HCI and Design

SPRING 2016

Today

HCI and Security

Two case studies

- Phishing (and warnings)
- Password managers

Step back:

- Root causes of security usability problems
- How to address them

Credit: Many of today's slides based on material from Franzi Roesner

Security is important…

Several high-profile hacks in past years
- Number of vulnerabilities/attacks increasing

Billion dollar market

Cyberwarfare

Increasing government, academic, industry interest

Just read the news…

Security is different

Most of what we have talked about in this class is concerned with *achieving desired user behavior*

- Assume people are trying to do the right/correct thing

Security is concerned with *preventing undesired behavior*

- Different way of thinking!
- An enemy/opponent/hacker/adversary who is actively and maliciously trying to circumvent any protective measures you put in place

Computers are everywhere…

…and can always be attacked

Electronic banking, social networks, e-voting

iPods, iPhones, PDAs, RFID transponders

Automobiles

Appliances, TVs

(Implantable) medical devices

Cameras, picture frames, baby monitors, IoT everything

- See http://www.securityfocus.com/news/11499

Security mindset

Learn to think with a "security mindset" in general

- What is "the system"?
- How could this system be attacked?
  - Who are the attackers/adversaries?
  - What are their motivations, what is at stake?
  - What are the weakest points of attack?
- How could this system be defended?
  - What threats am I trying to address?
  - How effective will a given countermeasure be?
  - What is the trade-off between security, cost, and usability?

An example: airline security

Ask: what is the cost (economic and otherwise) of current airline security?

Ask: do existing rules (e.g., banning liquids) make sense?

Ask: are the tradeoffs worth it?

- (Why do we not apply the same rules to train travel?)
- (Would spending money elsewhere be more effective?)

Ask: how would *you* get on a plane if you were on the no-fly list?

- (I will not give you the answer – you can find it online)
- This is a thought experiment only!

Why is security so hard?

Technical reasons (*not the focus of this class*)

Computer security is not just about computers!

- Humans in the loop… unreliable, unpredictable, irrational, susceptible
- Humans are unwilling to trade off features for security

Ease of attacks

- Cheap, distributed, automated, anonymous, insider threats

Security not built in from the beginning

Security as a trade-off

The goal is not (usually) "to make the system as secure as possible"…

- How would we do that easily?

…but instead, "to make the system as secure as possible *within certain constraints*" (cost, usability, convenience)

- Military vs. personal networks

Must understand the existing constraints

- e.g., passwords, education, context, expectations…

Usable Security

Why is usability important?

- People are the critical element of any computer system
- People are the reason computers exist in the first place

- Even if it is possible for a system to protect against an adversary, people may use the system in other, less secure ways.

Usable Security

Schneier on Security

A weblog covering security and security technology.

« The Emergence of a Global Infrastructure for Mass Registration and Surveillance | Main | PDF Redacting Failure »

May 02, 2005

Users Disabling Security

It's an old story: users disable a security measure because it's annoying, allowing an attacker to bypass the measure.

> A [redacted] accused in a deadly courthouse rampage was able to enter the chambers of the judge slain in the attack and hold the occupants hostage because the door was unlocked and a buzzer entry system was not activated, a sheriff's report says.

Security doesn't work unless the users want it to work. This is true on the personal and national scale, with or without technology.

