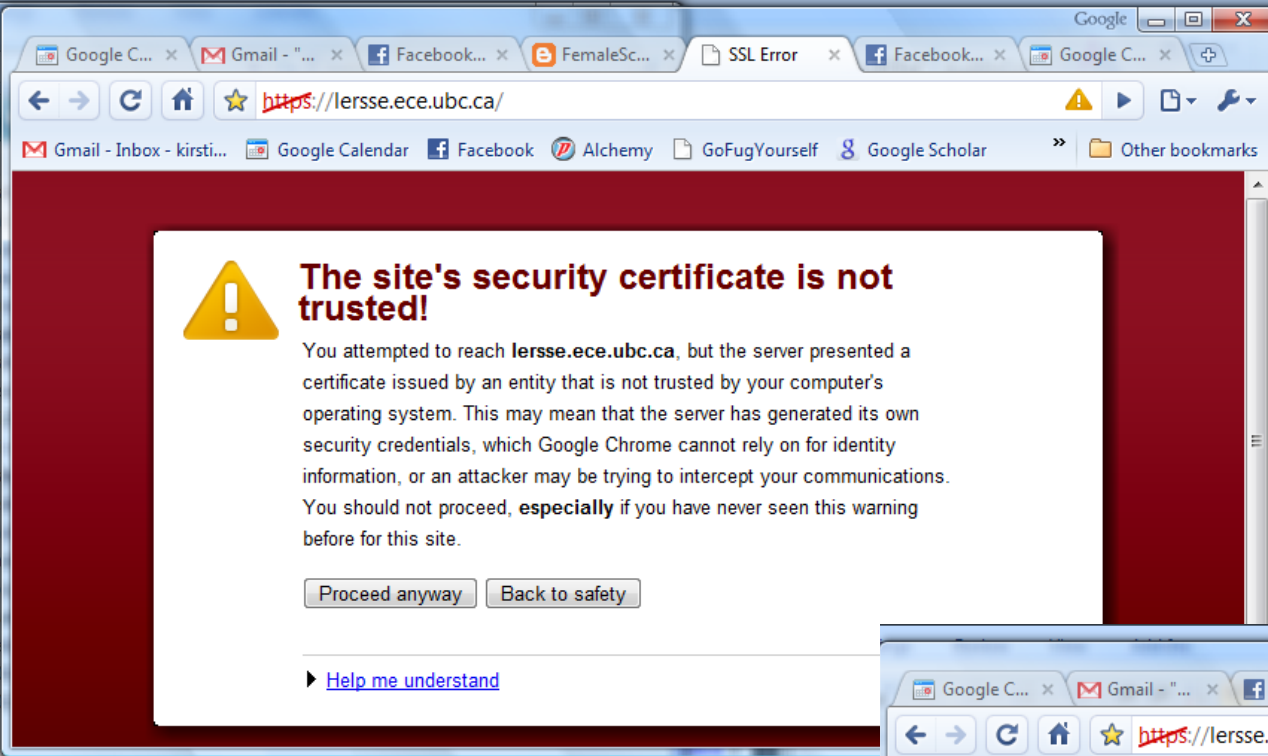
[Proceed anyway](#)

[Back to safety](#)

---

▶ [Help me understand](#)

