

CSE 484 / CSE M 584: Computer Security and Privacy

Usable Security

Spring 2020

Franziska (Franzi) Roesner
franzi@cs.washington.edu

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

Admin

- Lab 2 due on Friday
- Homework 3 out, due May 29
- There will be a Lab 3 (it is easier than 1+2)
 - Smart home security, preview in Section this week
- This week's lectures:
 - Usable security
 - Mobile platform security
 - Anonymity

Importance of Usability in 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

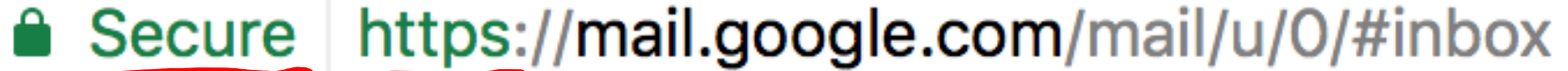
Usable Security Roadmap

- 2 case studies
 - HTTPS indicators + SSL warnings
 - Phishing
- **Step back:** root causes of usability problems, and how to address

Case Study #1: Browser HTTPS Indicators

- **Design question 1:** How to indicate encrypted connections to users?
- **Design question 2:** How to alert the user if a site's SSL certificate is untrusted?

The Lock Icon



- 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

Will You Notice?



Clever favicon inserted by network attacker

Do These Indicators Help? (2007)

- “The Emperor’s New Security Indicators”
 - <http://www.usablesecurity.org/emperor/emperor.pdf>

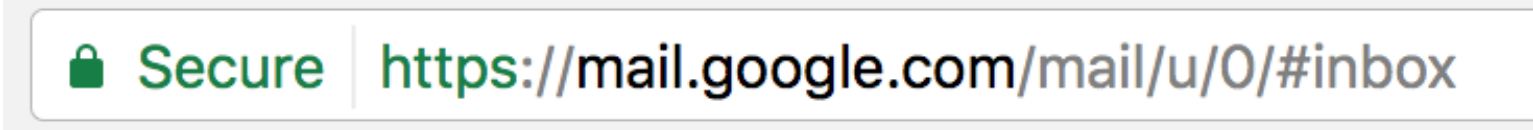
Score	First chose not to enter password...	Group								Total	
		1		2		3		1 ∪ 2			
0	upon noticing HTTPS absent	0	0%	0	0%	0	0%	0	0%	0	0%
1	after site-authentication image removed	0	0%	0	0%	2	9%	0	0%	2	4%
2	after warning page	8	47%	5	29%	12	55%	13	37%	25	44%
3	never (always logged in)	10	53%	12	71%	8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

Lesson:



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

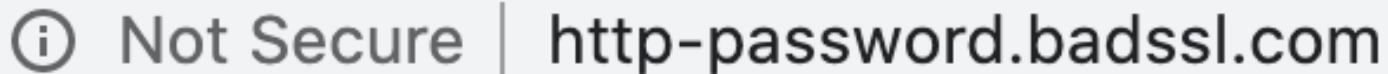
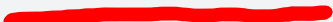
Newer Versions of Chrome

c. 2017

→  Secure | <https://mail.google.com/mail/u/0/#inbox>

2020

  mail.google.com/mail/u/0/#inbox

  Not Secure | http-password.badssl.com

(2017)



Case Study #2: Browser HTTPS Indicators

- **Design question 1:** How to indicate encrypted connections to users?
- **Design question 2:** How to alert the user if a site's SSL certificate is untrusted?

Firefox vs. Chrome Warning

(ignored warning)

33% vs. 70% clickthrough rate

Firefox design



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

2 clicks



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.

Proceed anyway

Back to safety

Help me understand

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.

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.

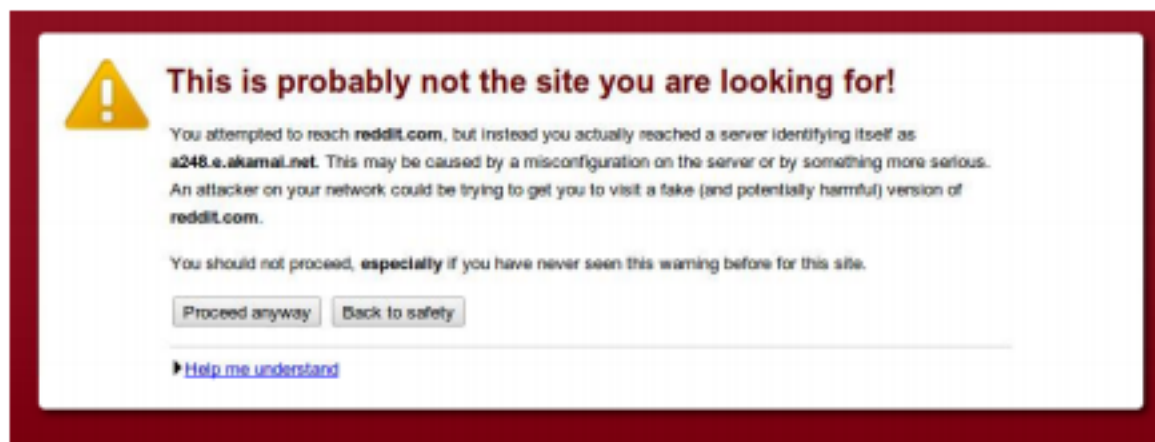


Figure 1. The default Chrome SSL warning (Condition 1).