Today

HCI and Security

Two case studies

- Phishing (and warnings)
- Password managers

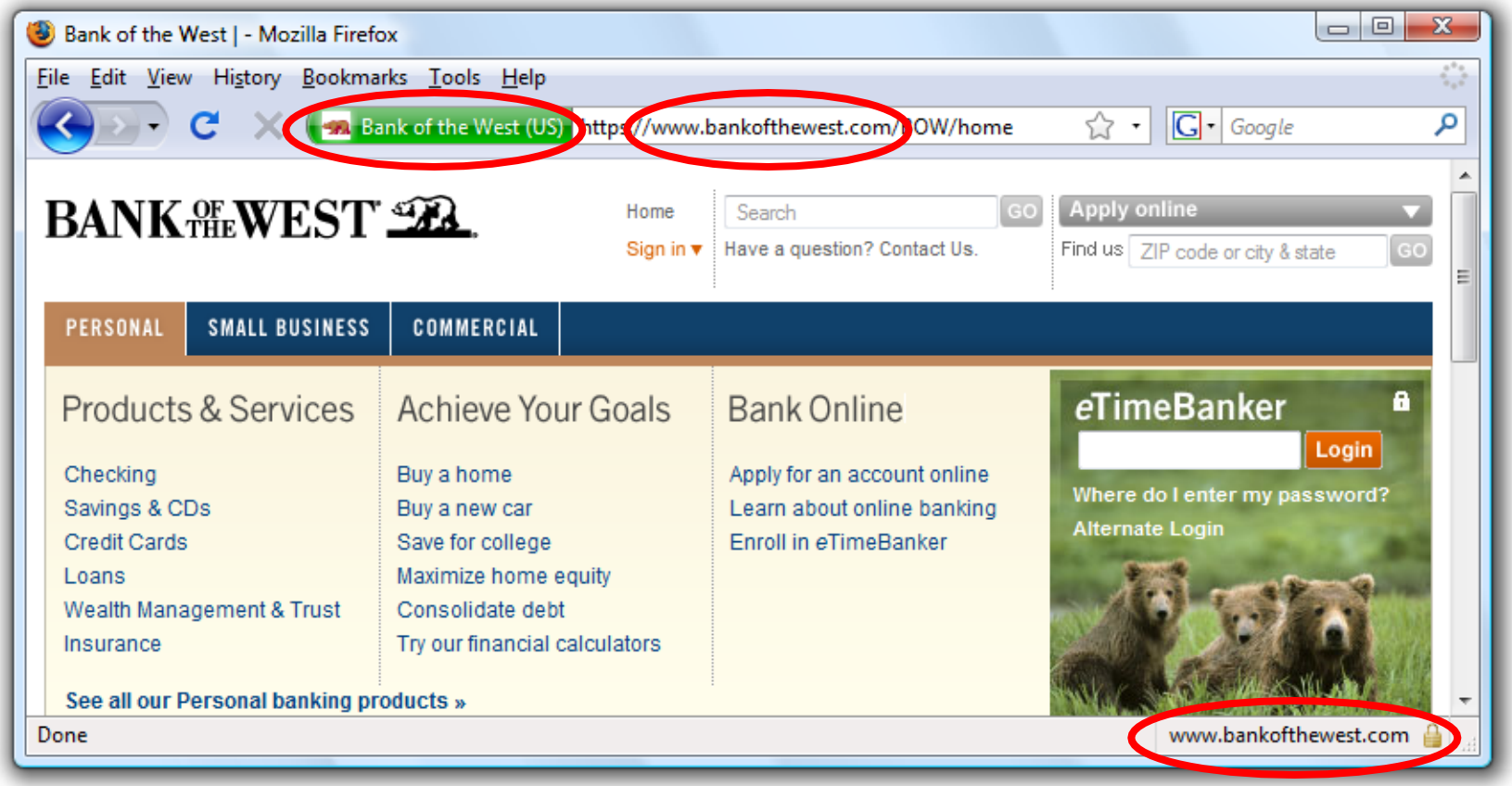
Step back:

- Root causes of security usability problems
- How to address them

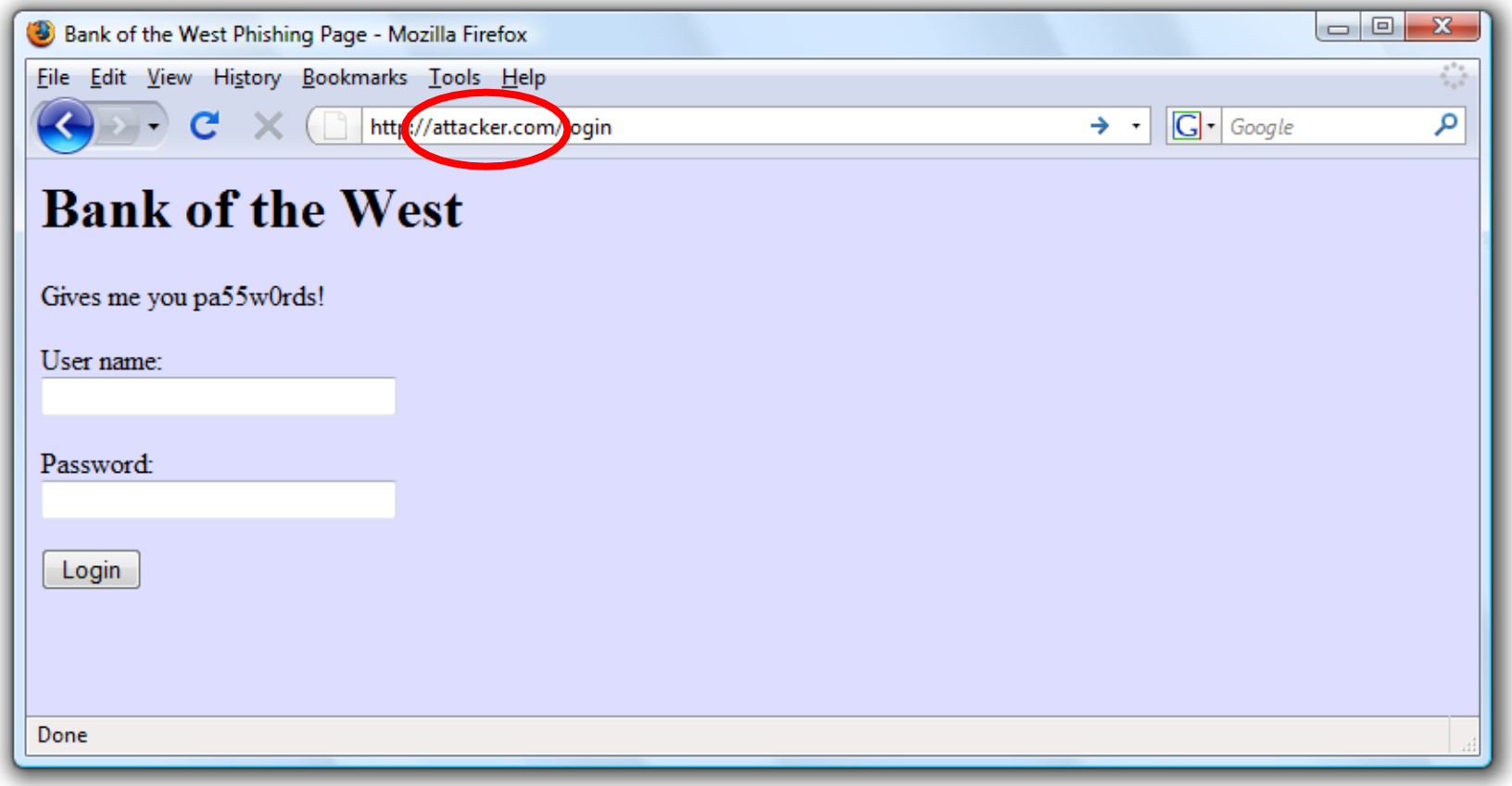
Credit: Many of today's slides based on material from Franzi Roesner

A Typical Phishing Page

Safe to Type Your Password?