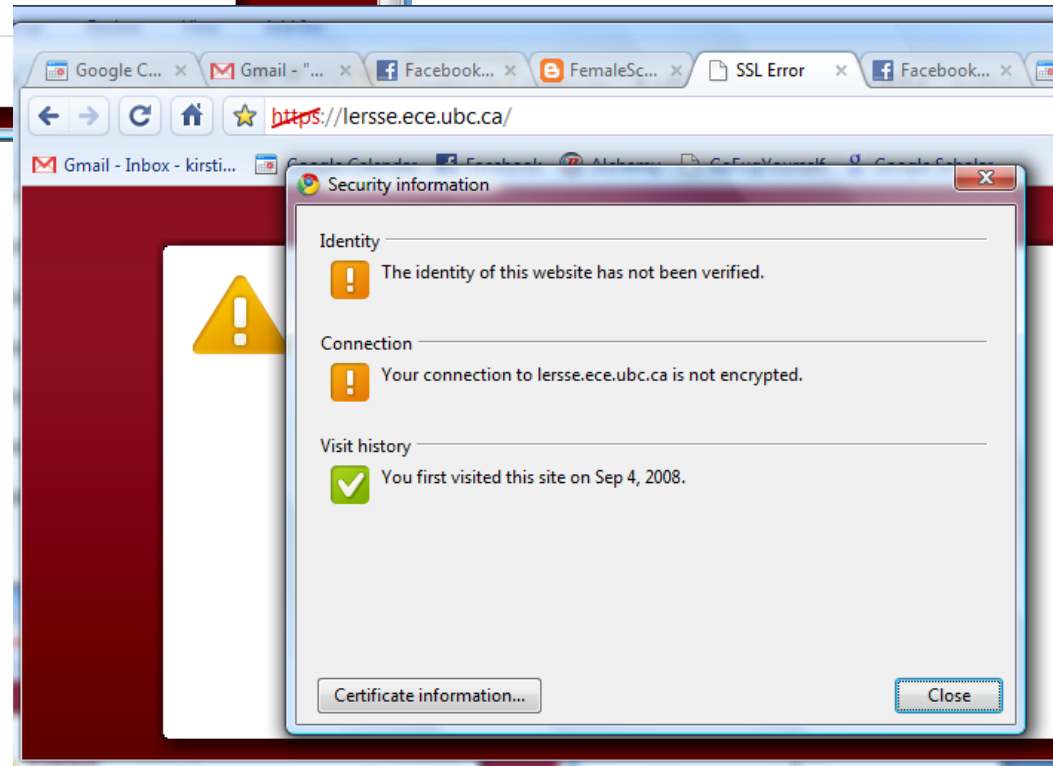




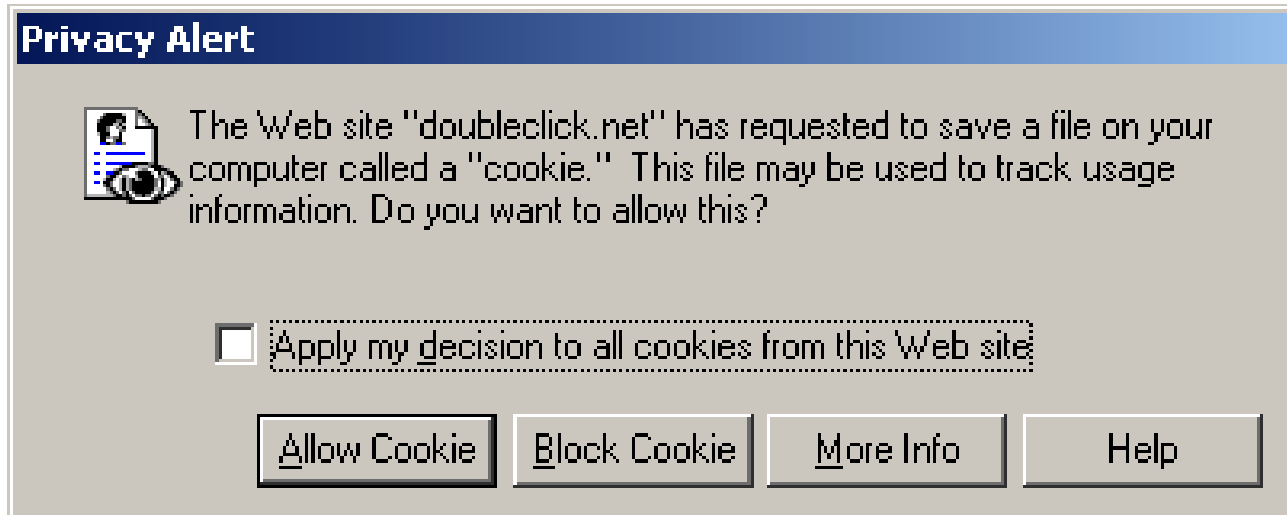
# Evaluate the usability of the warning and security cues.

## Reminder:

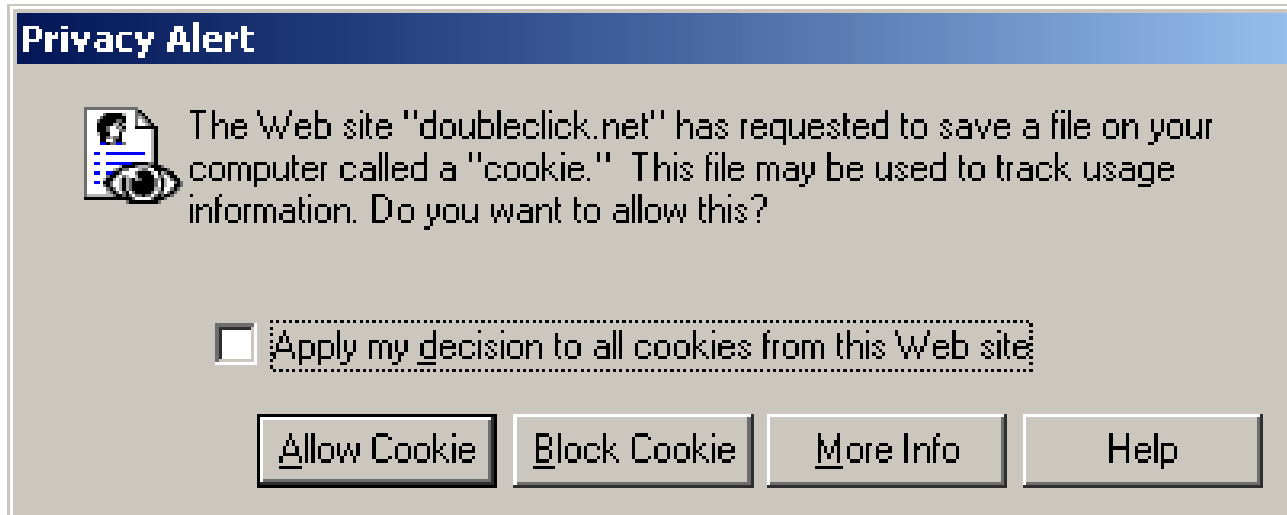
- Why is it there?
- Do users notice it?
- Do they know what it means?
- Do they know what they are supposed to do when they see it?
- Will they actually do it?
- Will they keep doing it?