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.

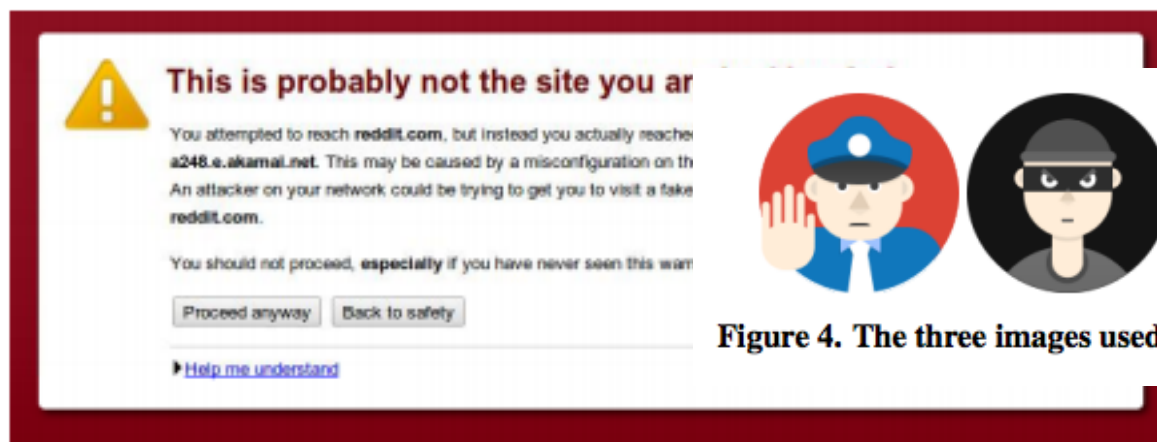


Figure 1. The default Chrome SSL warning (Condition 1).

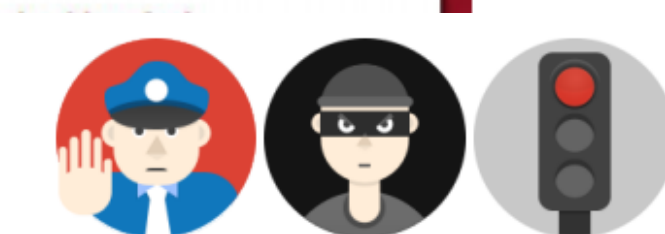


Figure 4. The three images used in Conditions 2-4.

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.

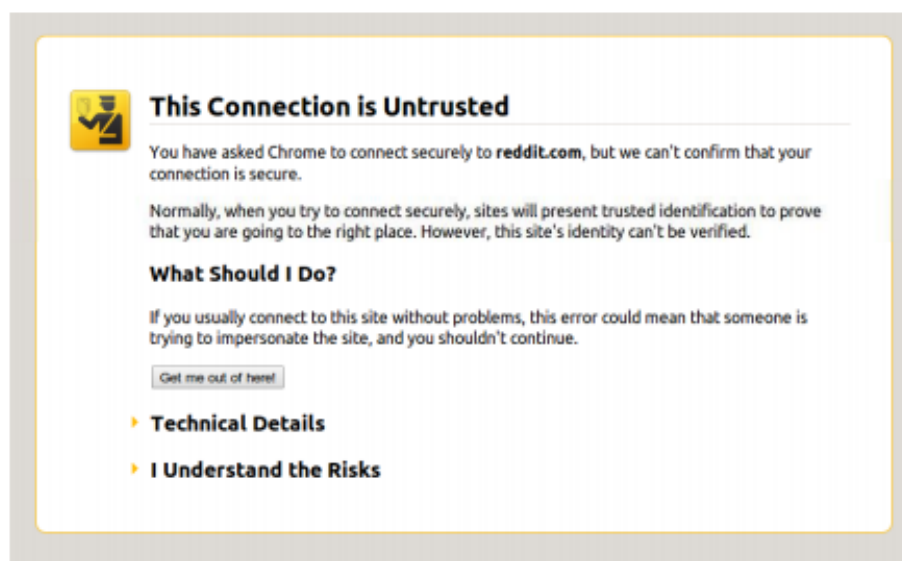
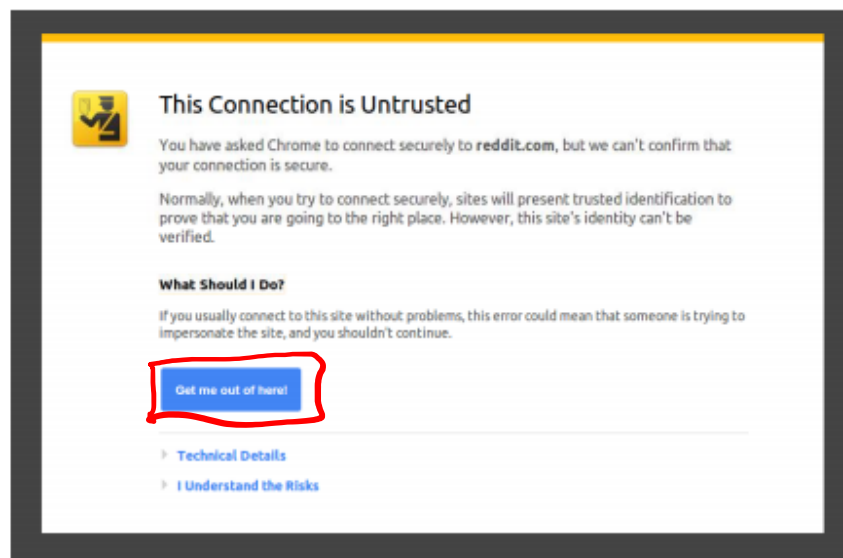