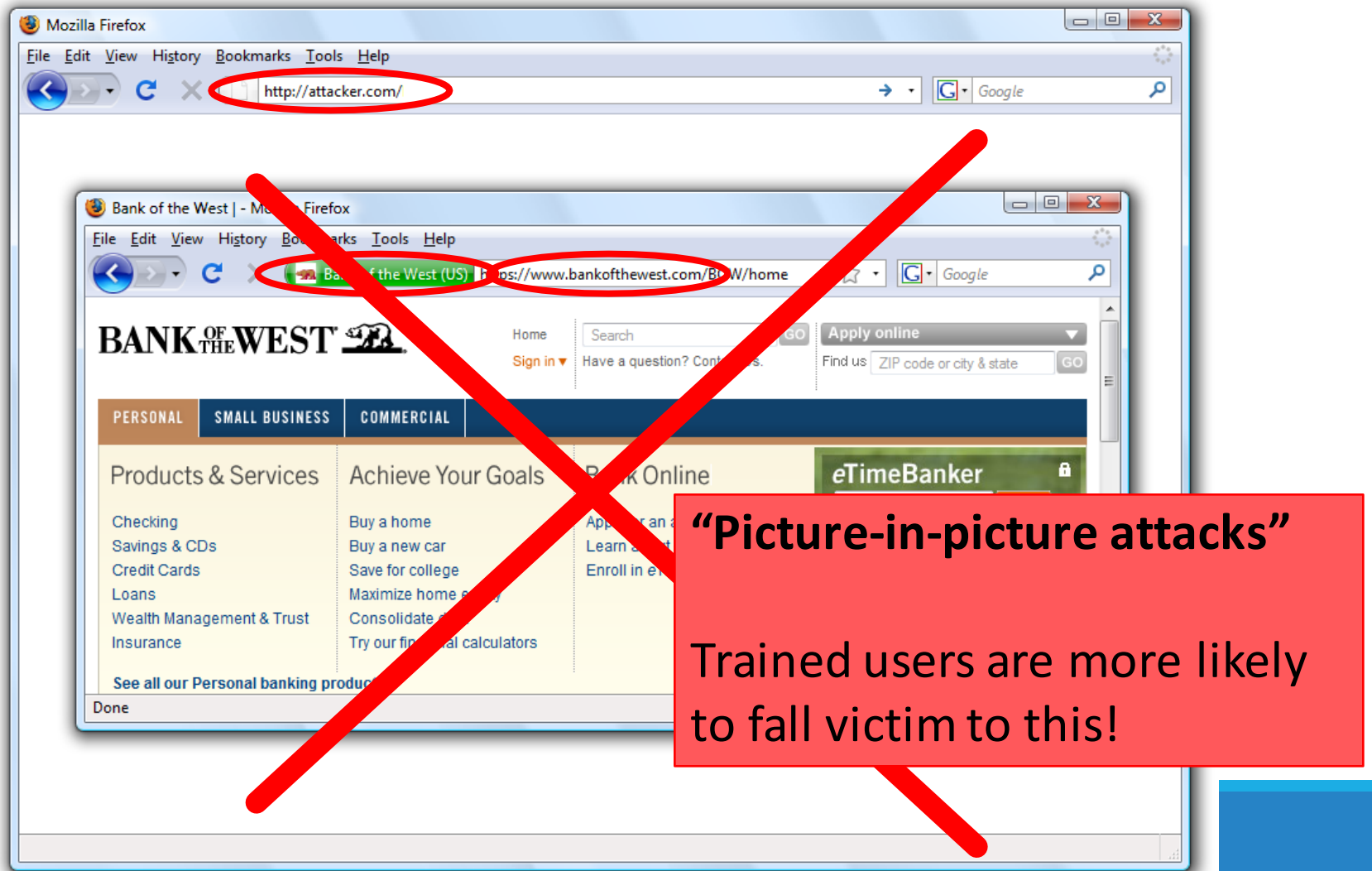


Safe to Type Your Password?



Safe to Type Your Password?

Safe to Type Your Password?



Experiments at Indiana University

Reconstructed the social network by crawling sites like Facebook, MySpace, LinkedIn and Friendster

Sent 921 Indiana University students a spoofed email that appeared to come from their friend

Email redirected to a spoofed site inviting the user to enter his/her secure university credentials

- Domain name clearly distinct from indiana.edu

72% of students entered their real credentials into the spoofed site

Experiments at Indiana University

Control group: 15 of 94 (16%) entered personal information

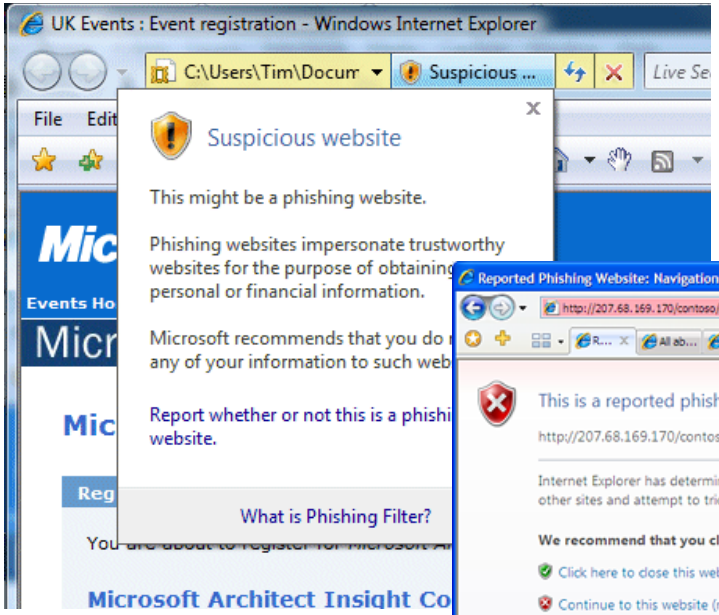
Social group: 349 of 487 (72%) entered personal information