# Making concepts understandable

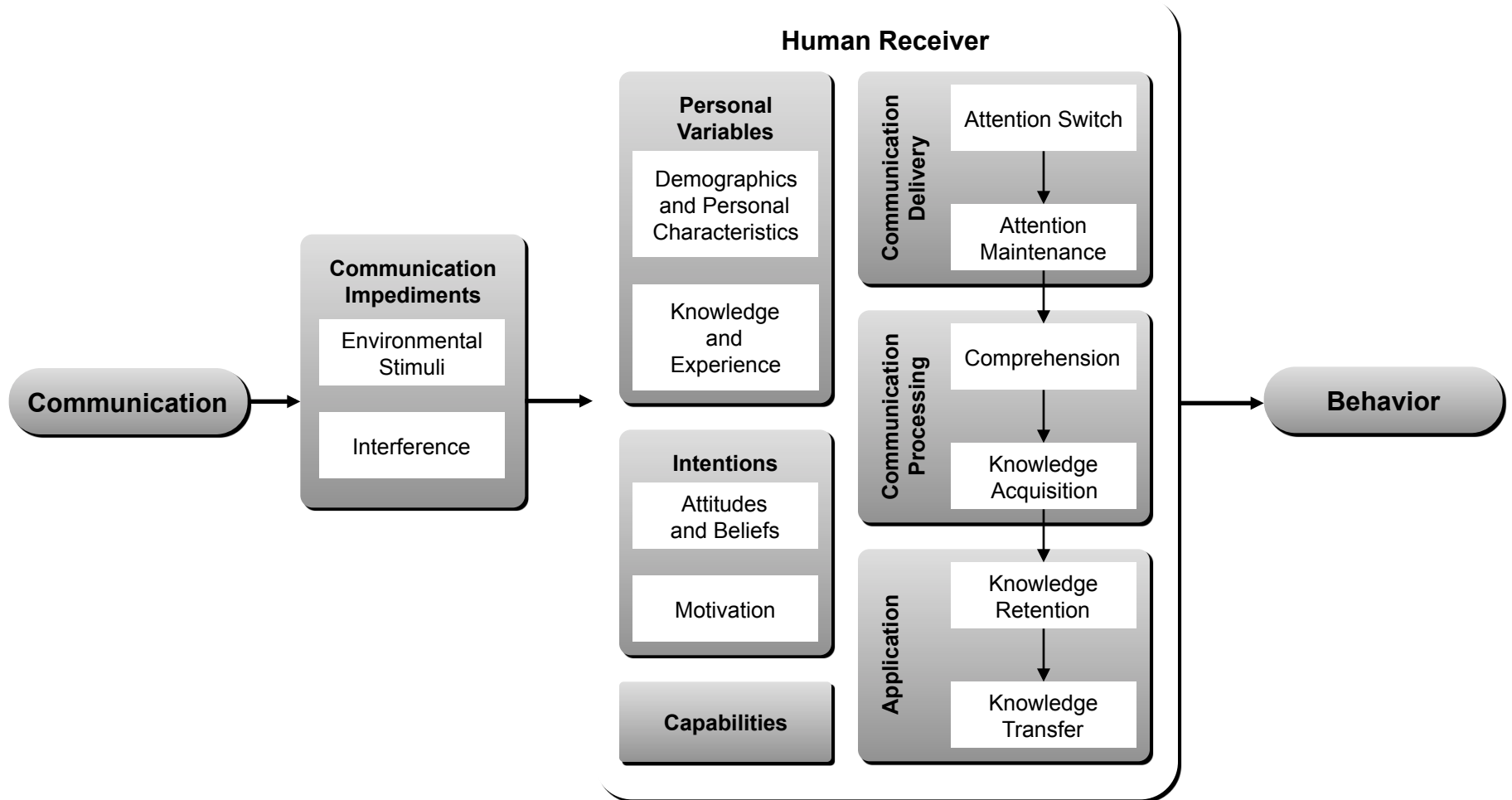


# Making concepts understandable



- 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

I HAVE A  
NEW HOBBY.  
IT'S CALLED  
PHISHING.



www.dilbert.com scottadams@aol.com

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



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

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.

# A Recent Email...



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.



# 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.](#)

#### Personal ID

#### Password

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

#### Select Your Destination

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



Member FDIC

# The next page requests:

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



## Internet Banking

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



Member FDIC

# But wait...

U.S. Bank Internet Banking - Microsoft Internet Explorer

File Edit View Favorites Tools Help

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...



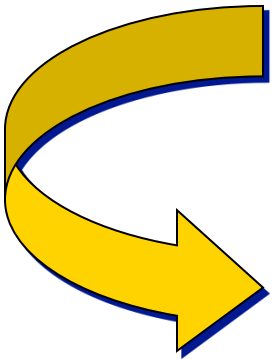
# Why is Phishing Successful?

- 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

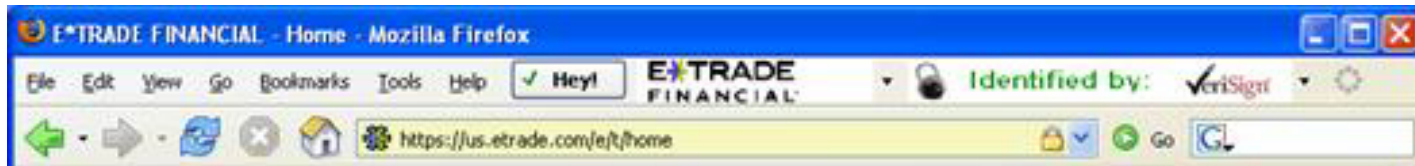
- Educate Users
- Good user interface design (usability guidelines)
- Help users make good decisions rather than presenting dilemmas



