CSE 484 / CSE M 584: Computer Security and Privacy

Usable Security

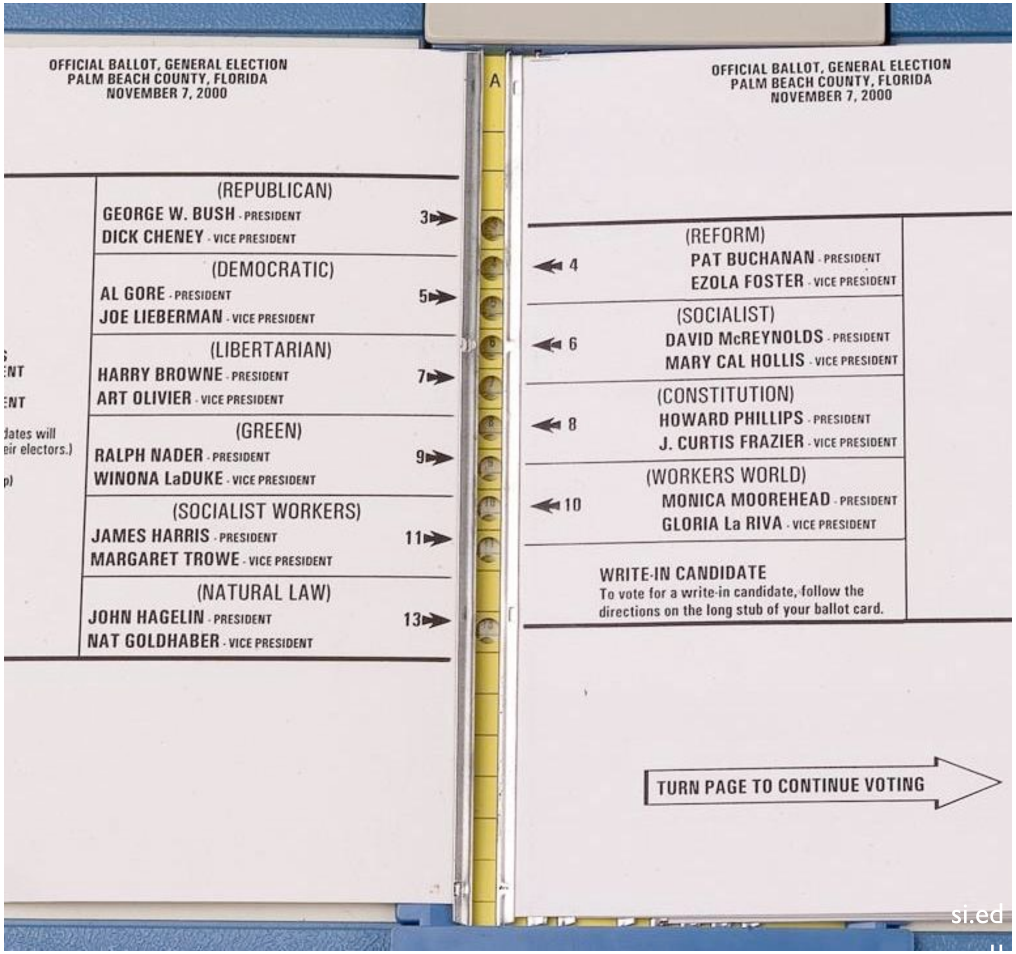
Spring 2015

Franziska (Franzi) Roesner

franzi@cs.washington.edu

Thanks to Dan Boneh, Dieter Gollmann, Dan Halperin, Yoshi Kohno, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...

Poor Usability Causes Problems



OFFICIAL BALLOT, GENERAL ELECTION
PALM BEACH COUNTY, FLORIDA
NOVEMBER 7, 2000

S
ENT
ENT
dates will
eir electors.)
p)

(REPUBLICAN)
GEORGE W. BUSH - PRESIDENT
DICK CHENEY - VICE PRESIDENT
3 ➡

(DEMOCRATIC)
AL GORE - PRESIDENT
JOE LIEBERMAN - VICE PRESIDENT
5 ➡

(LIBERTARIAN)
HARRY BROWNE - PRESIDENT
ART OLIVIER - VICE PRESIDENT
7 ➡

(GREEN)
RALPH NADER - PRESIDENT
WINONA LaDUKE - VICE PRESIDENT
9 ➡

(SOCIALIST WORKERS)
JAMES HARRIS - PRESIDENT
MARGARET TROWE - VICE PRESIDENT
11 ➡

(NATURAL LAW)
JOHN HAGELIN - PRESIDENT
NAT GOLDHABER - VICE PRESIDENT
13 ➡

A

OFFICIAL BALLOT, GENERAL ELECTION
PALM BEACH COUNTY, FLORIDA
NOVEMBER 7, 2000

⬅ 4
(REFORM)
PAT BUCHANAN - PRESIDENT
EZOLA FOSTER - VICE PRESIDENT

⬅ 6
(SOCIALIST)
DAVID McREYNOLDS - PRESIDENT
MARY CAL HOLLIS - VICE PRESIDENT

⬅ 8
(CONSTITUTION)
HOWARD PHILLIPS - PRESIDENT
J. CURTIS FRAZIER - VICE PRESIDENT

⬅ 10
(WORKERS WORLD)
MONICA MOOREHEAD - PRESIDENT
GLORIA La RIVA - VICE PRESIDENT

WRITE-IN CANDIDATE
To vote for a write-in candidate, follow the directions on the long stub of your ballot card.

TURN PAGE TO CONTINUE VOTING

si.ed

AP

Importance in Security

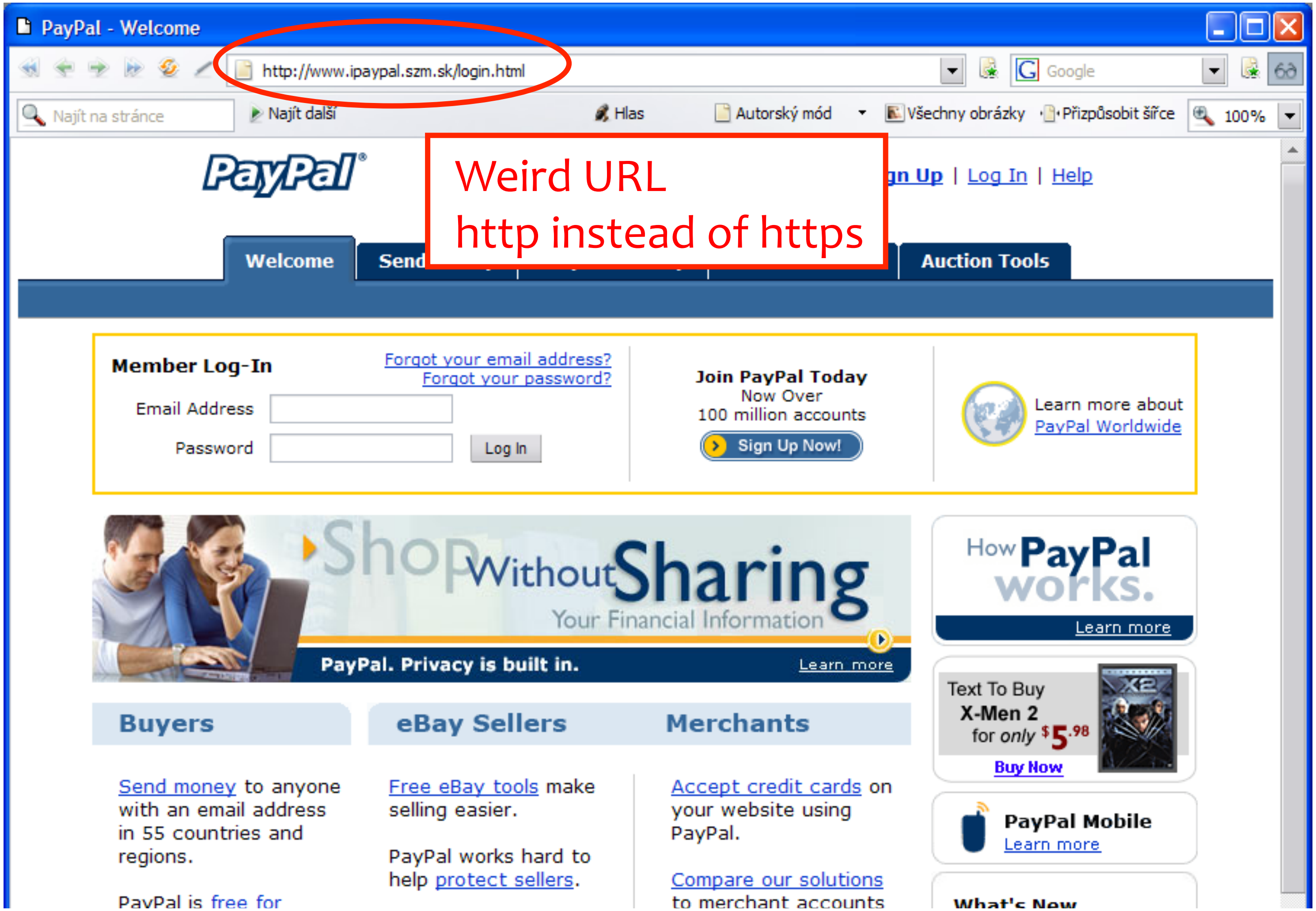
- Why is usability important?
  - People are the critical element of any computer system
    - People are the real reason computers exist in the first place
  - Even if it is **possible** for a system to protect against an adversary, people may use the system in other, **less secure** ways

Today

- 3 case studies
  - Phishing
  - SSL warnings
  - Password managers
- Step back: root causes of usability problems, and how to address

Case Study #1: Phishing

A Typical Phishing Page



Weird URL
http instead of https

PayPal - Welcome

http://www.ipaypal.szm.sk/login.html

Google

Najít na stránce ▶ Najít další Hlas Autorský mód Všechny obrázky Přizpůsobit šířce 100%

PayPal®

...gn Up | Log In | Help

Welcome | Send ... | Auction Tools

Member Log-In

Forgot your email address?
Forgot your password?

Email Address

Password

Log In

Join PayPal Today
Now Over
100 million accounts

Sign Up Now!

Learn more about
PayPal Worldwide

Shop Without Sharing
Your Financial Information

PayPal. Privacy is built in. Learn more

How PayPal works.
Learn more

Text To Buy
X-Men 2
for only $5.98
Buy Now

Buyers

Send money to anyone with an email address in 55 countries and regions.

PayPal is free for

eBay Sellers

Free eBay tools make selling easier.

PayPal works hard to help protect sellers.