Figure 2. The mock Firefox SSL warning (Condition 5).

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.



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.

Proceed anyway

Back to safety

▶ [Help me understand](#)

Adherence	N
30.9%	4,551

"dark pattern" if goals are bad

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 not trusted by your computer's operating system. This may mean that the server's credentials, which Chrome cannot rely on for identity information, or an attacker intercepted your communications.

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

[Proceed anyway](#) [Back to safety](#)

[Help me understand](#)

Your connection is not private

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

[Proceed to the site \(unsafe\)](#) [Back to safety](#)

[Advanced](#)

Your connection is not private

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

[Advanced](#) [Back to safety](#)

(opposite of firming)

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

Today's Warning



Your connection is not private

Attackers might be trying to steal your information from **untrusted-root.badssl.com** (for example, passwords, messages, or credit cards). [Learn more](#)

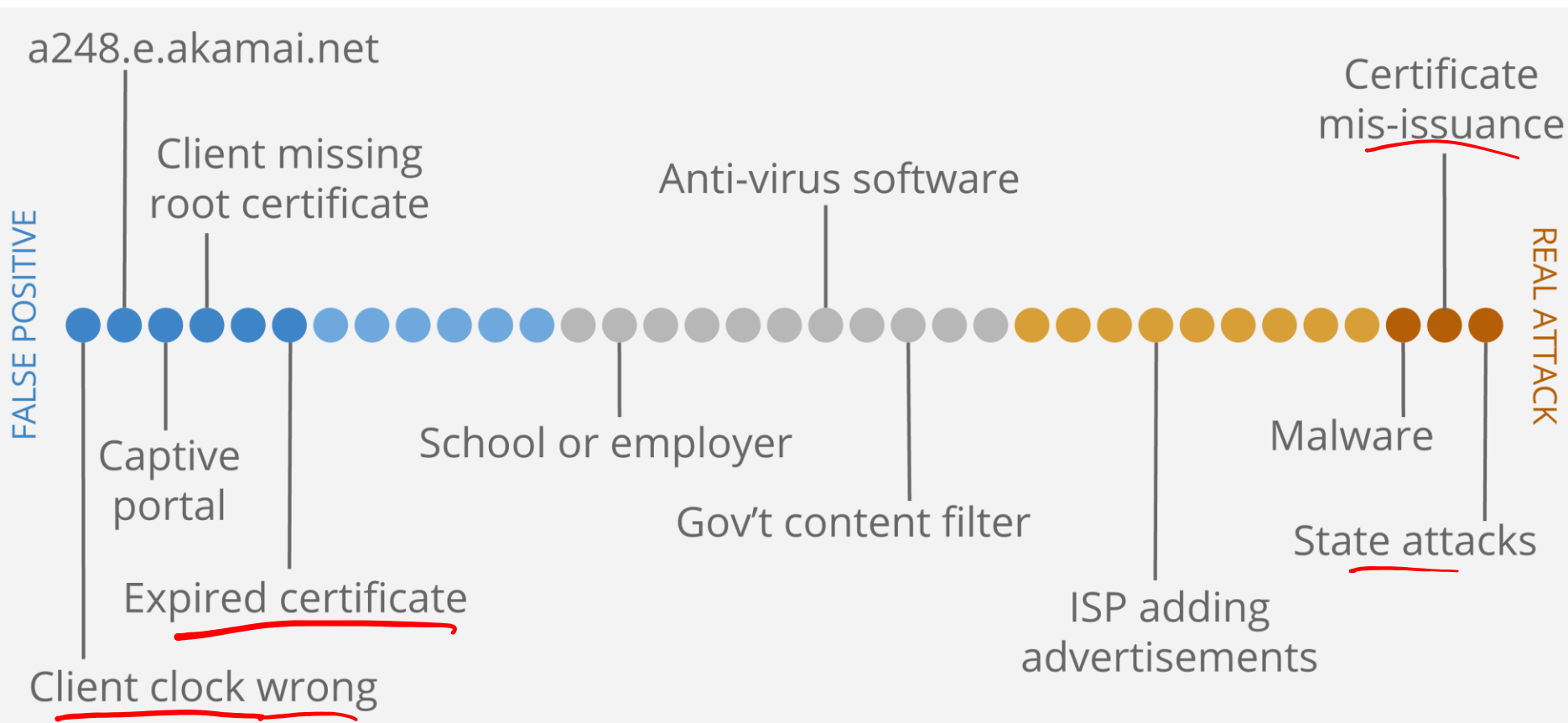
NET::ERR_CERT_INVALID

Help improve Chrome security by sending [URLs of some pages you visit, limited system information, and some page content](#) to Google. [Privacy policy](#).

Advanced

Reload

Challenge: Meaningful Warnings



See current designs for different conditions at <https://badssl.com/>.

Case Study #2: Phishing

- **Design question:** How do you help users avoid falling for phishing sites?

paypal.com

paypal.com, attacker.com

A Typical Phishing Page

PayPal - Welcome

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

PayPal®

Log In | Log In | Help

Welcome Send Auction Tools

Member Log-In [Forgot your email address?](#)
[Forgot your password?](#)

Email Address

Password

Join PayPal Today
Now Over 100 million accounts

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 **eBay Sellers** **Merchants**

[Send money](#) to anyone with an email address in 55 countries and regions.
PayPal is [free](#) for

[Free eBay tools](#) make selling easier.
PayPal works hard to help [protect sellers](#).

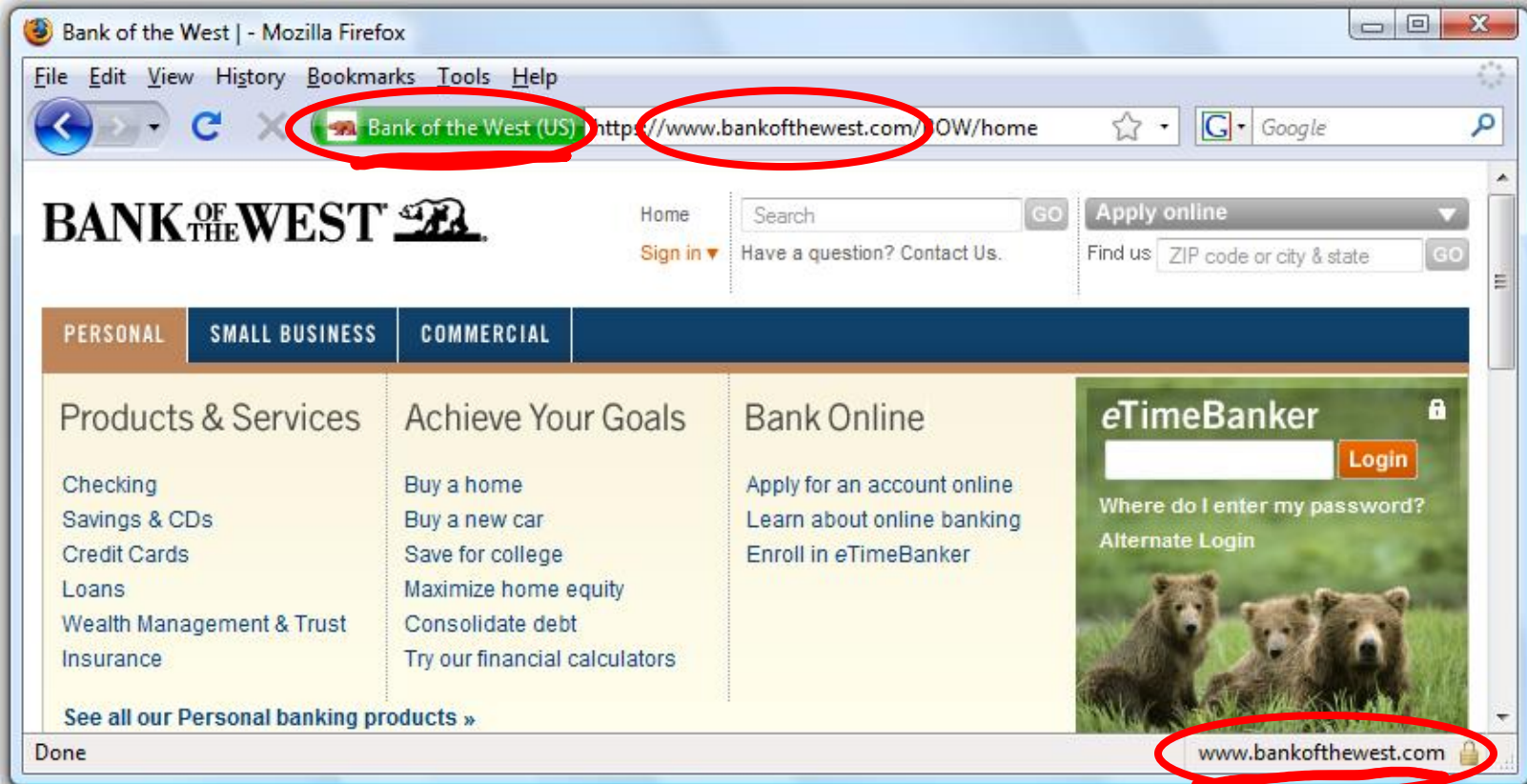
[Accept credit cards](#) on your website using PayPal.
[Compare our solutions](#) to merchant accounts