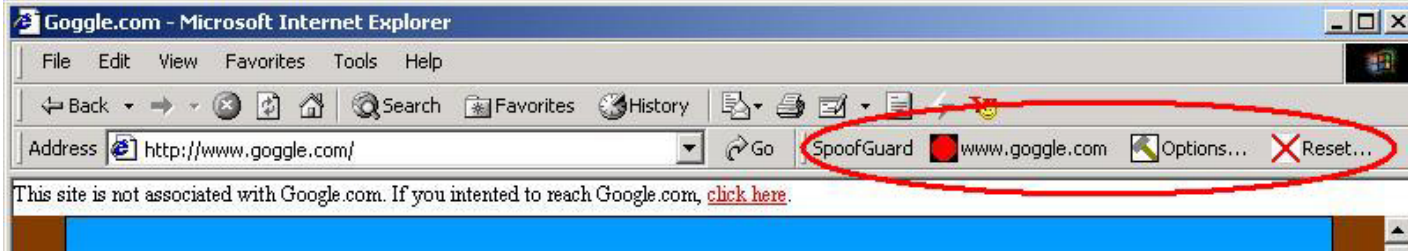
# Phishing Education

- Anti-Fishing Phil
- [http://cups.cs.cmu.edu/antiphishing\\_phil/](http://cups.cs.cmu.edu/antiphishing_phil/)