Merchants

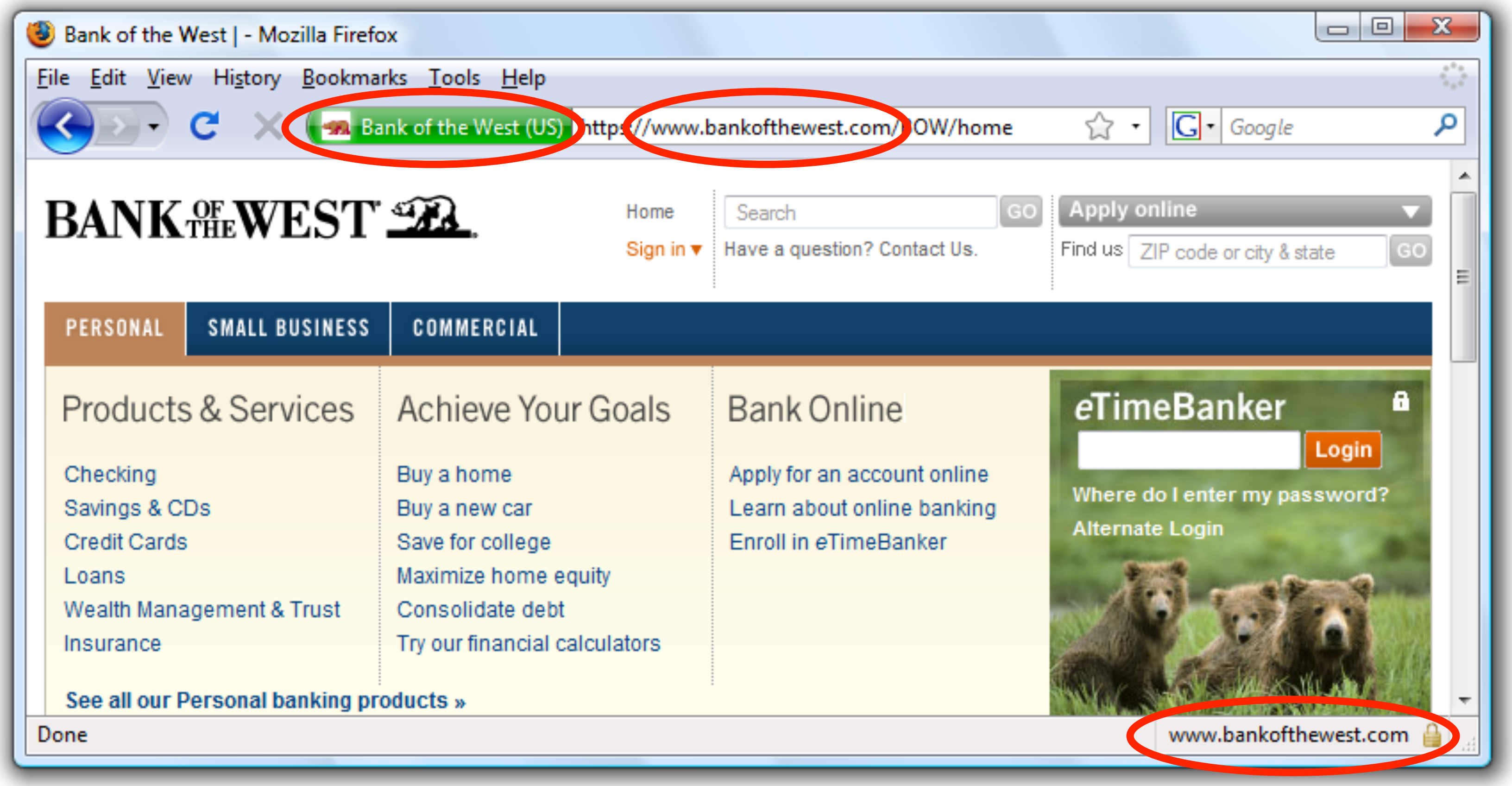
Accept credit cards on your website using PayPal.

Compare our solutions to merchant accounts

PayPal Mobile
Learn more

What's New

Safe to Type Your Password?


Bank of the West | - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Bank of the West (US)
https://www.bankofthewest.com/BOW/home
Google
Done
www.bankofthewest.com

BANK OF THE WEST

Home

Sign in ▾

Search GO

Have a question? Contact Us.

Apply online

Find us ZIP code or city & state GO

PERSONAL | SMALL BUSINESS | COMMERCIAL

Products & Services

- Checking
- Savings & CDs
- Credit Cards
- Loans
- Wealth Management & Trust
- Insurance

Achieve Your Goals

- Buy a home
- Buy a new car
- Save for college
- Maximize home equity
- Consolidate debt
- Try our financial calculators

Bank Online

- Apply for an account online
- Learn about online banking
- Enroll in eTimeBanker

eTimeBanker

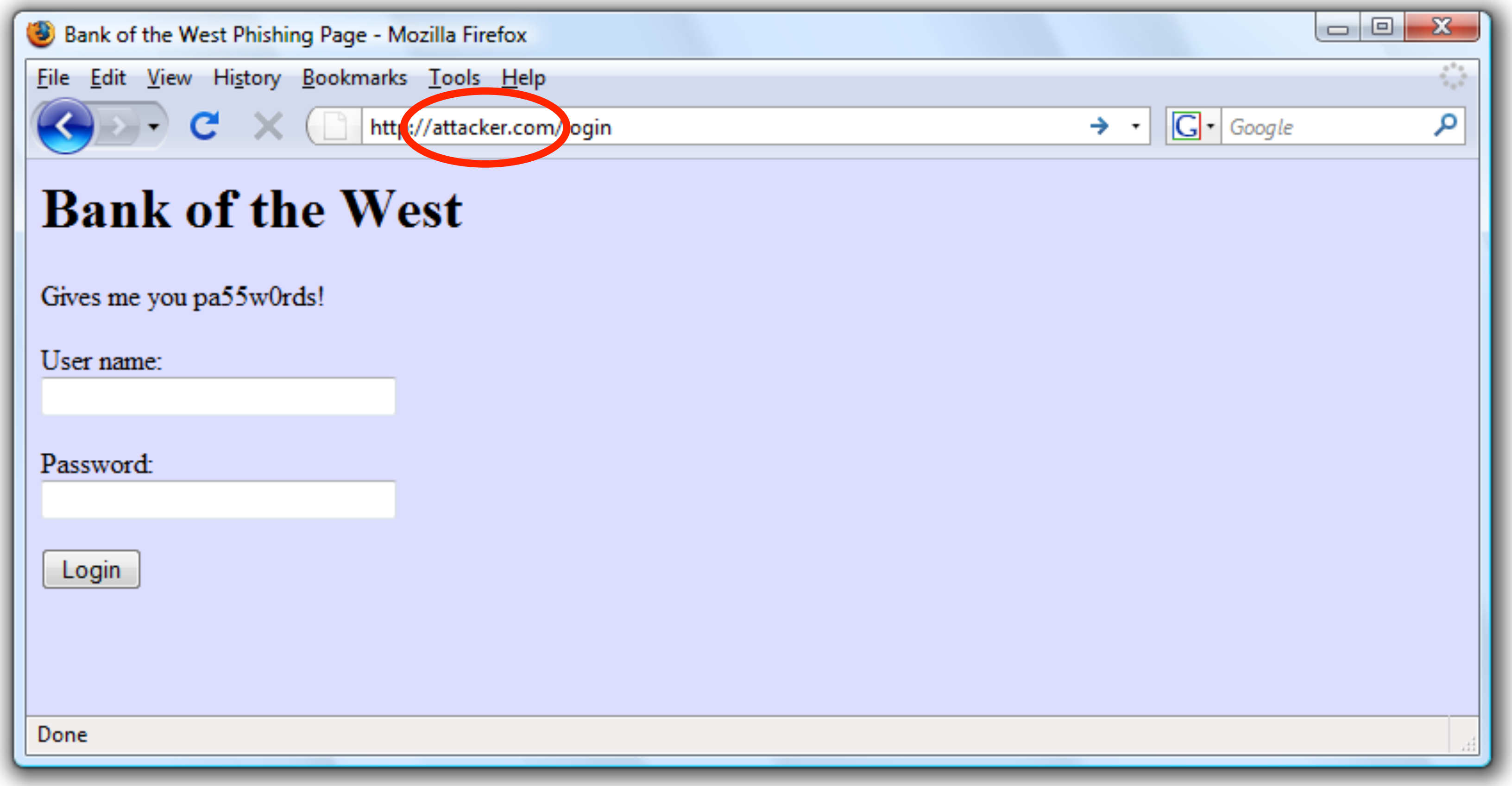
Login

Where do I enter my password?

Alternate Login

See all our Personal banking products »

Safe to Type Your Password?



Bank of the West Phishing Page - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://attacker.com/login
Google

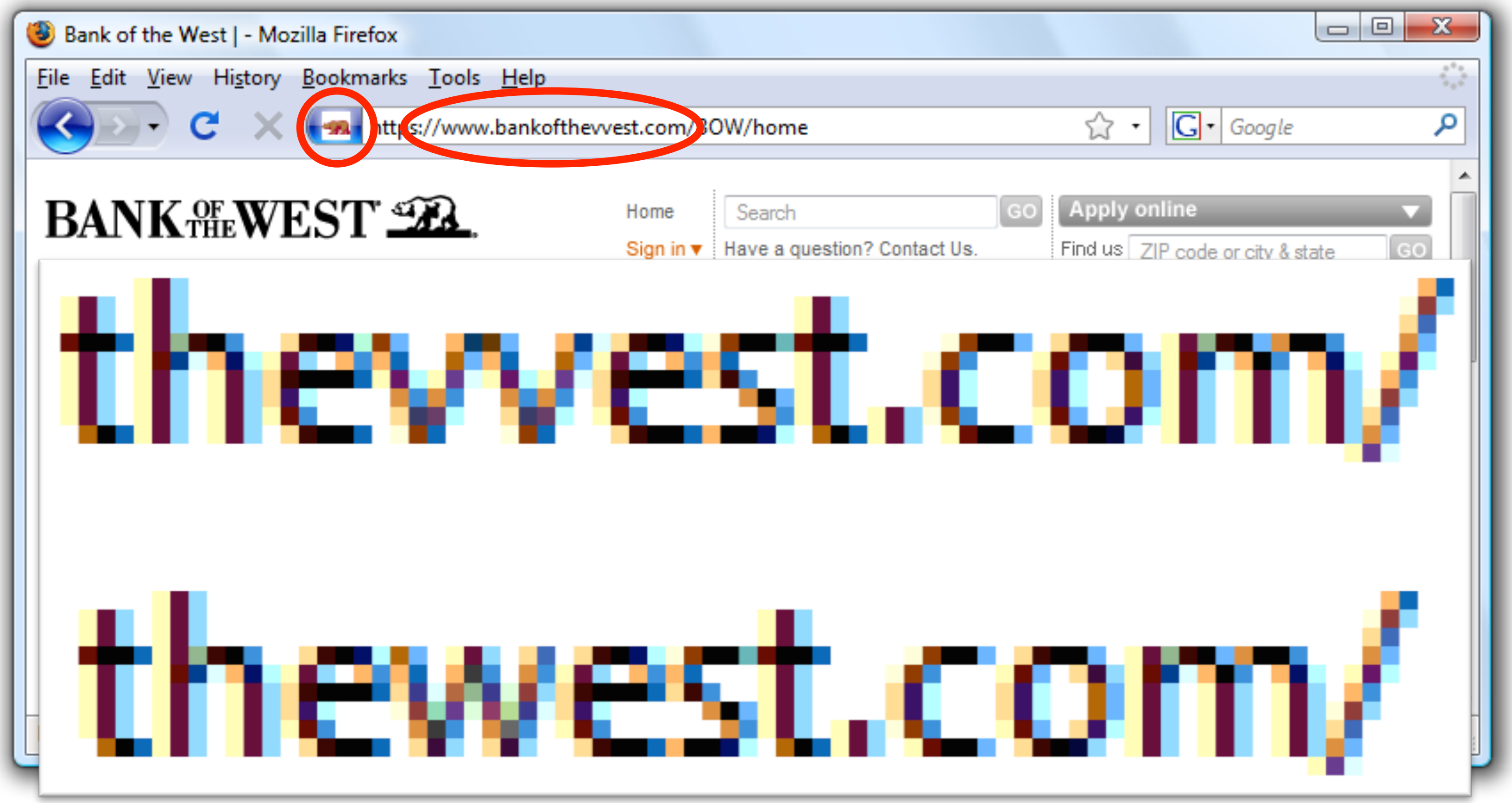
Bank of the West

Gives me you pa55w0rds!