PayPal Mobile
[Learn more](#)

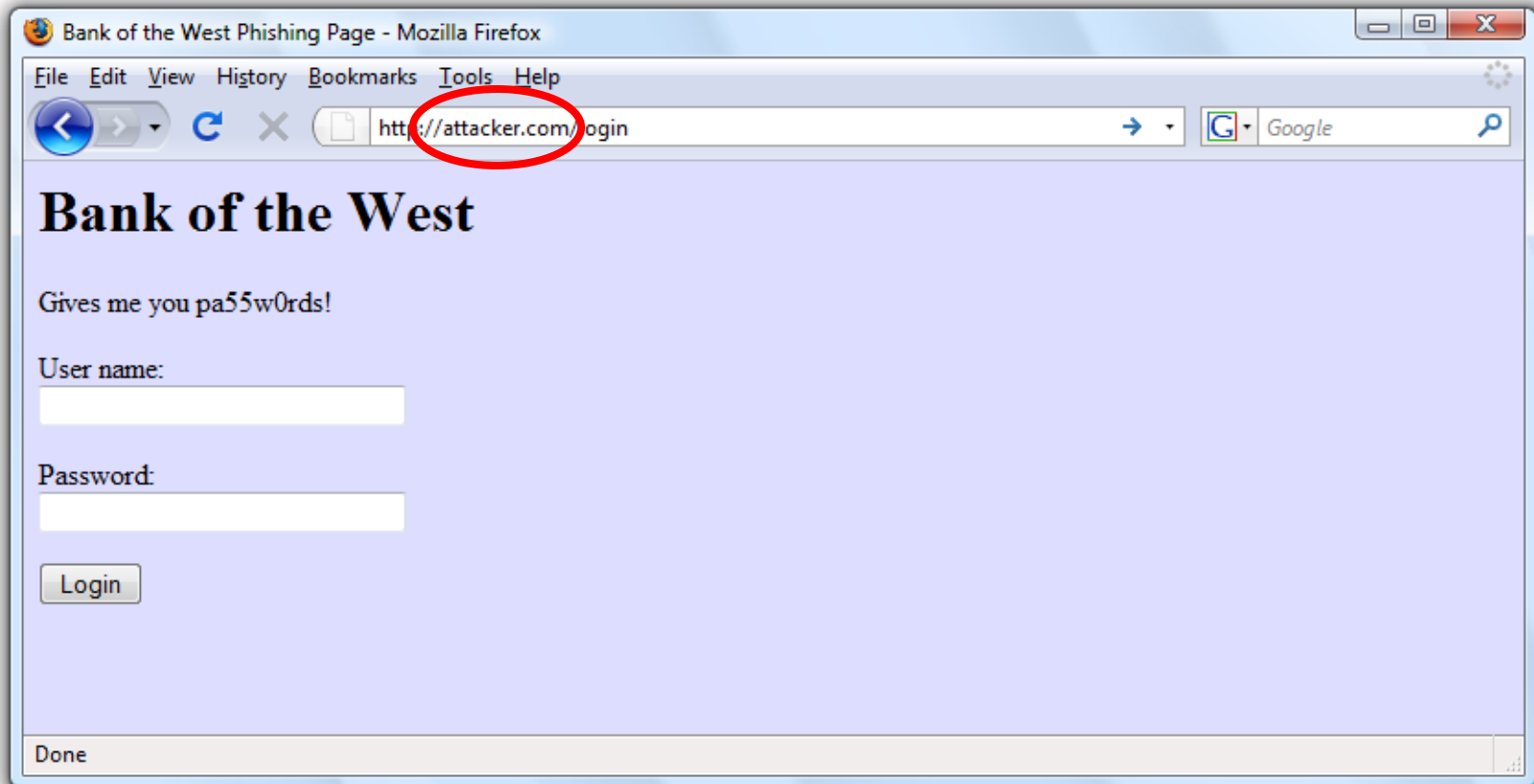
What's New

Safe to Type Your Password?