70% of responses within first 12 hours

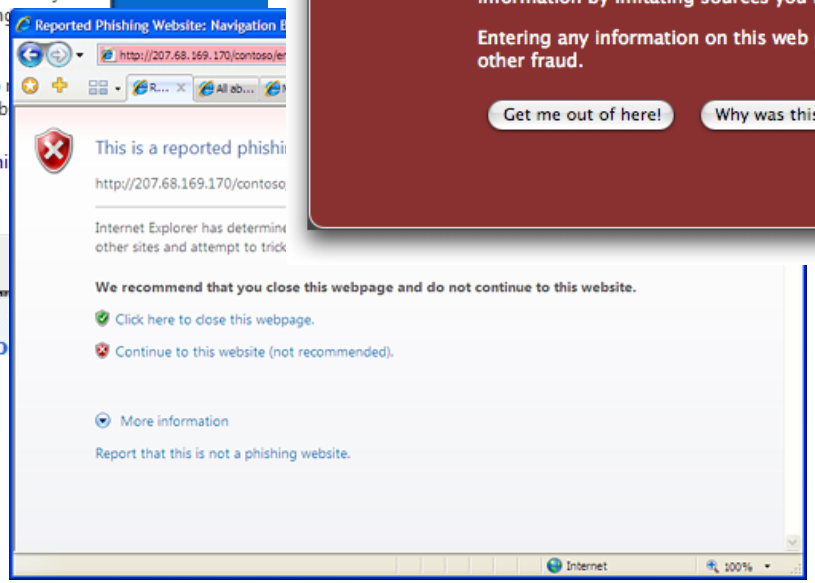
Adversary wins by gaining users' trust

Also: If a site looks "professional", people likely to believe that it is legitimate

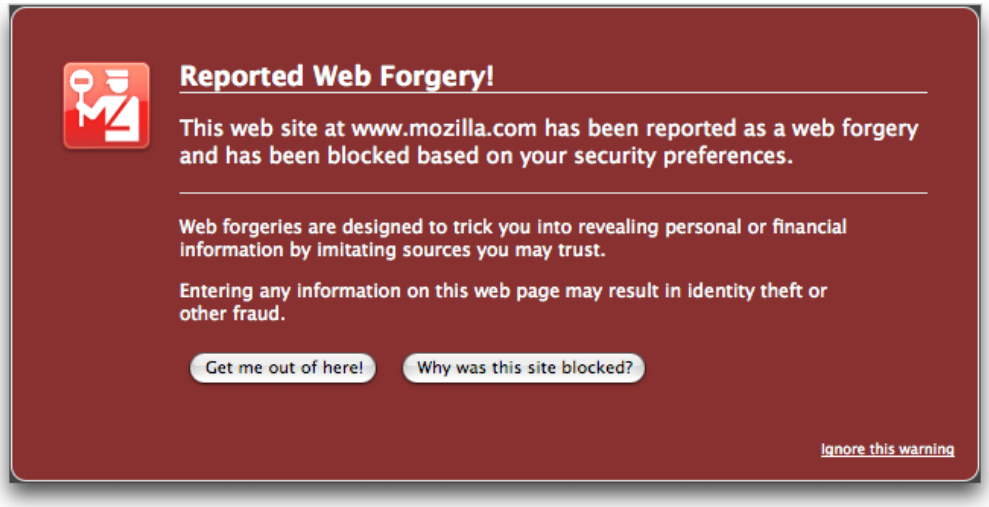
Phishing Warnings



Passive (IE)



Active (IE)



Active (Firefox)

[Egelman et al.]

Are Phishing Warnings Effective?

CMU study of 60 users

Asked to make eBay and Amazon purchases

All were sent phishing messages in addition to the real purchase confirmations

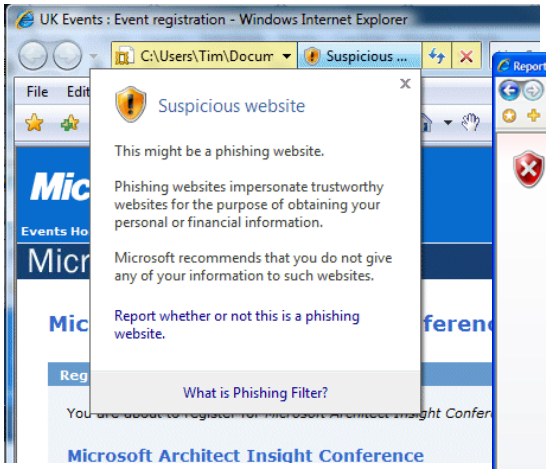
Goal: compare active and passive warnings

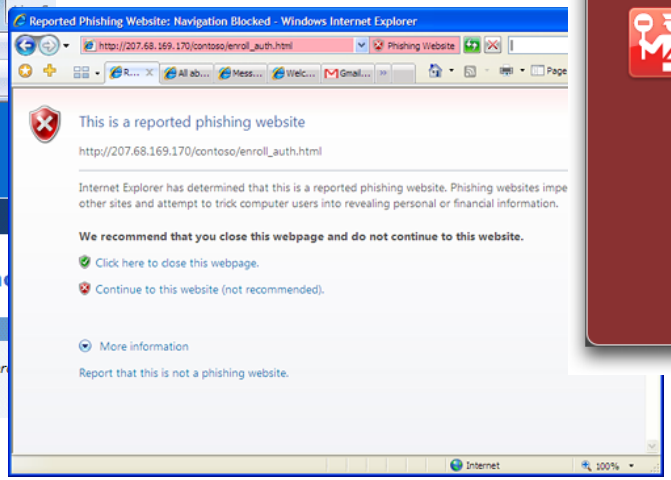
[Egelman et al.]