User name:

Password:

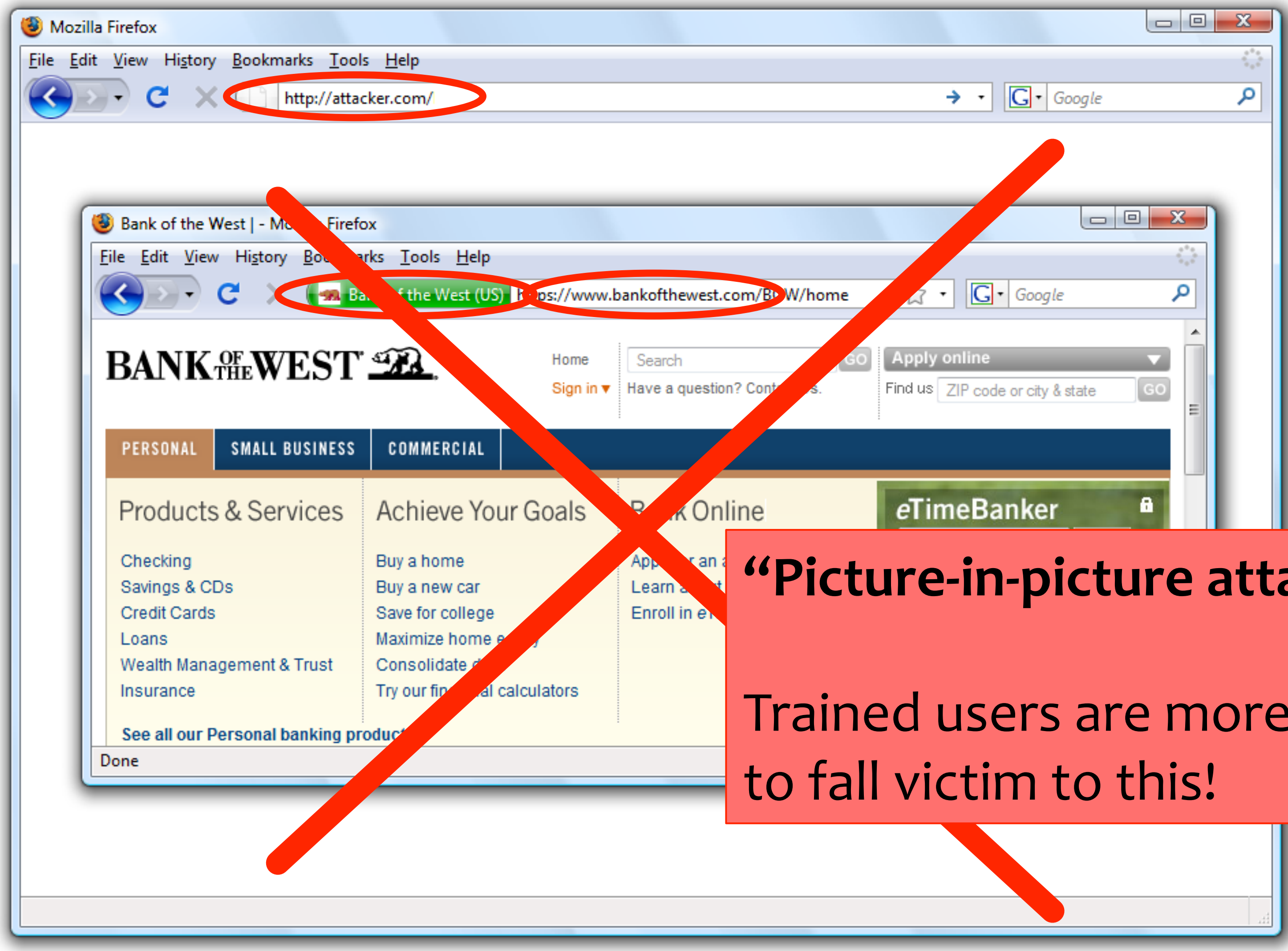
Safe to Type Your Password?



Bank of the West | - Mozilla Firefox

https://www.bankofthevvest.com/BOW/home

Safe to Type Your Password?



"Picture-in-picture attacks"

Trained users are more likely to fall victim to this!

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

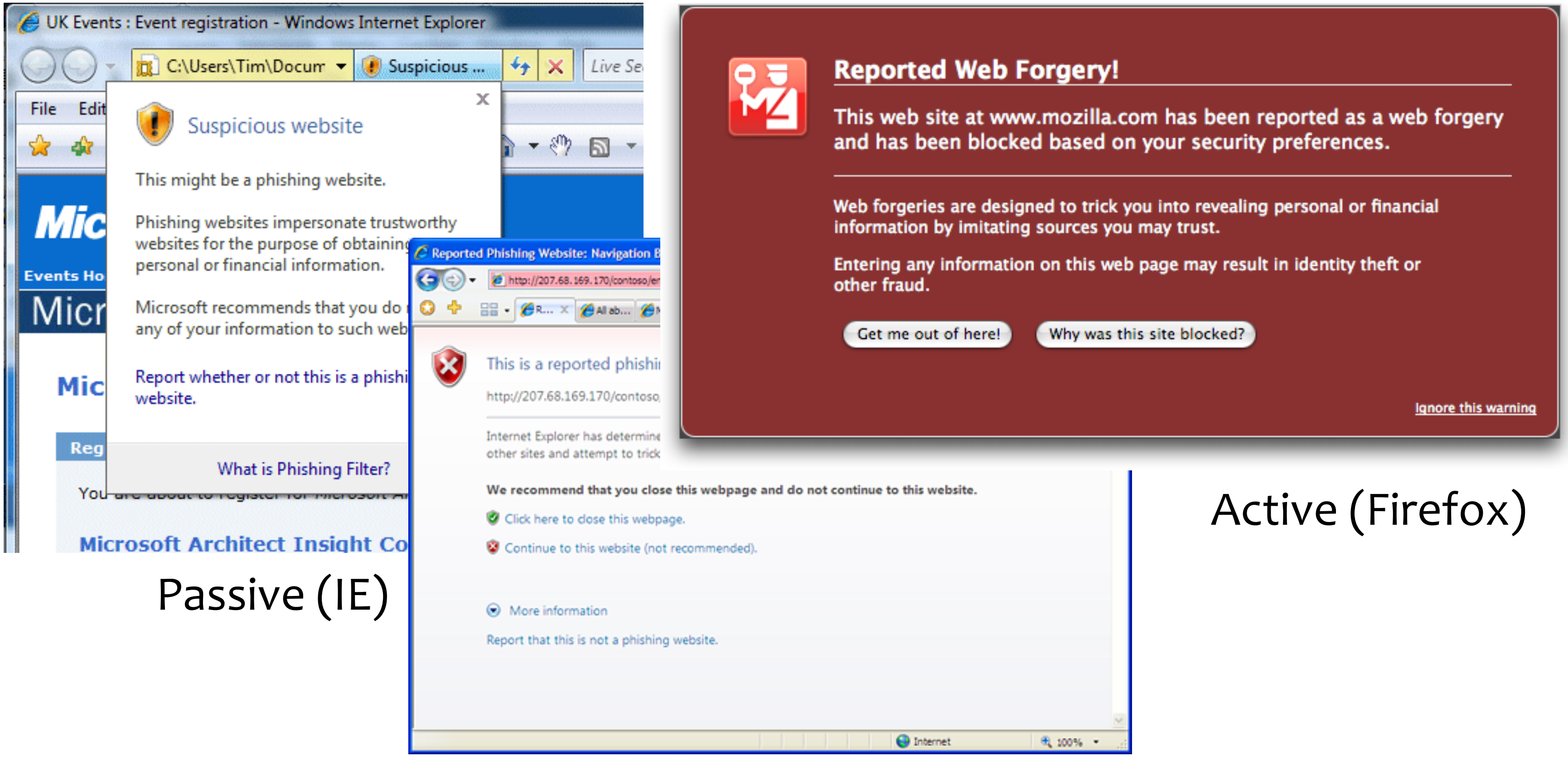
More Details

- 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



UK Events : Event registration - Windows Internet Explorer

C:\Users\Tim\Docum

Suspicious ...

Suspicious website

This might be a phishing website.

Phishing websites impersonate trustworthy websites for the purpose of obtaining personal or financial information.

Microsoft recommends that you do any of your information to such web

Report whether or not this is a phishi website.

What is Phishing Filter?

Passive (IE)

Reported Phishing Website: Navigation B

http://207.68.169.170/contoso/er

This is a reported phishi

http://207.68.169.170/contoso

Internet Explorer has determine other sites and attempt to trick

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

Report that this is not a phishing website.

Active (IE)

Reported Web Forgery!

This web site at www.mozilla.com has been reported as a web forgery and has been blocked based on your security preferences.

Web forgeries are designed to trick you into revealing personal or financial information by imitating sources you may trust.

Entering any information on this web page may result in identity theft or other fraud.

Get me out of here!

Why was this site blocked?

Ignore this warning

Active (Firefox)

[Egelman et al.]

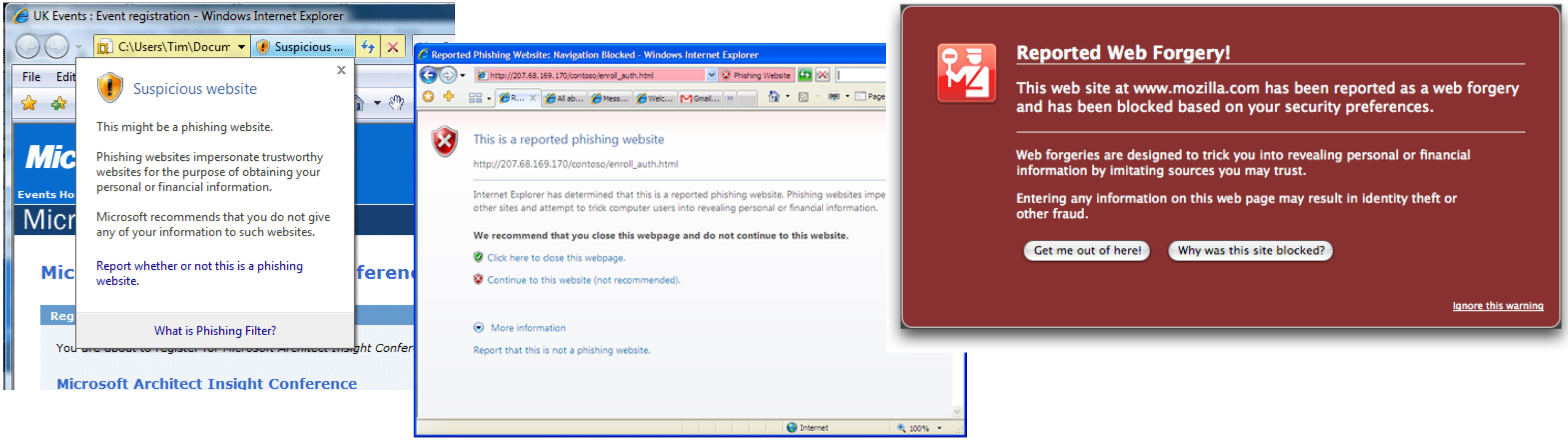
Are Phishing Warnings Effective?