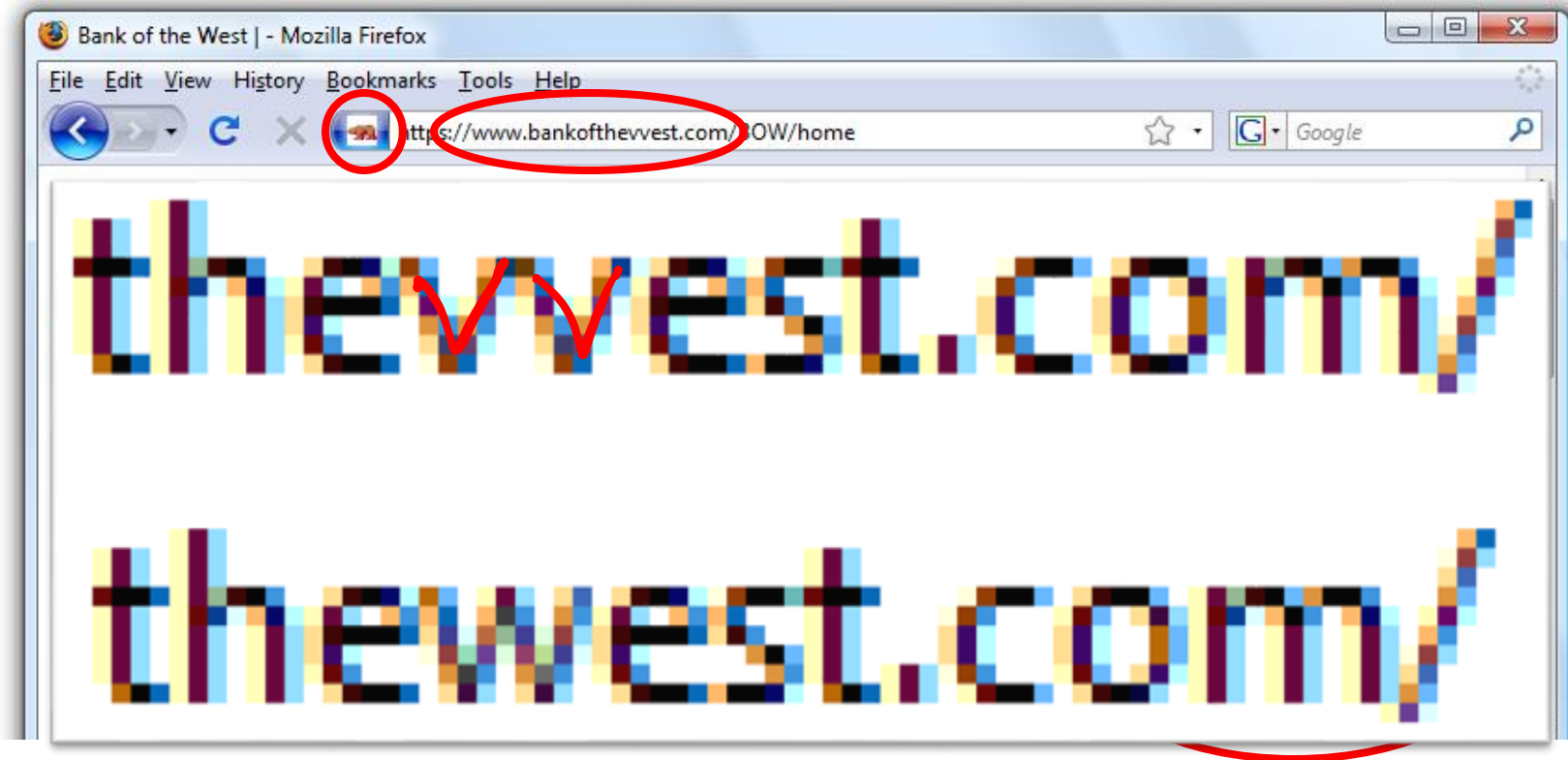
extended validation cert.