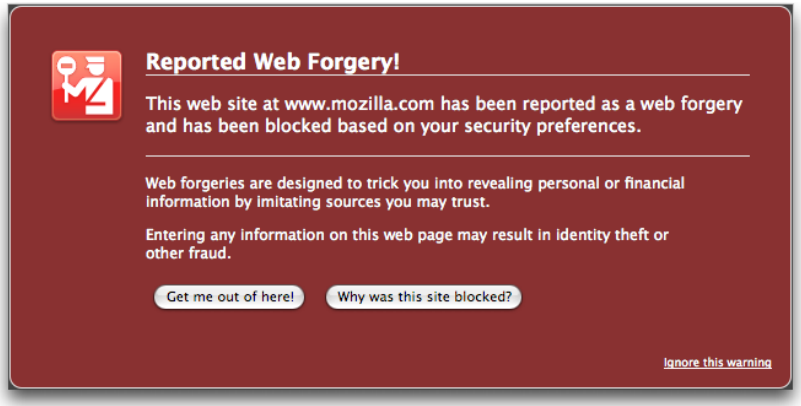
Active vs. Passive Warnings

Active warnings significantly more effective

- Passive (IE): 100% clicked, 90% phished
- Active (IE): 95% clicked, 45% phished
- Active (Firefox): 100% clicked, 0% phished







Passive (IE) Active (IE) Active (Firefox)

[Egelman et al.]

User Response to Warnings

Some fail to notice warnings entirely

- Passive warning takes a couple of seconds to appear; if user starts typing, their keystrokes dismiss the warning

Some saw the warning, closed the window, went back to email, clicked links again, were presented with the same warnings… repeated 4-5 times

- Conclusion: "website is not working"
- Users never bothered to read the warnings, but were still prevented from visiting the phishing site
- Active warnings work!

[Egelman et al.]

Why Do Users Ignore Warnings?

Don't trust the warning

- "Since it gave me the option of still proceeding to the website, I figured it couldn't be that bad"

Ignore warning because it's familiar (IE users)

- "Oh, I always ignore those"
- "Looked like warnings I see at work which I know to ignore"
- "I thought that the warnings were some usual ones displayed by IE"
- "My own PC constantly bombards me with similar messages"

Case Study #2: Password Managers

Password managers: software tools that handle creating and "remembering" strong passwords

Potentially:

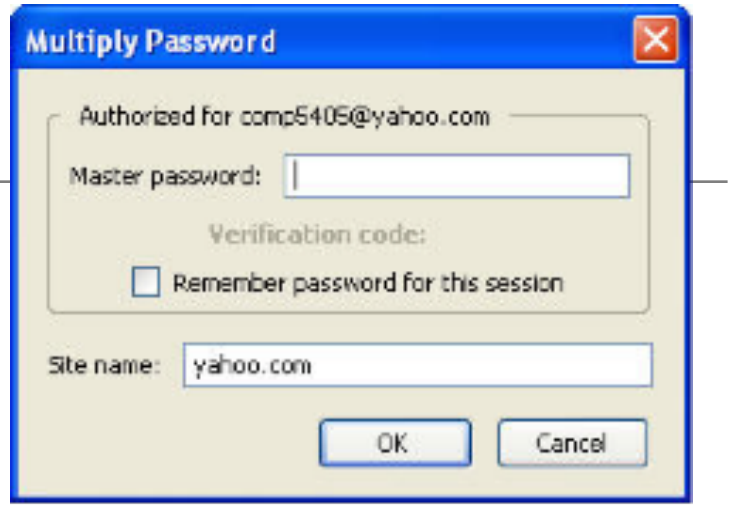
- **Easier** for users
- More **secure**

Examples:

- PwdHash (Usenix Security 2005)
- Password Multiplier (WWW 2005)

PwdHash

Password Multiplier



@@ in front of passwords to protect; or F2

sitePwd = Hash(pwd,domain)

Prevent phishing attacks

Activate with Alt-P or double-click

sitePwd = Hash(username, pwd, domain)

Both solutions target simplicity and transparency.