- 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



UK Events : Event registration - Windows Internet Explorer

Suspicious website

This might be a phishing website.

Phishing websites impersonate trustworthy websites for the purpose of obtaining your personal or financial information.

Microsoft recommends that you do not give any of your information to such websites.

Report whether or not this is a phishing website.

What is Phishing Filter?

Reported Phishing Website: Navigation Blocked - Windows Internet Explorer

http://207.68.169.170/contoso/enroll_auth.html

This is a reported phishing website

http://207.68.169.170/contoso/enroll_auth.html

Internet Explorer has determined that this is a reported phishing website. Phishing websites impe
other sites and attempt to trick computer users into revealing personal or financial information.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

Report that this is not a phishing website.

Reported Web Forgery!

This web site at www.mozilla.com has been reported as a web forgery and has been blocked based on your security preferences.

Web forgeries are designed to trick you into revealing personal or financial information by imitating sources you may trust.

Entering any information on this web page may result in identity theft or other fraud.

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

[Egelman et al.]

User Response to Warnings

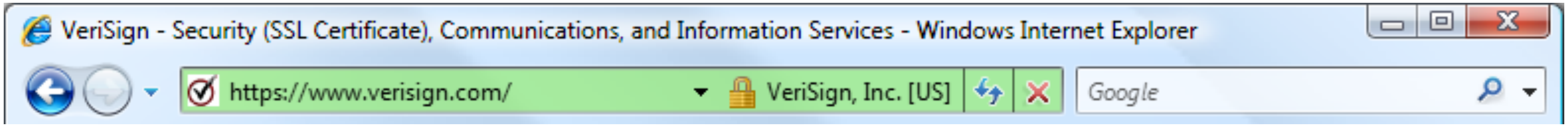
- Some fail to notice warnings entirely
  - Passive warning takes a couple of seconds to appear; if user starts typing, his keystrokes dismiss the warning
- Some saw the warning, closed the window, went back to email, clicked links again, were presented with the same warnings… repeated 4-5 times
  - 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”

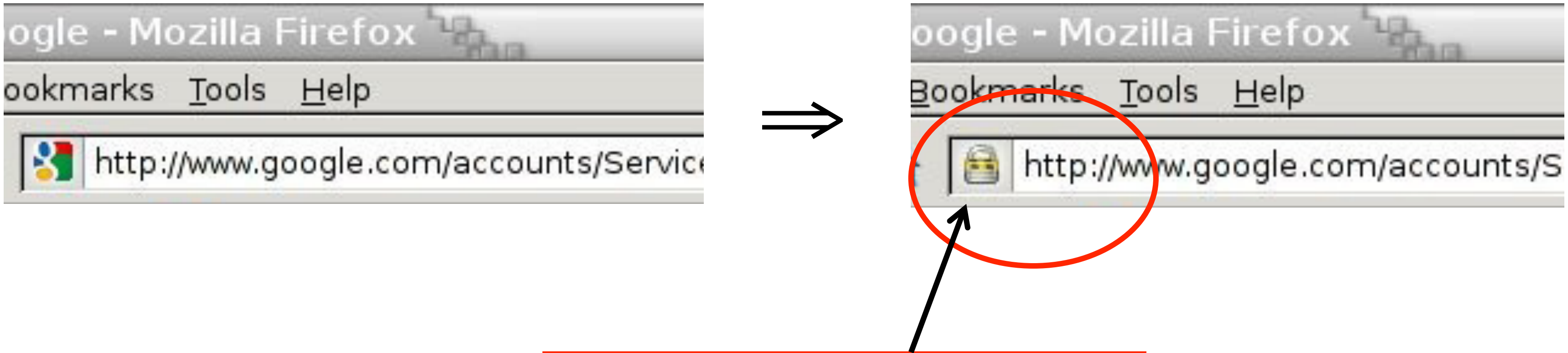
The Lock Icon


VeriSign - Security (SSL Certificate), Communications, and Information Services - Windows Internet Explorer
https://www.verisign.com/
VeriSign, Inc. [US]
Google

- Goal: identify secure connection
  - SSL/TLS is being used between client and server to protect against active network attacker
- Lock icon should only be shown when the page is secure against network attacker
  - Semantics subtle and not widely understood by users
  - Whose certificate is it??
  - Problem in user interface design

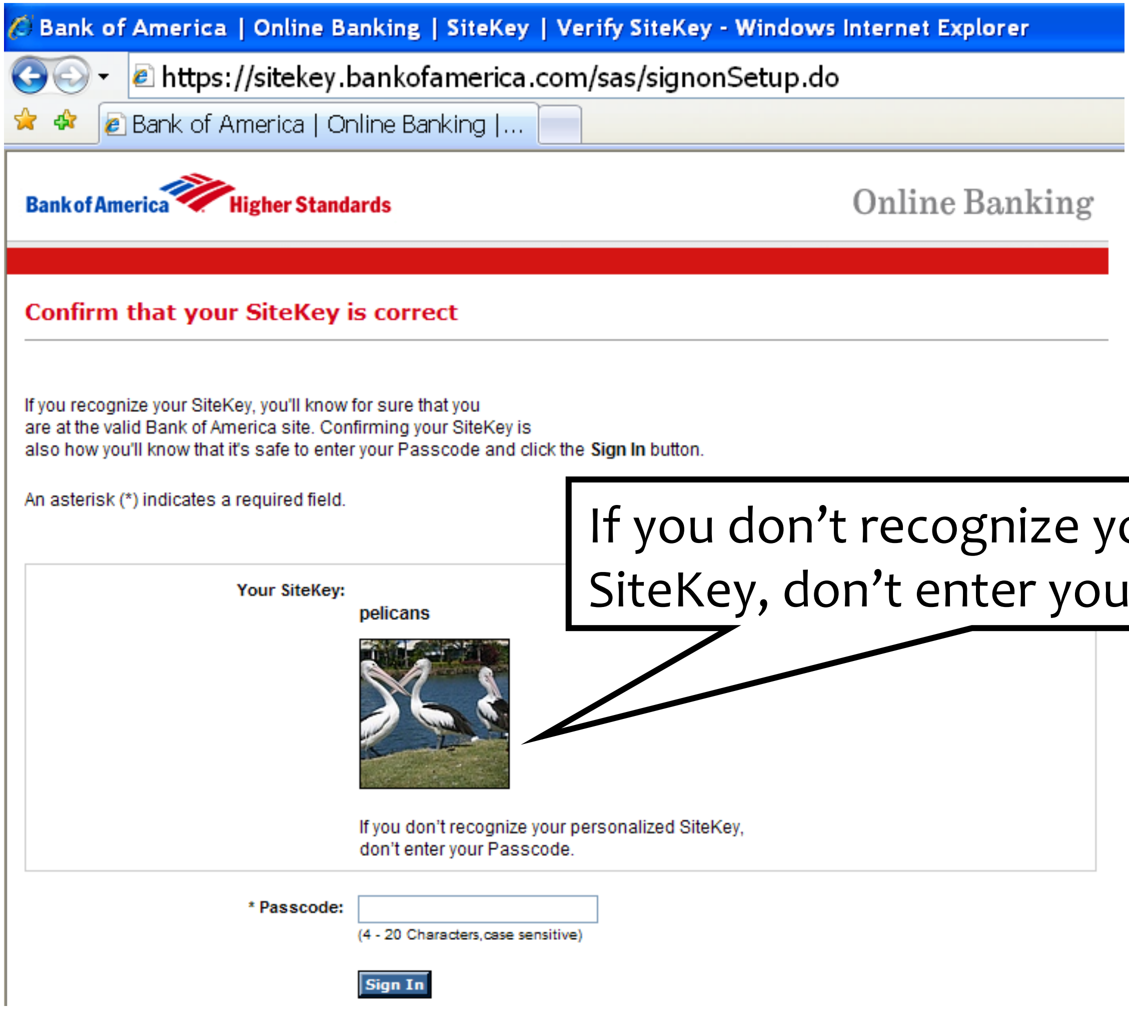
[Moxie Marlinspike]

Will You Notice?



Clever favicon inserted by network attacker

Site Authentication Image (SiteKey)



Bank of America | Online Banking | SiteKey | Verify SiteKey - Windows Internet Explorer
https://sitekey.bankofamerica.com/sas/signonSetup.do
Bank of America | Online Banking |...
Bank of America Higher Standards
Online Banking

Confirm that your SiteKey is correct

If you recognize your SiteKey, you'll know for sure that you are at the valid Bank of America site. Confirming your SiteKey is also how you'll know that it's safe to enter your Passcode and click the **Sign In** button.

An asterisk (*) indicates a required field.

Your SiteKey: pelicans

If you don't recognize your personalized SiteKey, don't enter your Passcode.

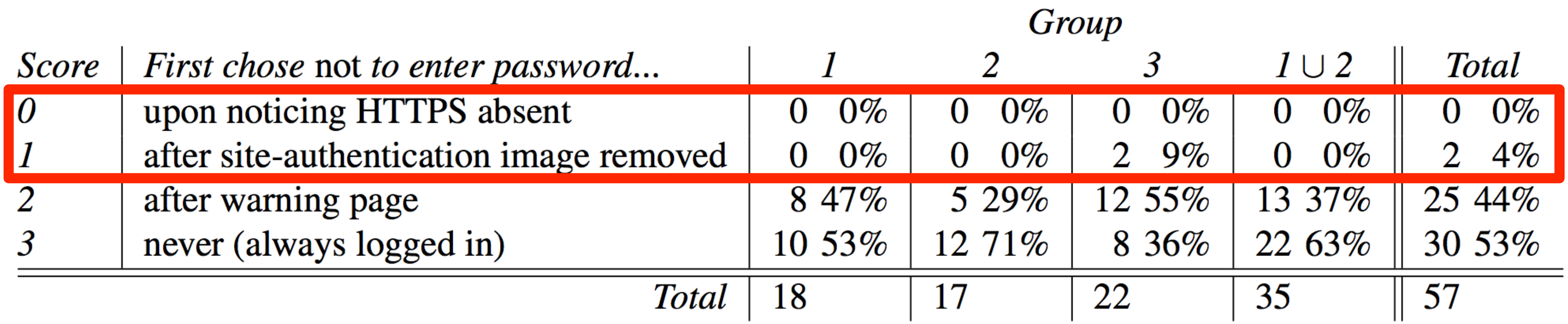
* Passcode:

(4 - 20 Characters, case sensitive)

If you don’t recognize your personalized SiteKey, don’t enter your Passcode

Do These Indicators Help?

- "The Emperor's New Security Indicators"
  - http://www.usablesecurity.org/emperor/emperor.pdf



		Group									
Score	*First chose* not *to enter password...*	*1*		*2*		*3*		*1* ∪ *2*		*Total*	
0	upon noticing HTTPS absent	0	0%	0	0%	0	0%	0	0%	0	0%
1	after site-authentication image removed	0	0%	0	0%	2	9%	0	0%	2	4%
2	after warning page	8	47%	5	29%	12	55%	13	37%	25	44%
3	never (always logged in)	10	53%	12	71%	8	36%	22	63%	30	53%
	Total	18		17		22		35		57	

Users don't notice the **absence** of indicators!