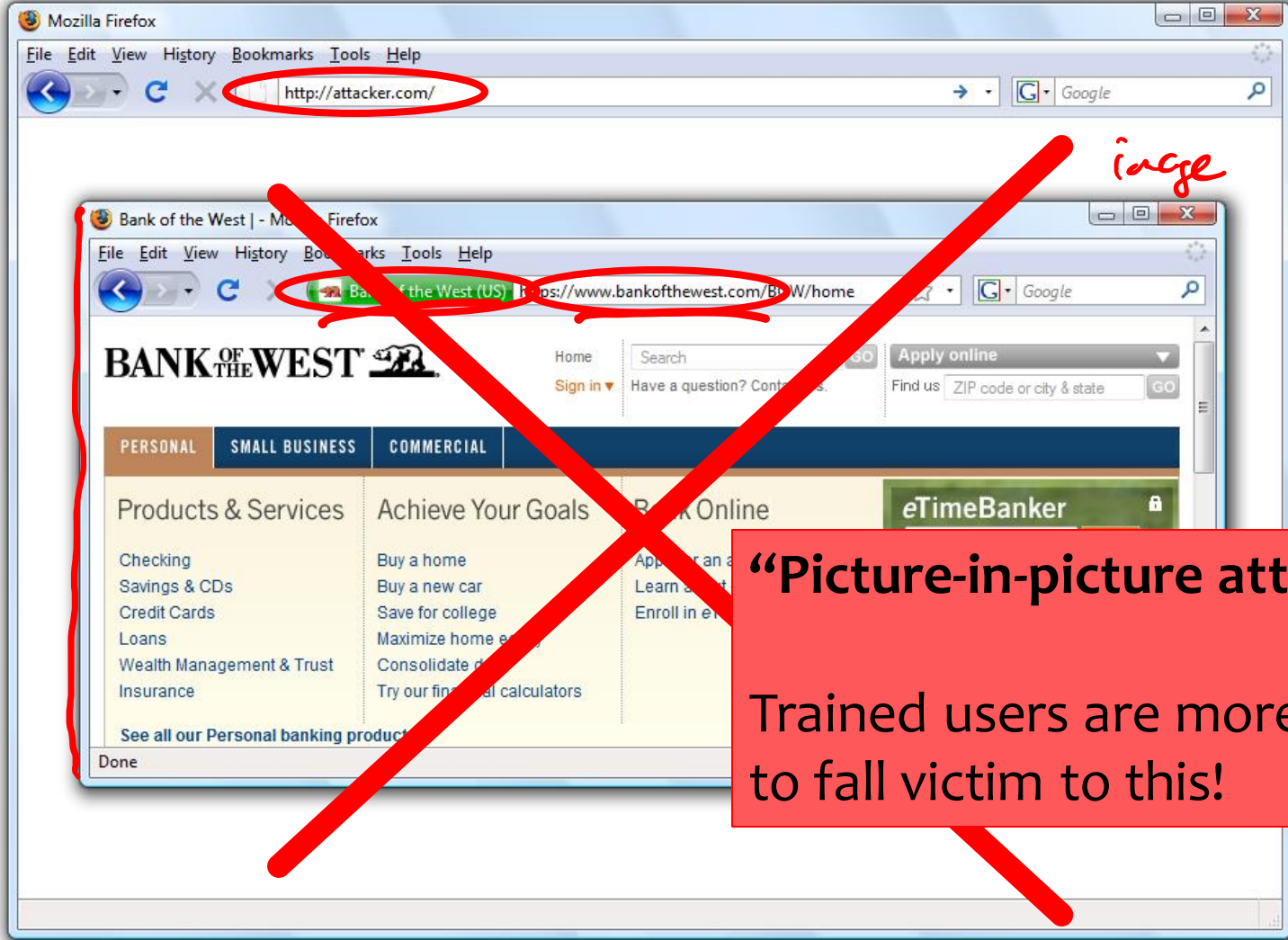
Safe to Type Your Password?



Safe to Type Your Password?



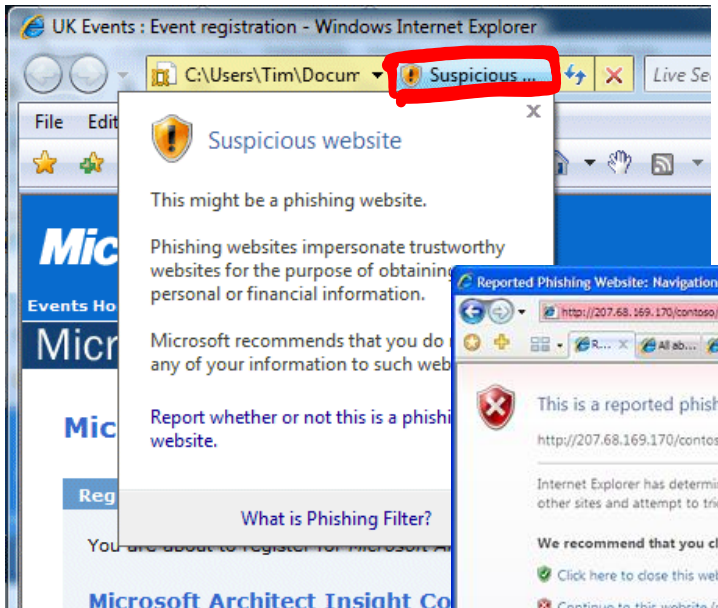
Safe to Type Your Password?



“Picture-in-picture attacks”
Trained users are more likely to fall victim to this!