[Chiasson, van Oorschot, Biddle]

Usability Testing

Are these programs usable? If not, what are the problems?

[Chiasson, van Oorschot, Biddle]

Task Completion Results

	Success	Potentially Causing Security Exposures			
		Dangerous Success	Failures		
			Failure	False Completion	Failed due to Previous
PwdHash					
Log In	48%	44%	8%	0%	N/A
Migrate Pwd	42%	35%	11%	11%	N/A
Remote Login	27%	42%	31%	0%	N/A
Update Pwd	19%	65%	8%	8%	N/A
Second Login	52%	28%	4%	0%	16%
Password Multiplier					
Log In	48%	44%	8%	0%	N/A
Migrate Pwd	16%	32%	28%	20%	N/A
Remote Login	N/A	N/A	N/A	N/A	N/A
Update Pwd	16%	4%	44%	28%	N/A
Second Login	16%	4%	16%	0%	16%

[Chiasson, van Oorschot, Biddle]

Problem: Transparency

Unclear to users whether actions successful or not.

- Should be obvious when plugin activated.
- Should be obvious when password protected.

Users feel that they should be able to know their own password.

[Chiasson, van Oorschot, Biddle]

Problem: Mental Model

Users seemed to have misaligned mental models

- Not understand that one needs to put "@@" before *each* password to be protected.
- Think different passwords generated for each session.
- Think successful when were not.
- Not know to click in field before Alt-P.
- Don't understand what's happening: "Really, I don't see how my password is safer because of two @'s in front"

[Chiasson, van Oorschot, Biddle]

When "Nothing Works"

Tendency to try all passwords

- A poor security choice – phishing site could collect many passwords!
- May make the use of PwdHash or Password Multiplier *worse* than not using any password manager.

Usability problem leads to security vulnerabilities.

- Sometimes things designed to increase security can also increase other risks

Today

HCI and Security

Two case studies

- Phishing (and warnings)
- Password managers

Step back:

- Root causes of security usability problems
- How to address them

Credit: Many of today's slides based on material from Franzi Roesner

Question

Q. What are the root causes of usability issues in computer security?

Issue #1: Complexities, Lack of Intuition

Real World

We can see, understand, relate to.

Electronic World

Too complex, hidden, no intuition.

Issue #1: Complexities, Lack of Intuition

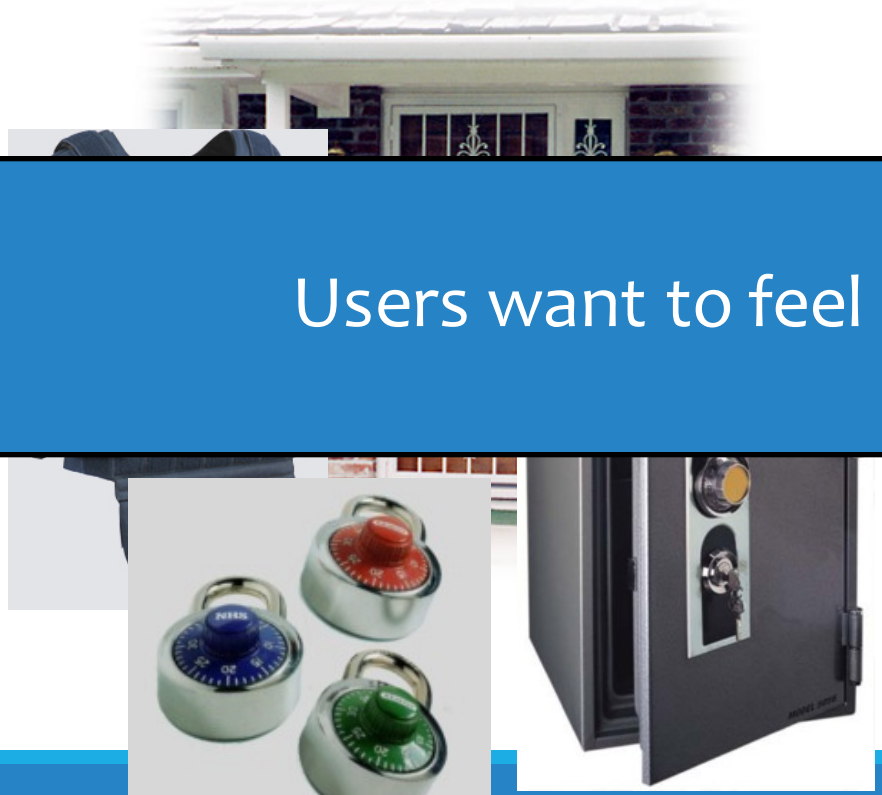
Mismatch between perception of technology and what really happens

- Public keys?
- Signatures?
- Encryption?
- Message integrity?
- Chosen-plaintext attacks?
- Chosen-ciphertext attacks?
- Password management?
- ...