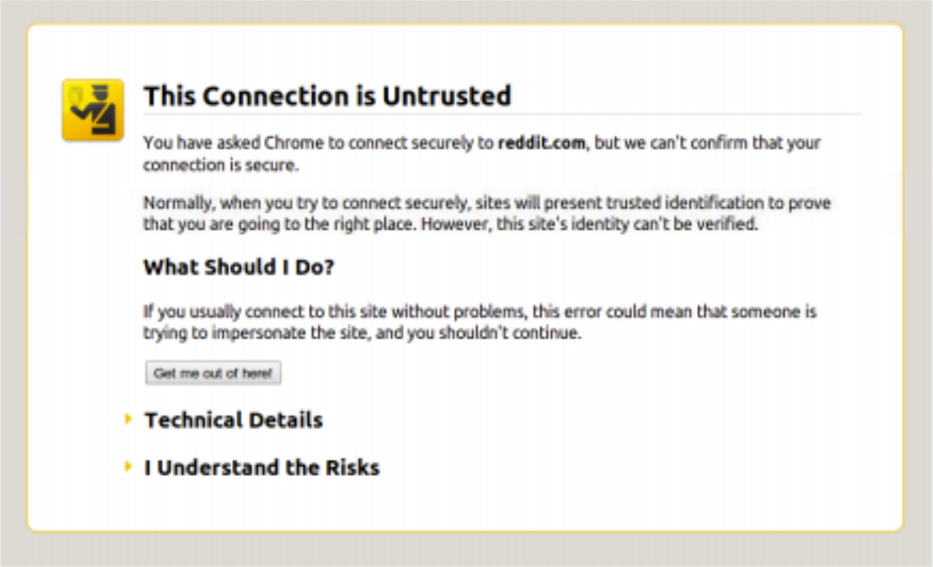
Case Study #2: Browser SSL Warnings

- Design question: How to alert the user if a site's SSL certificate is untrusted?

[Felt et al.]

Firefox vs. Chrome Warning

33% vs. 70% clickthrough rate



This Connection is Untrusted

You have asked Chrome to connect securely to **reddit.com**, but we can't confirm that your connection is secure.

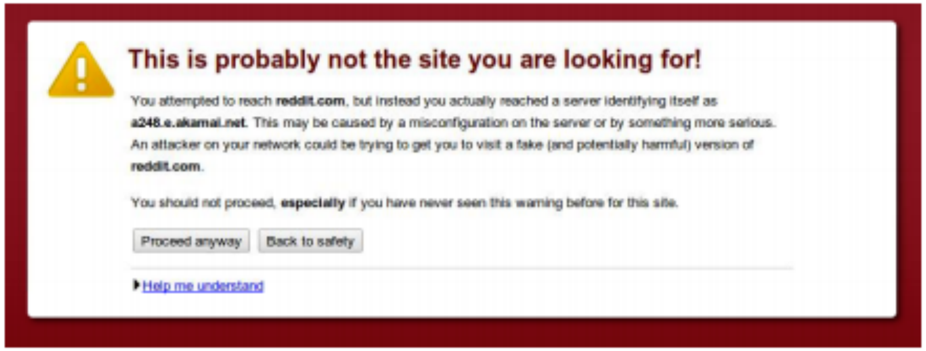
Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Technical Details

I Understand the Risks



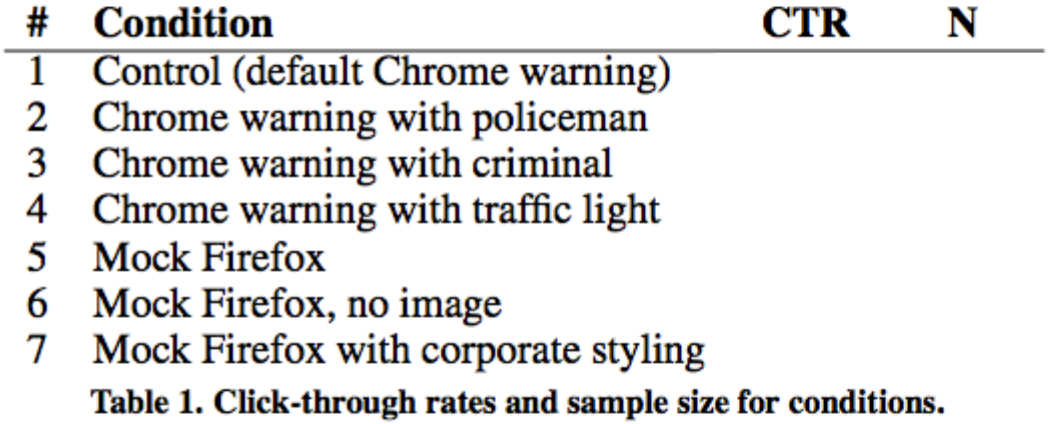
This is probably not the site you are looking for!

You attempted to reach **reddit.com**, but instead you actually reached a server identifying itself as **a248.e.akamai.net**. This may be caused by a misconfiguration on the server or by something more serious. An attacker on your network could be trying to get you to visit a fake (and potentially harmful) version of **reddit.com**.

You should not proceed, **especially** if you have never seen this warning before for this site.

[Felt et al.]

Experimenting w/ Warning Design



#	Condition	CTR	N
1	Control (default Chrome warning)		
2	Chrome warning with policeman		
3	Chrome warning with criminal		
4	Chrome warning with traffic light		
5	Mock Firefox		
6	Mock Firefox, no image		
7	Mock Firefox with corporate styling		

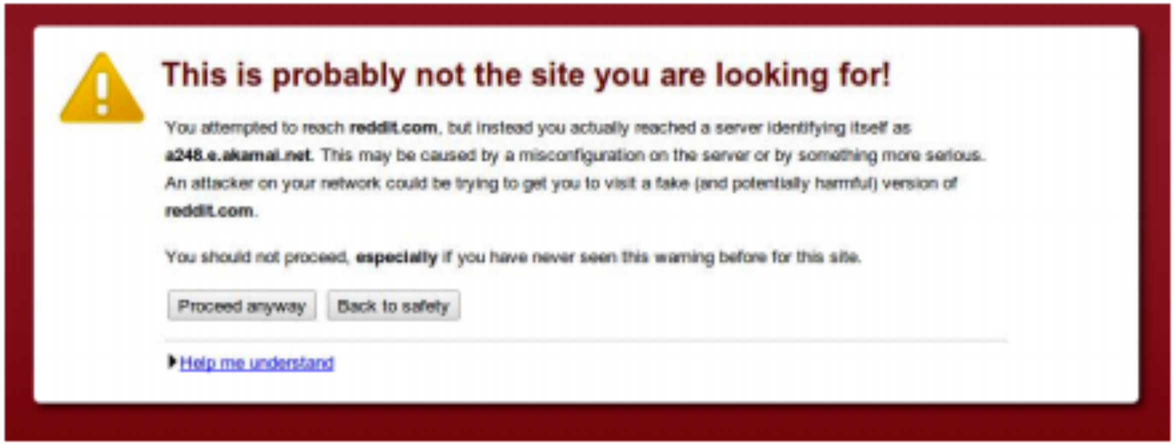
Table 1. Click-through rates and sample size for conditions.

[Felt et al.]

Experimenting w/ Warning Design

#	Condition	CTR	N
1	Control (default Chrome warning)	67.9%	17,479
2	Chrome warning with policeman		
3	Chrome warning with criminal		
4	Chrome warning with traffic light		
5	Mock Firefox		
6	Mock Firefox, no image		
7	Mock Firefox with corporate styling		

Table 1. Click-through rates and sample size for conditions.



This is probably not the site you are looking for!

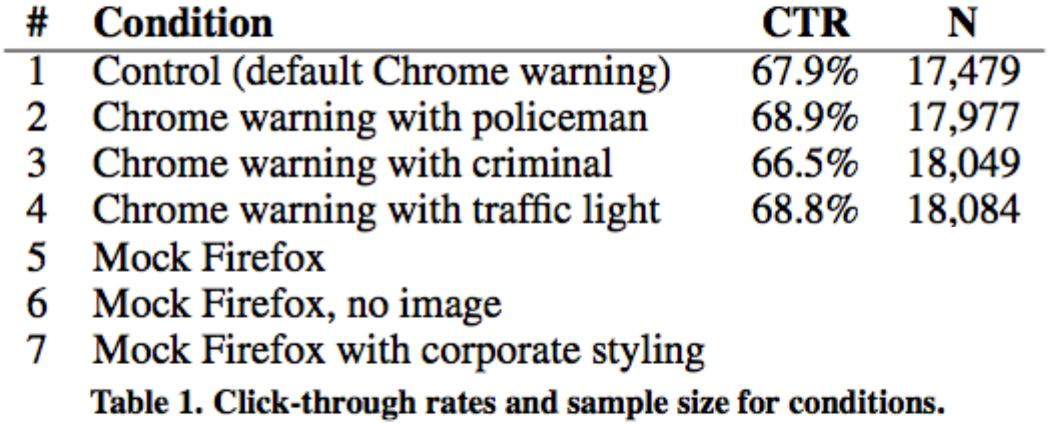
You attempted to reach **reddit.com**, but instead you actually reached a server identifying itself as **a248.e.akamai.net**. This may be caused by a misconfiguration on the server or by something more serious. An attacker on your network could be trying to get you to visit a fake (and potentially harmful) version of **reddit.com**.

You should not proceed, **especially** if you have never seen this warning before for this site.

Figure 1. The default Chrome SSL warning (Condition 1).

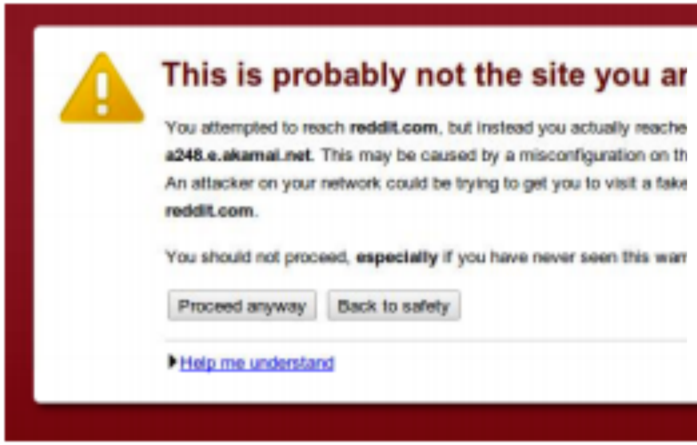
[Felt et al.]

Experimenting w/ Warning Design



#	Condition	CTR	N
1	Control (default Chrome warning)	67.9%	17,479
2	Chrome warning with policeman	68.9%	17,977
3	Chrome warning with criminal	66.5%	18,049
4	Chrome warning with traffic light	68.8%	18,084
5	Mock Firefox		
6	Mock Firefox, no image		
7	Mock Firefox with corporate styling		

Table 1. Click-through rates and sample size for conditions.



This is probably not the site you ar

You attempted to reach **reddit.com**, but instead you actually reache **a248.e.akamai.net**. This may be caused by a misconfiguration on th An attacker on your network could be trying to get you to visit a fake **reddit.com**.