Browsers also do this for malware

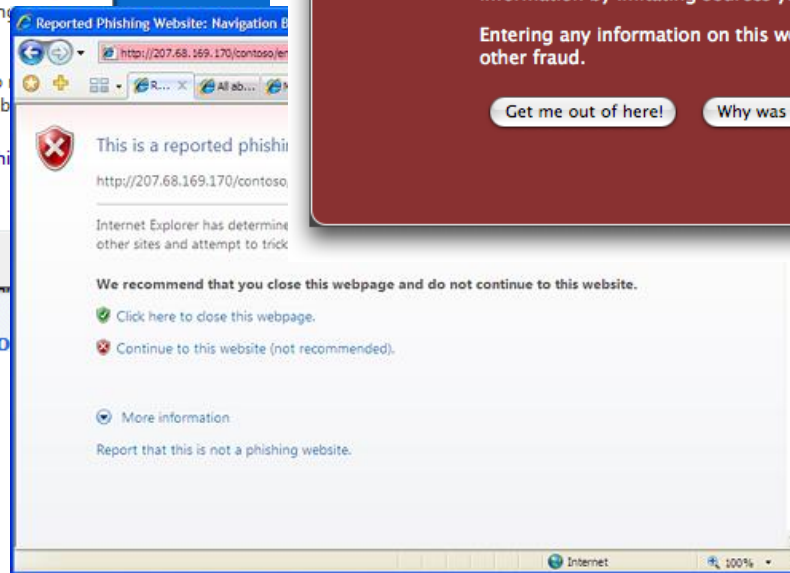
Phishing Warnings (2008)



Passive (IE)



Active (Firefox)



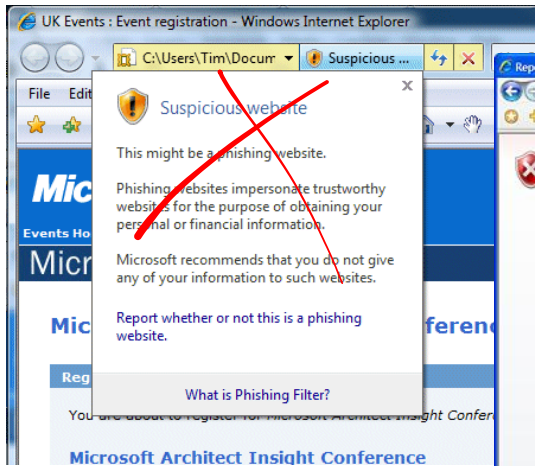
Active (IE)

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

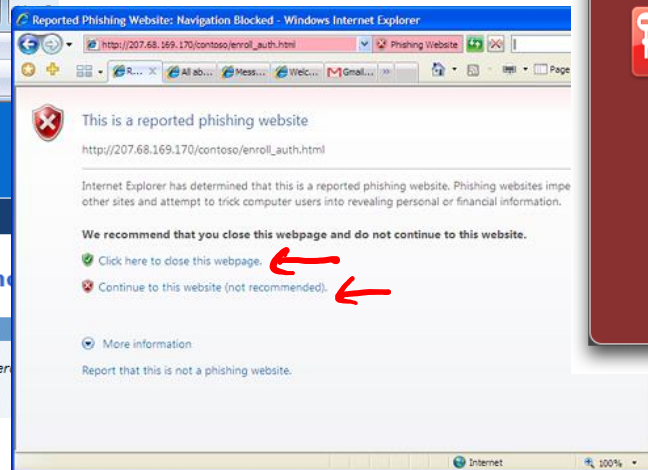
Active vs. Passive Warnings

- 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)

5/18/2020



Active (IE)

CSE 484 / CSE M 584 - Spring 2020



Active (Firefox)

Active vs. Passive 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!

Why Warnings Fail

- 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”
- **Common issue: Warning/prompt fatigue**
 - We'll see this issue again re: mobile security...

FYI: Site Authentication Image

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)

Sign In

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

Root Causes? How to Improve?

ppl don't act as designers anticipate

- they don't know

→ education

- lazy

- trying to do something else

→ make things simple

- false positives

- black box systems

take users for granted:
→ how to design?

→ study people

Stepping Back: Root Causes?

- Computer systems are complex; users lack intuition
- Users in charge of managing own devices
 - Unlike other complex systems, like healthcare or cars.
- Hard to gauge risks
 - “It won’t happen to me!”
- Annoying, awkward, difficult
- Social issues
 - Send encrypted emails about lunch?...

How to Improve?

- Security education and training
- Help users build accurate mental models
- Make security invisible
- Make security the least-resistance path
- ...?

Beyond Specific Tools: Different User Groups

- Not all users are the same!
- Designing for one group of users, or “generic” users, may lead to **dangerous failures** or **reasons that people will not use security tools**
- Examples from (qualitative) research at UW:
 - **Journalists** (**most sources are not like Snowden!**)
 - **Refugees in US** (**security measures may embed US cultural assumptions!**)