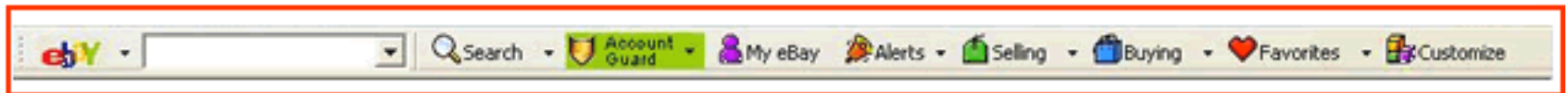
# Other Solutions: Toolbars



Trustbar

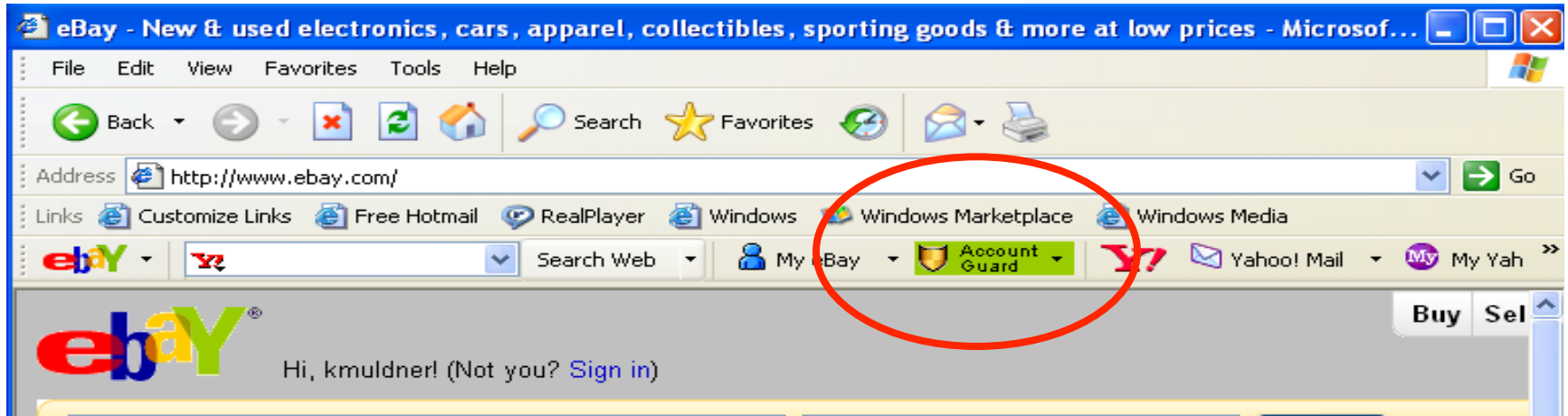


spooftguard

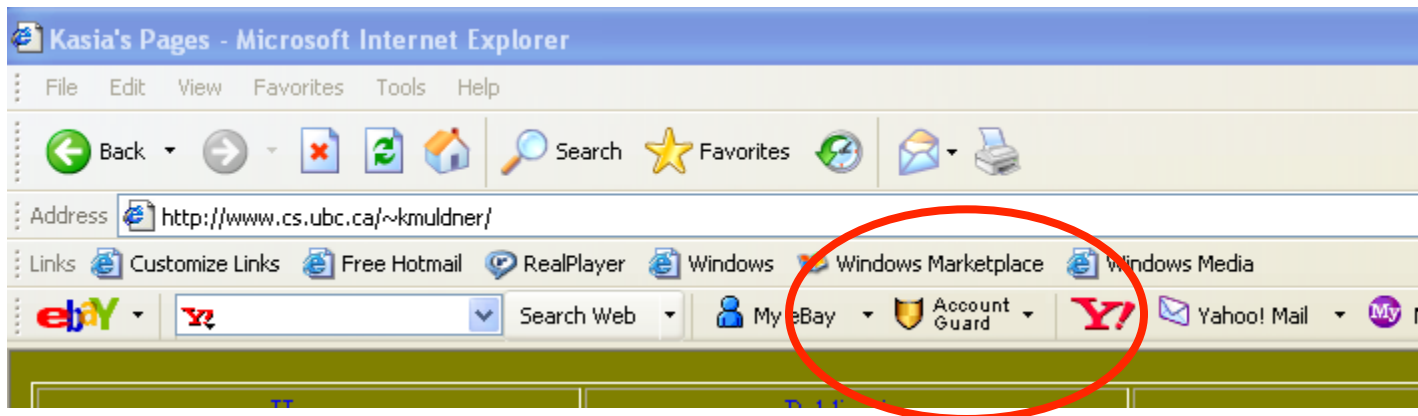


Accountguard

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



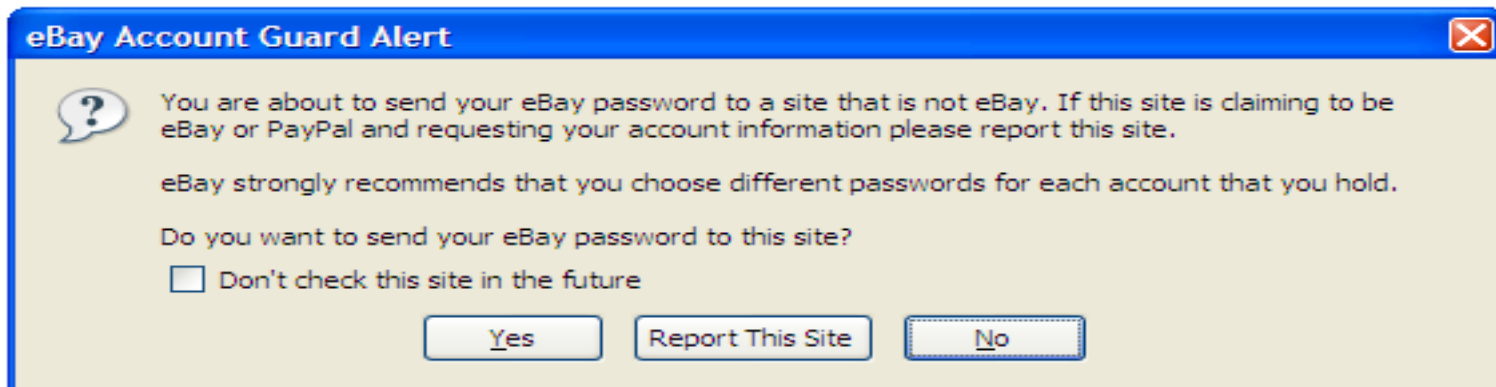
2) If you are on a non eBay or PayPal web site.



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



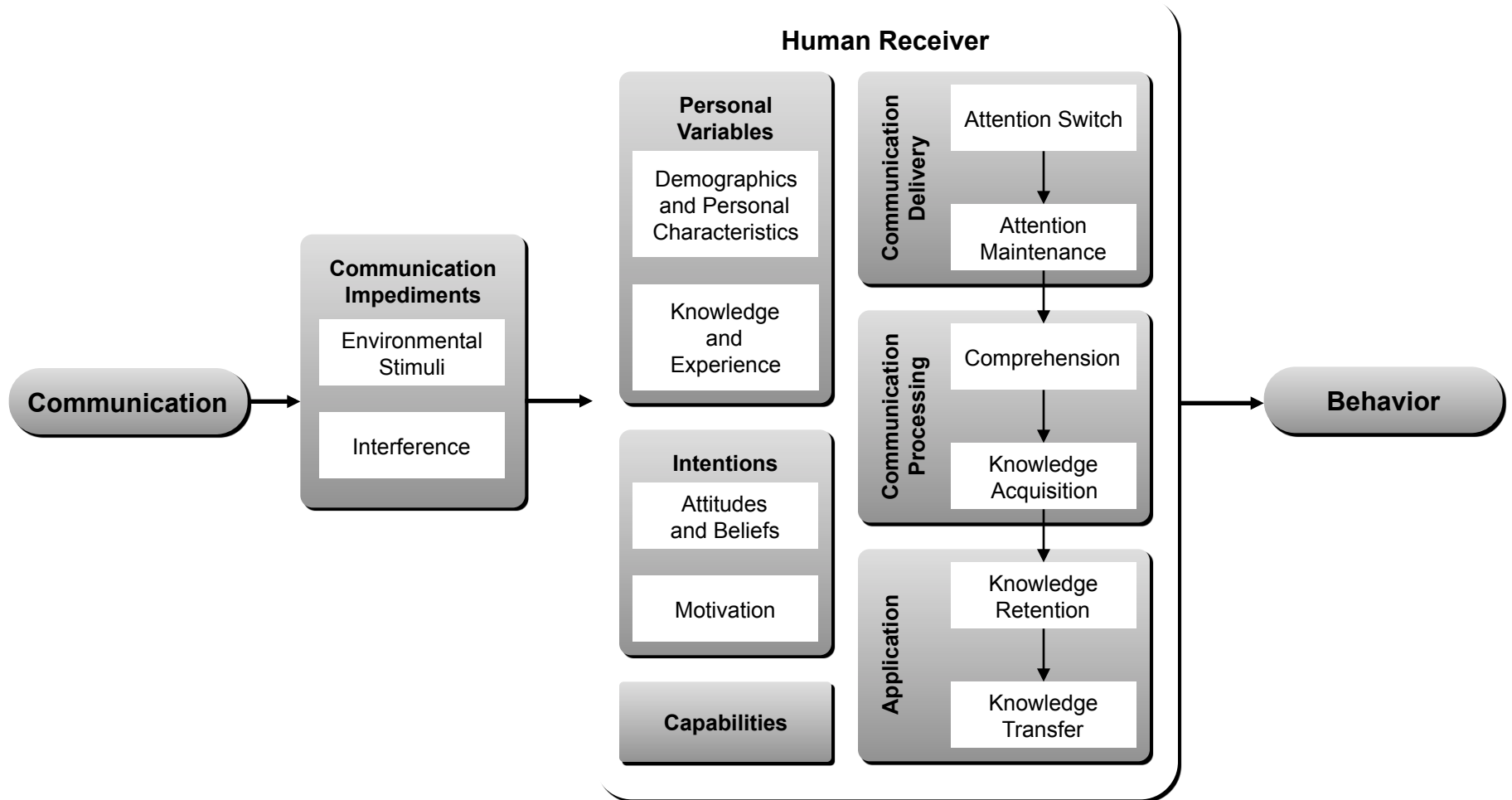
Will warn you when you are about to enter your eBay password into a non-eBay site .