You should not proceed, **especially** if you have never seen this war

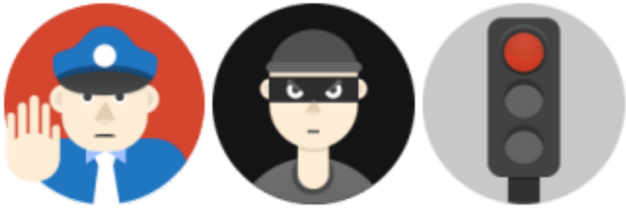


Figure 4. The three images used in Conditions 2-4.

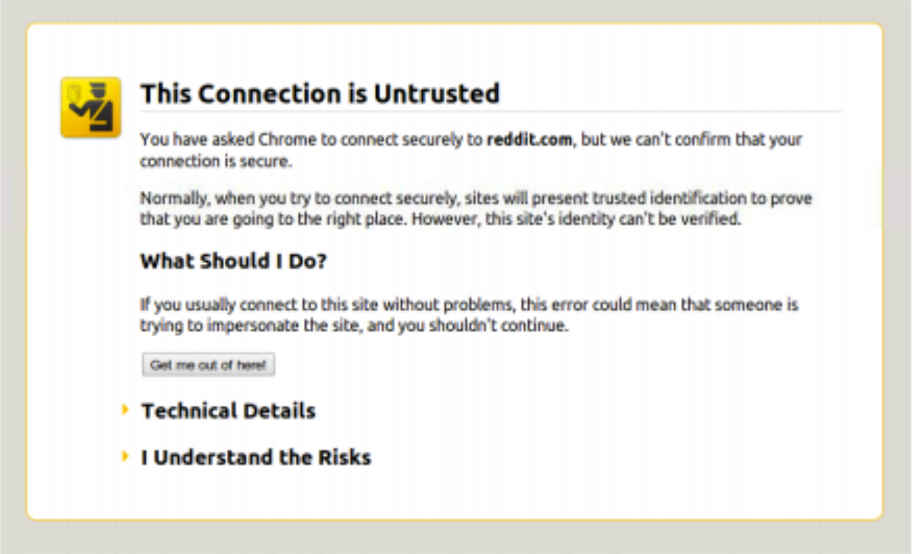
Figure 1. The default Chrome SSL warning (Condition 1).

[Felt et al.]

Experimenting w/ Warning Design

#	Condition	CTR	N
1	Control (default Chrome warning)	67.9%	17,479
2	Chrome warning with policeman	68.9%	17,977
3	Chrome warning with criminal	66.5%	18,049
4	Chrome warning with traffic light	68.8%	18,084
5	Mock Firefox	56.1%	20,023
6	Mock Firefox, no image	55.9%	19.297
7	Mock Firefox with corporate styling		

Table 1. Click-through rates and sample size for conditions.



This Connection is Untrusted

You have asked Chrome to connect securely to **reddit.com**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

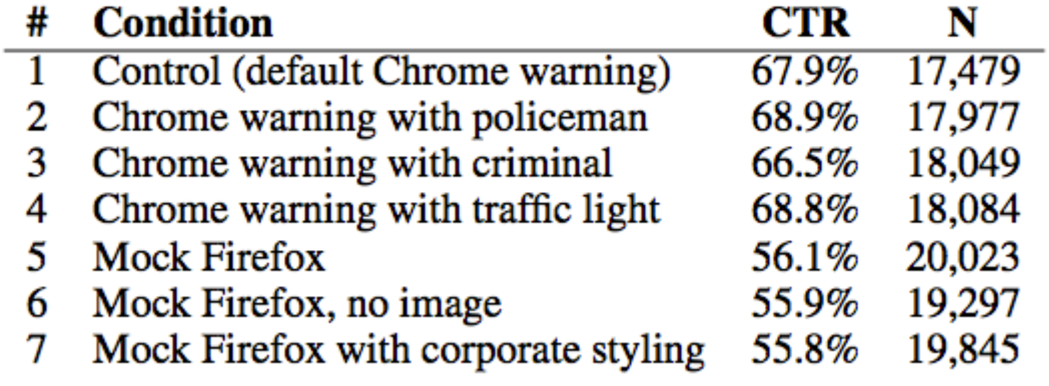
Get me out of here!

- **Technical Details**
- **I Understand the Risks**

Figure 2. The mock Firefox SSL warning (Condition 5).

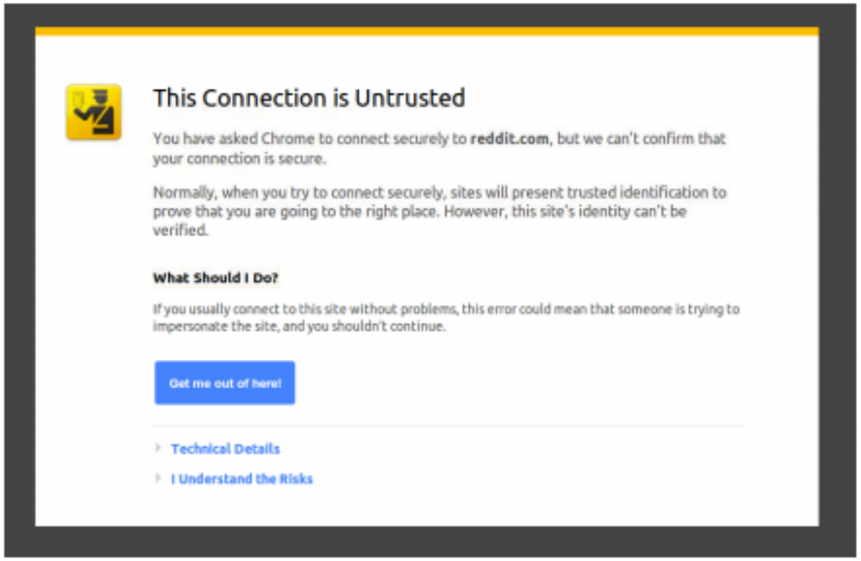
[Felt et al.]

Experimenting w/ Warning Design



#	Condition	CTR	N
1	Control (default Chrome warning)	67.9%	17,479
2	Chrome warning with policeman	68.9%	17,977
3	Chrome warning with criminal	66.5%	18,049
4	Chrome warning with traffic light	68.8%	18,084
5	Mock Firefox	56.1%	20,023
6	Mock Firefox, no image	55.9%	19,297
7	Mock Firefox with corporate styling	55.8%	19,845

Table 1. Click-through rates and sample size for conditions.



This Connection is Untrusted

You have asked Chrome to connect securely to **reddit.com**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

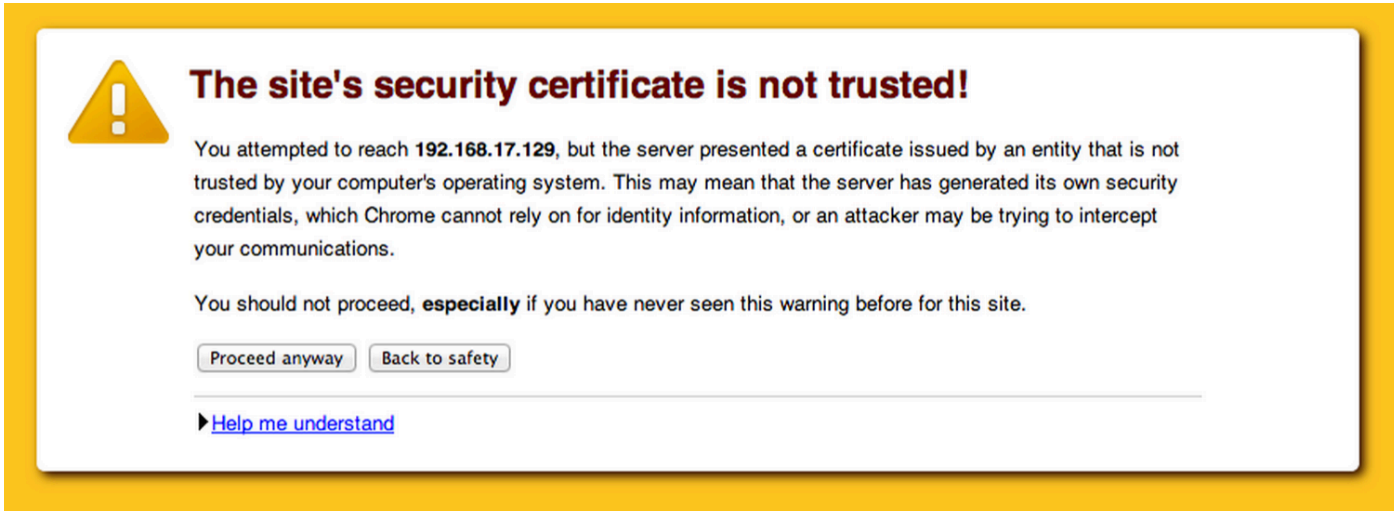
What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Figure 3. The Firefox SSL warning with Google styling (Condition 7).

[Felt et al.]

Opinionated Design Helps!



The site's security certificate is not trusted!

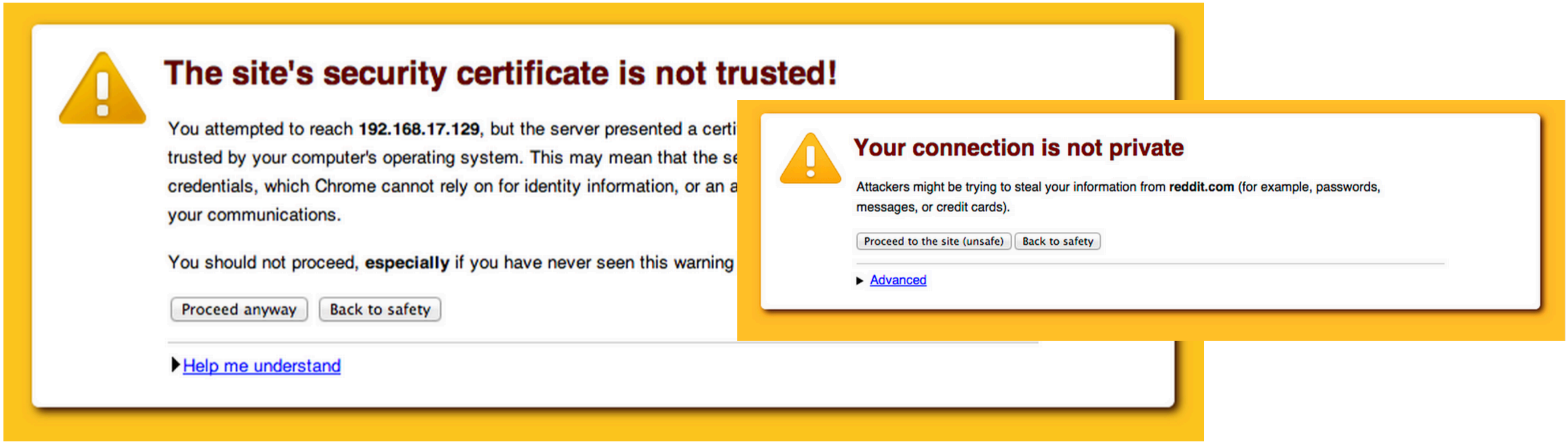
You attempted to reach **192.168.17.129**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications.

You should not proceed, **especially** if you have never seen this warning before for this site.

Adherence	N
30.9%	4,551

[Felt et al.]

Opinionated Design Helps!