Issue #2: Who's in Charge?

Real World

We can see, understand, relate to.



Electronic World

Too complex, hidden, no intuition.

Users want to feel like they're in control.

Issue #2: Who's in Charge?

Systems developers should help protect users

- Usable authentication systems
- Usable privacy settings (e.g., on social media)
- User-driven access control

Software applications help users manage their applications

- Anti-virus software
- Anti-web tracking browser add-ons
- PwdHash, Keychain for password management
- Some say: Can we trust software for these tasks?

Issue #3: Hard to Gauge Risks

"It won't happen to me!"

Sometimes a reasonable assumption, sometimes not.

"I remembered hearing about it and thinking that people that click on those links are stupid," she says. "Then it happened to me."

Ms. Miller says she now changes her password regularly and avoids clicking on strange links.
(Open Doors, by V. Vara, The Wall Street Journal, Jan 29, 2007)

Issue #4: No Accountability

Issue #3 is amplified when users are not held accountable for their actions

- E.g., from employers, service providers, etc.
- (Not all parties will perceive risks the same way)

Also, recall that a user's poor security choices may affect **other** people

- E.g., compromise account of user with weak password, then exploit a local (rather than remote) vulnerability to get root access

Issue #5: Annoying, Awkward, or Difficult

Difficult

- Remembering 50 different, "random" passwords

Awkward

- Lock computer screen every time leave the room

Annoying

- Browser warnings, virus alerts, forgotten passwords, firewalls

Consequence:

- Changing user's knowledge may **not** affect their behavior

Issue #6: Social Issues

Public opinion, self-image

- Only “nerds” or the “super paranoid” follow security guidelines

Unfriendly

- Locking computers suggests distrust of co-workers

Annoying

- Sending encrypted emails that say, “what would you like for lunch?”

Question

Q. What approaches can we take to mitigate usability issues in computer security?

Response #1: Education and Training

Education:

- Teaching technical concepts, risks

Training

- Change behavior through:
  - Drill
  - Monitoring
  - Feedback
  - Reinforcement
  - Punishment

May be part of the solution – but not the whole solution

Response #2: Security Should Be Invisible

Security should happen

- Naturally
- By Default
- Without user input or understanding

Recognize and stop bad actions

- Leads to things not working for reasons user doesn't understand

Users will then try to get the system to work, possibly further reducing security

- E.g., "dangerous successes" for password managers

Starting to see some invisibility

- VPNs, Automatic Security Updates, etc.

Response #3: "Are You Sure?"

Security should be invisible

- Except when the user tries something dangerous
- In which case a warning is given

But as we have discussed, warnings have limitations

Two realistic cases:

- Heed warning. But see problems / commonality with Response #2 ("security should be invisible")
- Ignore warning. If so, it is not effective

Response #4: Focus on Users, Use Metaphors

Clear, understandable metaphors:

- Physical analogs; e.g., red stop signs

User-centered design: Start with user's model of the world

Standardized security model across applications

- User doesn't need to learn many models, one for each application

Meaningful, intuitive user input

- Don't assume things on user's behalf
- Figure out how to ask so that user can answer intelligently

Response #5: Least Resistance

"Match the most comfortable way to do tasks with the least granting of authority"

- Ka-Ping Yee, Security and Usability

Should be "easy" to comply with security policy

"Users value and want security and privacy, but they regard them only as secondary to completing the primary tasks"

- Karat et al, Security and Usability

Today

HCI and Security

Two case studies

- Phishing (and warnings)
- Password managers

Step back:

- Root causes of security usability problems
- How to address them

Next time…

- HCI for global development and ICTD
- i.e., my work ☺

Credit: Many of today's slides based on material from Franzi Roesner

Activity

THINK OUTSIDE THE BOX!

- Do a "security analysis" for your project.
- What is "the system"?
- How could the system be attacked? ---- come up with a few scenarios!
  - Who are the attackers/adversaries?
  - What are their motivations?
  - What is at stake? i.e. what are the "resources"?
  - What are the weakest points of the system? Susceptible to attack?
- How could the system be defended?
  - What threats am I trying to address?
  - What countermeasures can I use?
  - How effective will the countermeasures be?
  - What is the trade-off between security, cost, and usability?