# 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

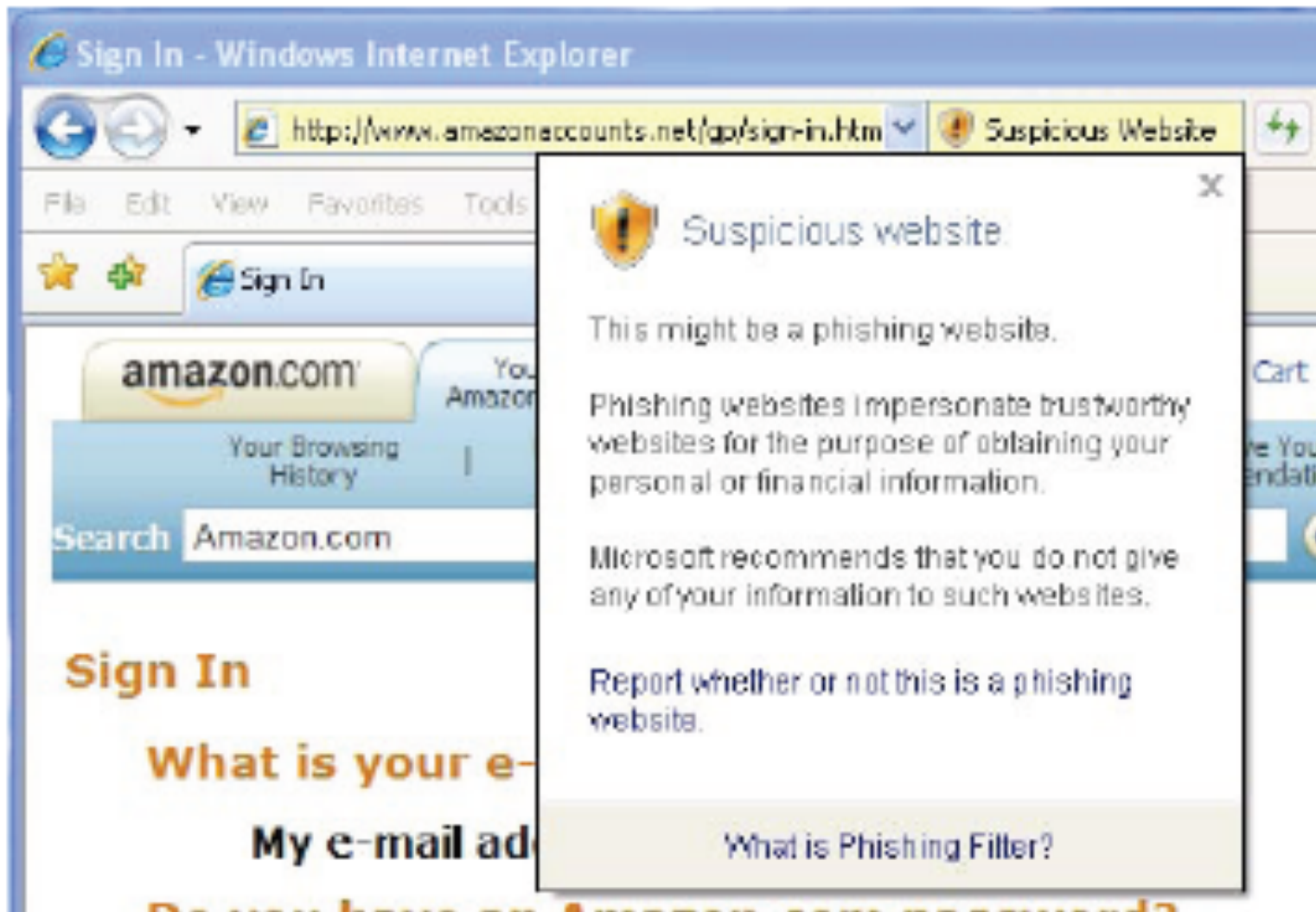
Serge Egelman  
Carnegie Mellon University  
egelman@cs.cmu.edu