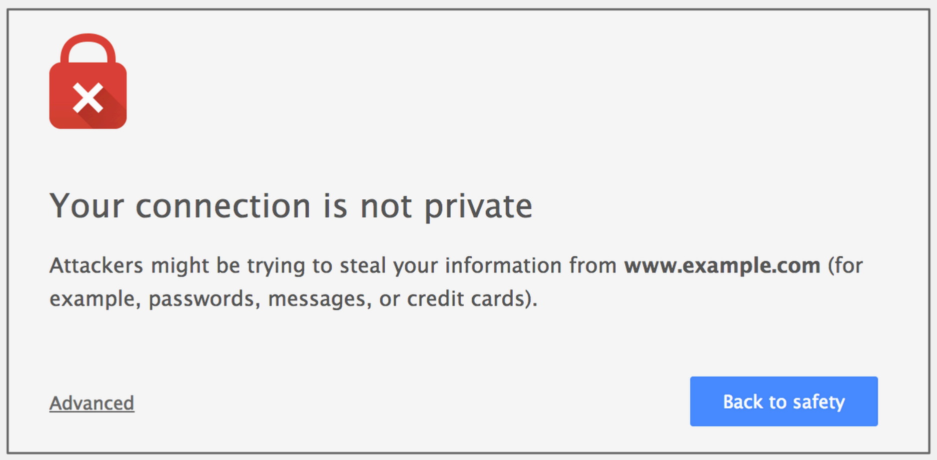
The site's security certificate is not trusted!

You attempted to reach **192.168.17.129**, but the server presented a certi trusted by your computer's operating system. This may mean that the se credentials, which Chrome cannot rely on for identity information, or an a your communications.

You should not proceed, **especially** if you have never seen this warning

Your connection is not private

Attackers might be trying to steal your information from **reddit.com** (for example, passwords, messages, or credit cards).



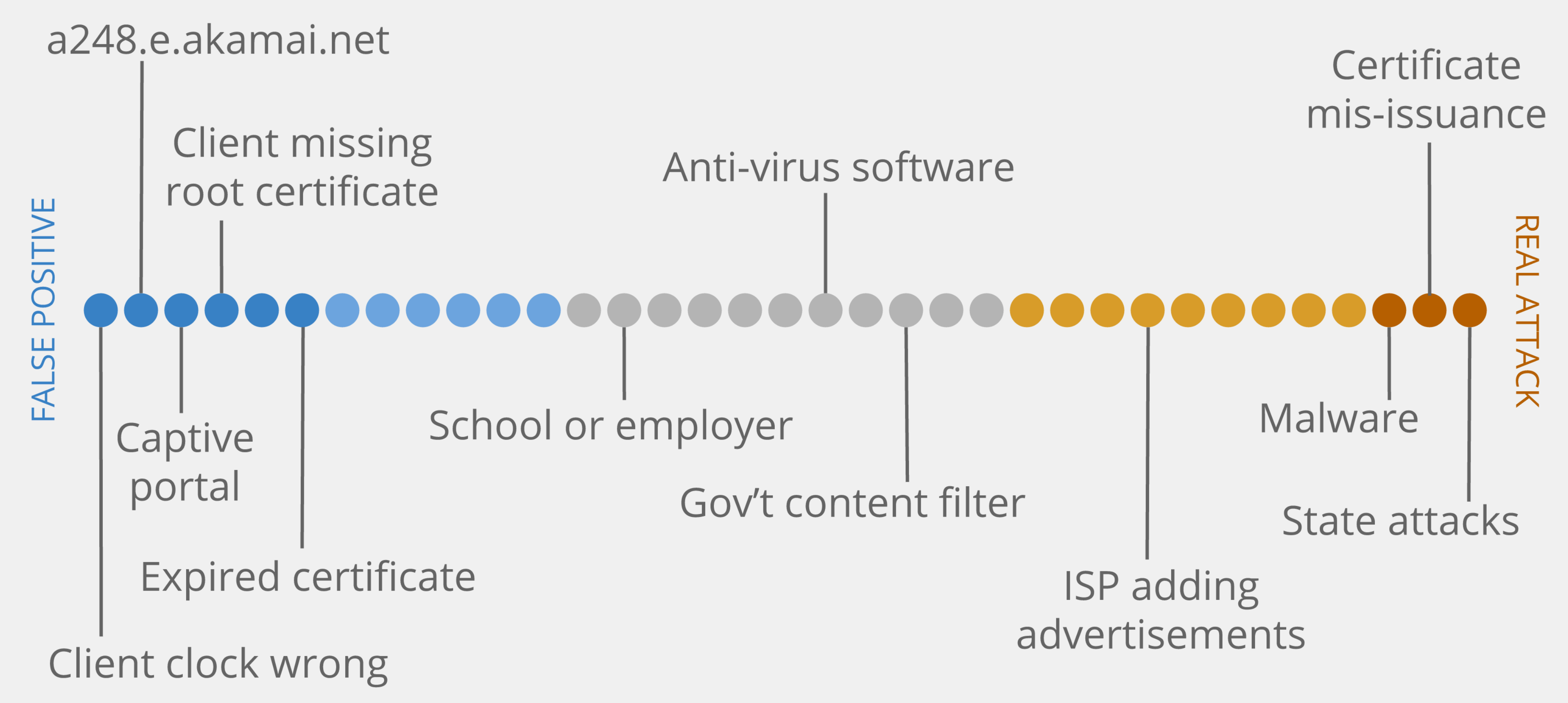
Your connection is not private

Attackers might be trying to steal your information from **www.example.com** (for example, passwords, messages, or credit cards).

Adherence	N
30.9%	4,551
32.1%	4,075
58.3%	4,644

[Felt et al.]

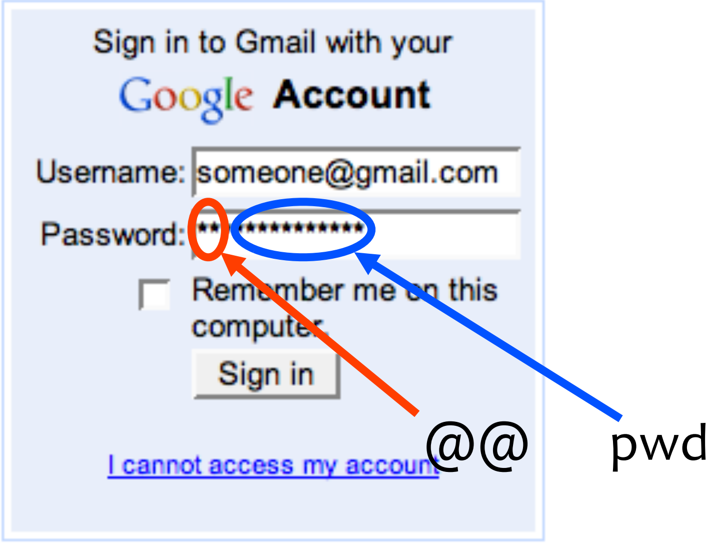
Challenge: Meaningful Warnings



Case Study #3: Password Managers

- Password managers handle creating and "remembering" strong passwords
- Potentially:
  - **Easier** for users
  - More **secure**
- Examples:
  - PwdHash (Usenix Security 2005)
  - Password Multiplier (WWW 2005)

PwdHash



Sign in to Gmail with your Google Account

Username: someone@gmail.com

Password: **************

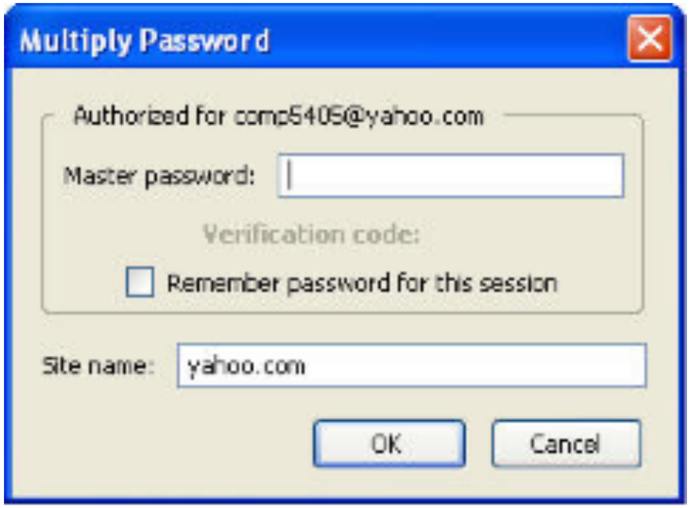
□ Remember me on this computer

@@ in front of passwords to protect; or F2

sitePwd = Hash(pwd,domain)

Prevent phishing attacks

Password Multiplier



Multiply Password

Authorized for comp5405@yahoo.com

Master password:

Verification code:

□ Remember password for this session

Site name: yahoo.com

Activate with Alt-P or double-click

sitePwd = Hash(username, pwd, domain)

Both solutions target simplicity and transparency.

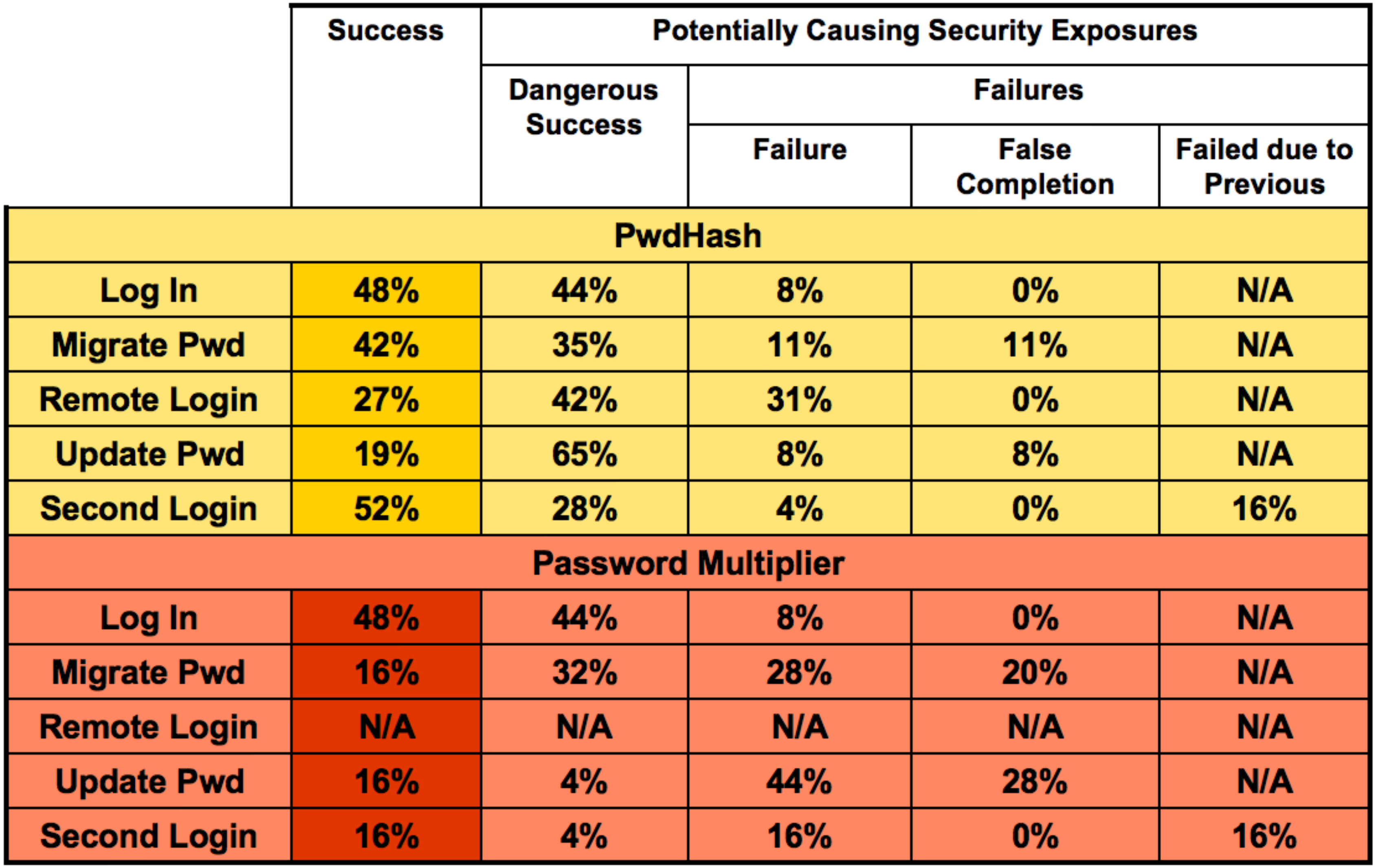
[Chiasson, van Oorschot, Biddle]

Usability Testing

- Are these programs usable? If not, what are the problems?
- Two main approaches for evaluating usability:
  - Usability inspection (no users)
    - Cognitive walkthroughs
    - Heuristic evaluation
  - User study
    - Controlled experiments
    - Real usage

[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.
  - Theme in course: sometimes things designed to increase security can also increase other risks

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.