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

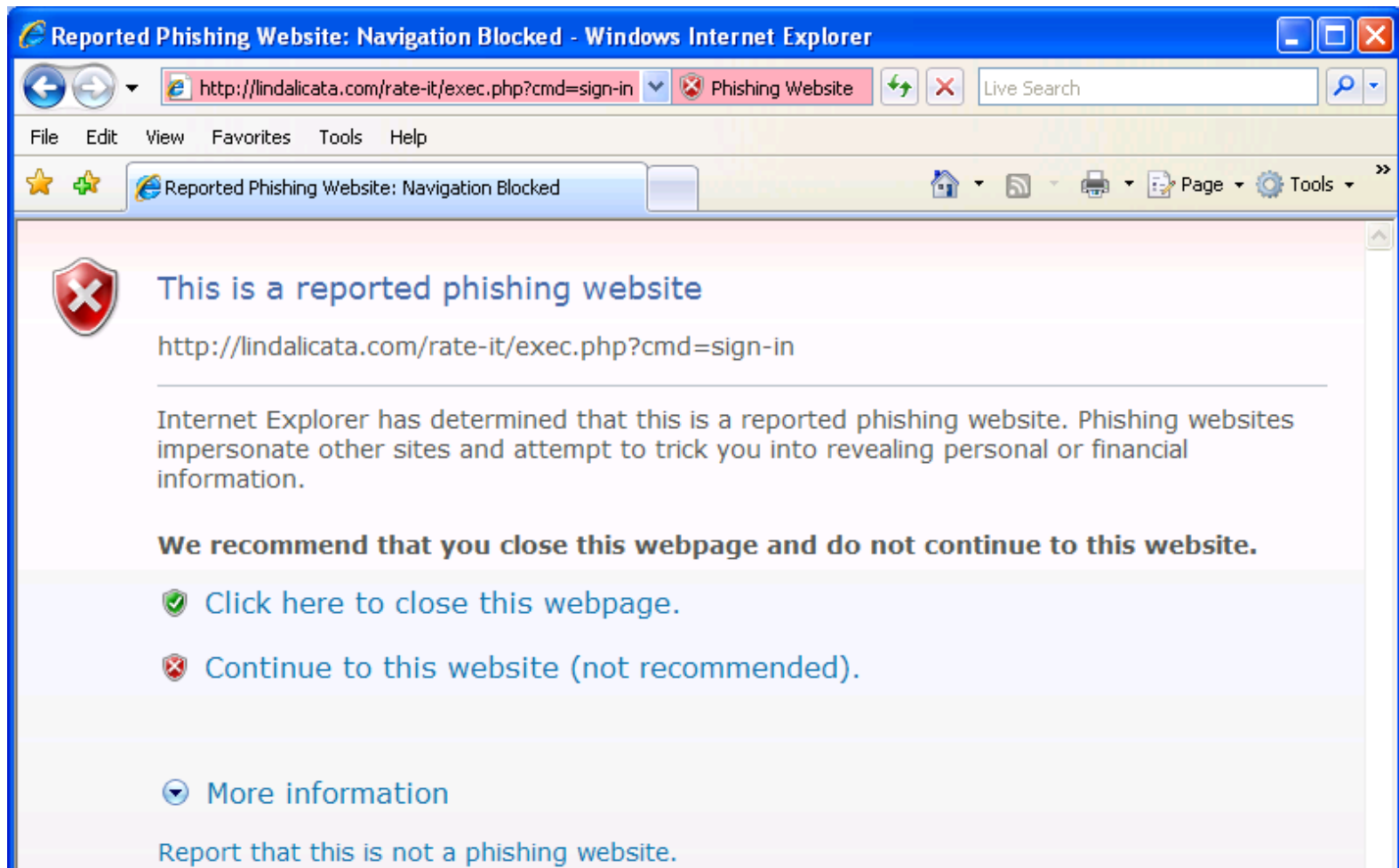
Jason Hong  
Carnegie Mellon University  
jasonh@cs.cmu.edu

- 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

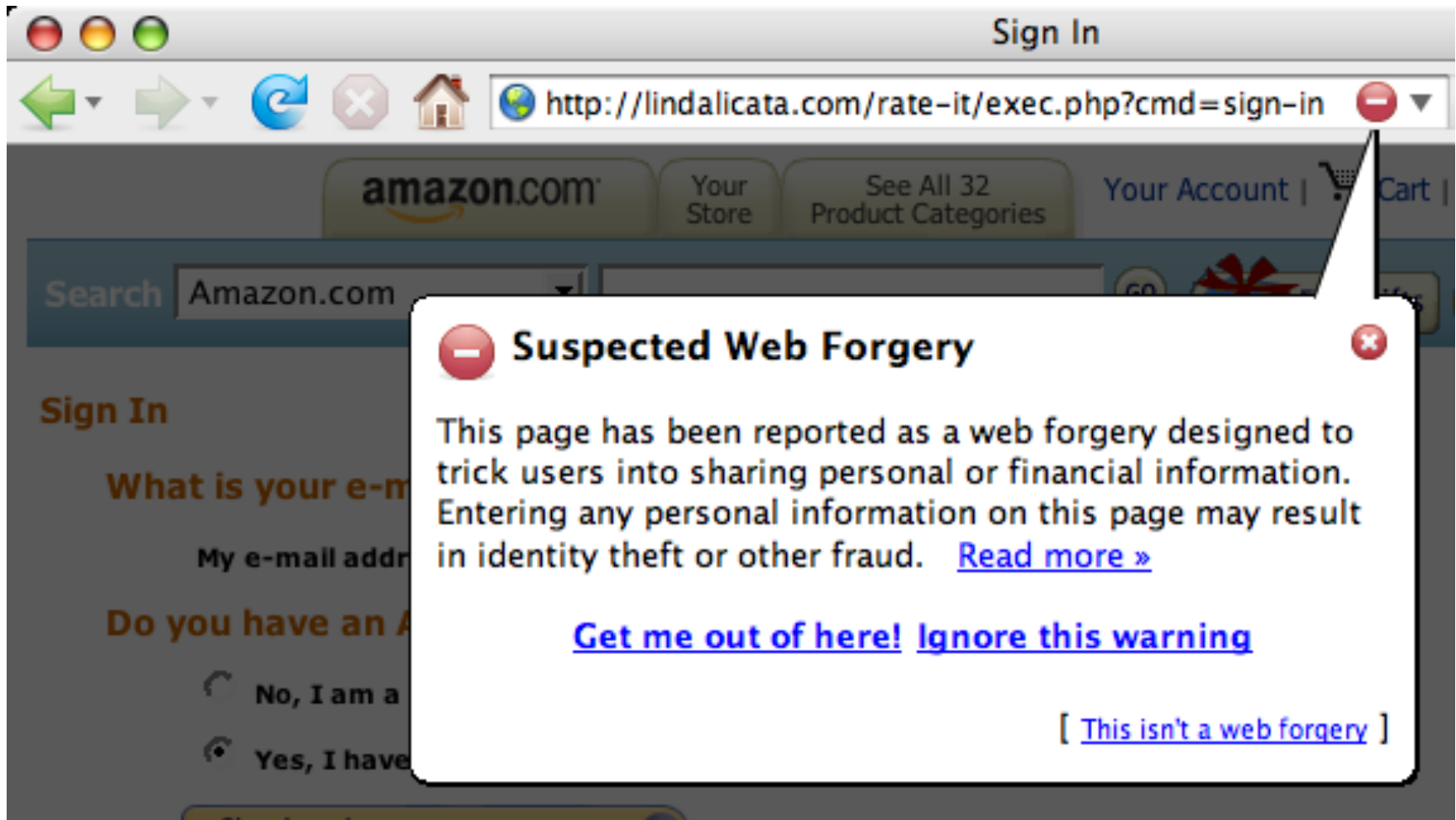
# Passive IE Phishing Warning



# Active IE Phishing Warning



# Active Firefox Phishing Warning





**How well do you think the phishing warnings work?**

# How well do the techniques work?

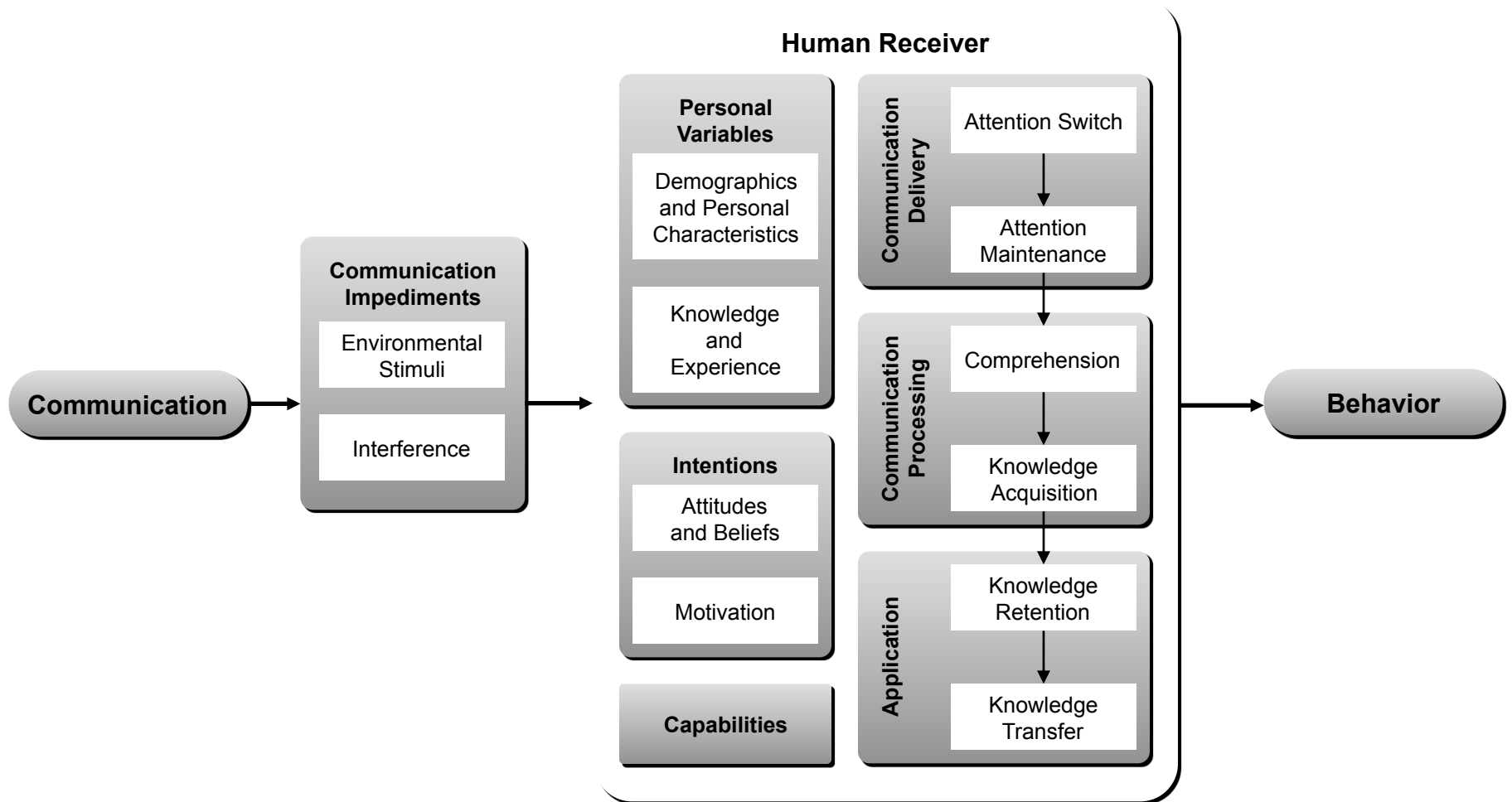
Condition Name	Size	Clicked	Phished
Firefox	20	20 (100%)	0 (0%)
Active IE	20	19 (95%)	9 (45%)
Passive IE	10	10 (100%)	9 (90%)
Control	10	9 (90%)	9 (90%)

**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





# 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