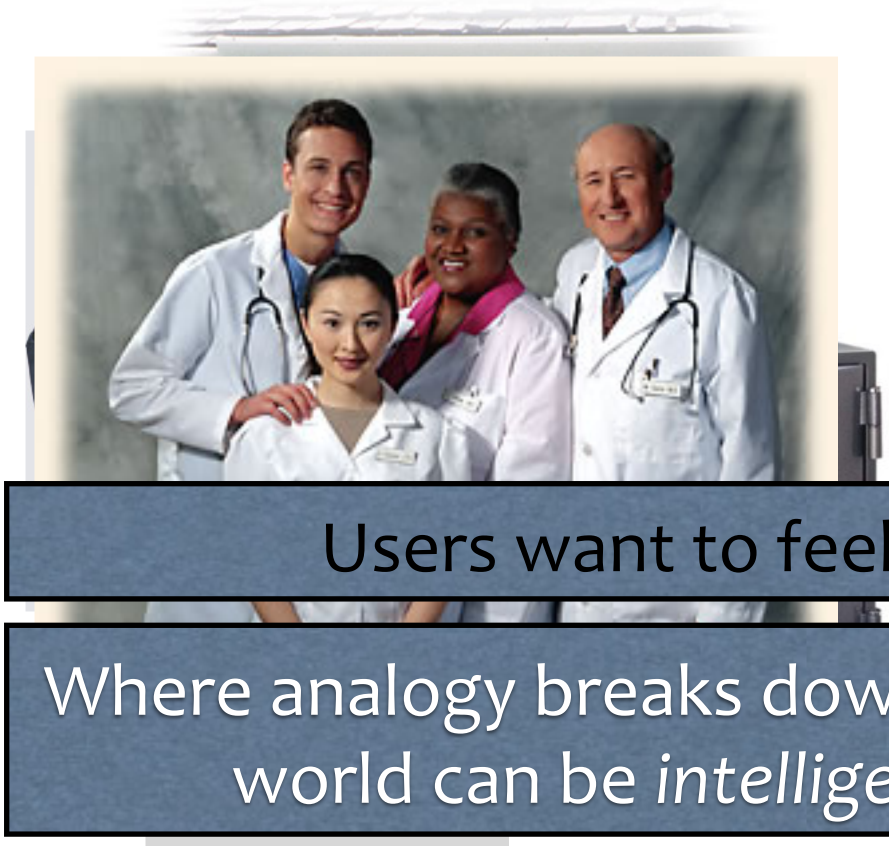
Issue #1: Complexities, Lack of Intuition

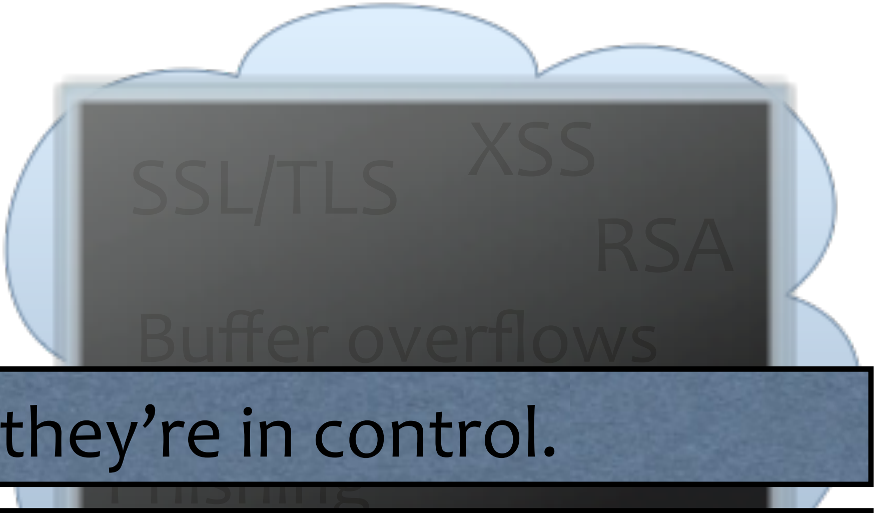
- Mismatch between perception of technology and what really happens
  - Public keys?
  - Signatures?
  - Encryption?
  - Message integrity?
  - Chosen-plaintext attacks?
  - Chosen-ciphertext attacks?
  - Password management?
  - …

Issue #2: Who's in Charge?

Real World

Electronic World





Users want to feel like they're in control.

Where analogy breaks down: *Adversaries* in the electronic world can be *intelligent*, *sneaky*, and *malicious*.

Complex, hidden, but *doctors manage*

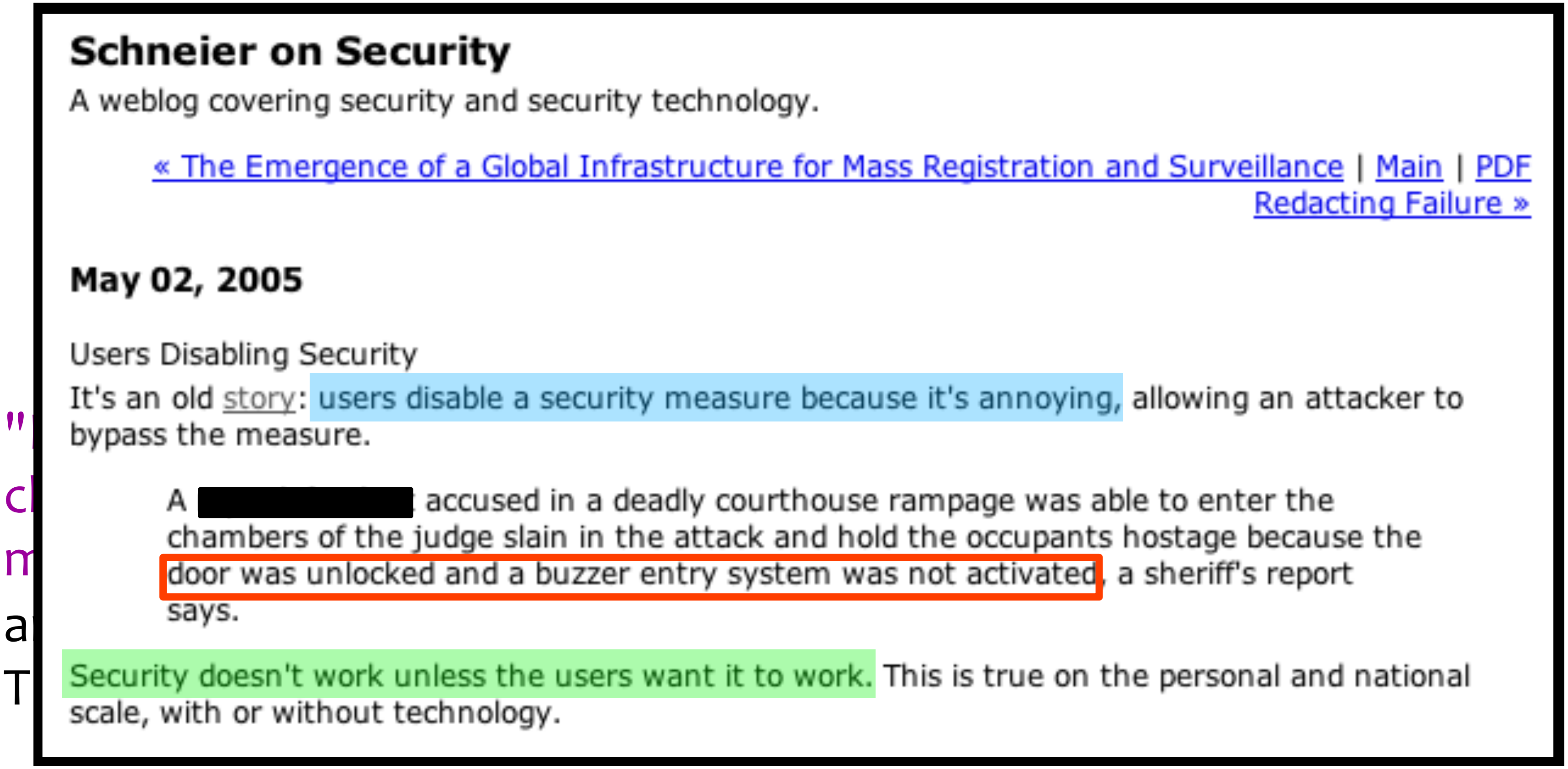
Complex, hidden, and *users manage*

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.)



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.

"I
cl
m
a
T

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?"

Issues with Usability

1. Lack of intuition
   – See a safe, understand threats. Not true for computers.
2. Who’s in charge?
   – Doctors keep your medical records safe, you manage your passwords.
3. Hard to gauge risks
   – “It would never happen to me!”
4. No accountability
   – Asset-holder is not the only one you can lose assets.
5. Awkward, annoying, or difficult
6. Social issues

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 solution

Response #2: Security Should Be Invisible

- Security should happen
  - Naturally
  - By Default
  - Without user input or understanding

- Recognize and stop bad actions
- Starting to see some invisibility
  - SSL/TLS
  - VPNs
  - Automatic Security Updates
  - User-driven access control

Response #2: Security Should Be Invisible

- "Easy" at extremes, or for simple examples
  - Don't give everyone access to everything

- But hard to generalize

- Leads to things not working for reasons user doesn't understand
- Users will then try to get the system to work, possibly further <u>reducing</u> security
  - E.g., "dangerous successes" for password managers

Response #3: “3 Word UI”: “Are You Sure?”

- Security should be invisible
  - Except when the user tries something dangerous
  - In which case a warning is given
- But how do users evaluate the warning? Two realistic cases:
  - Always heed warning. But see problems / commonality with Response #2 (“security should be invisible”)
  - Always ignore the warning. If so, then how can it be effective?

Response #4: Focus on Users, Use Metaphors

- Clear, understandable metaphors:
  - Physical analogs; e.g., red-green lights
- User-centered design: Start with user model
- Unified 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