CSE 484 / CSE M 584: Computer Security and Privacy

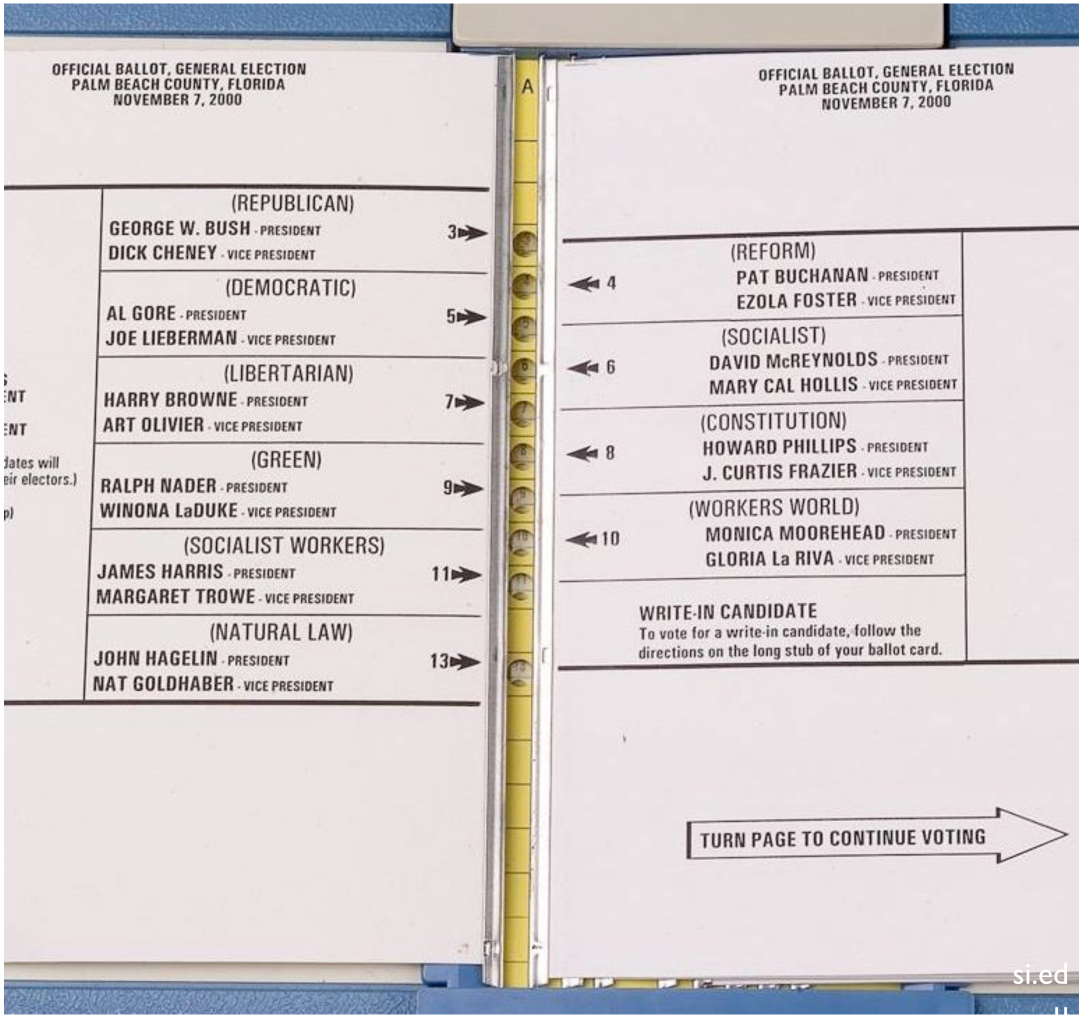
Usable Security

Fall 2017

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 ...

Poor Usability Causes Problems



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

(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▶

S
ENT
ENT
dates will
eir electors.)
p)

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

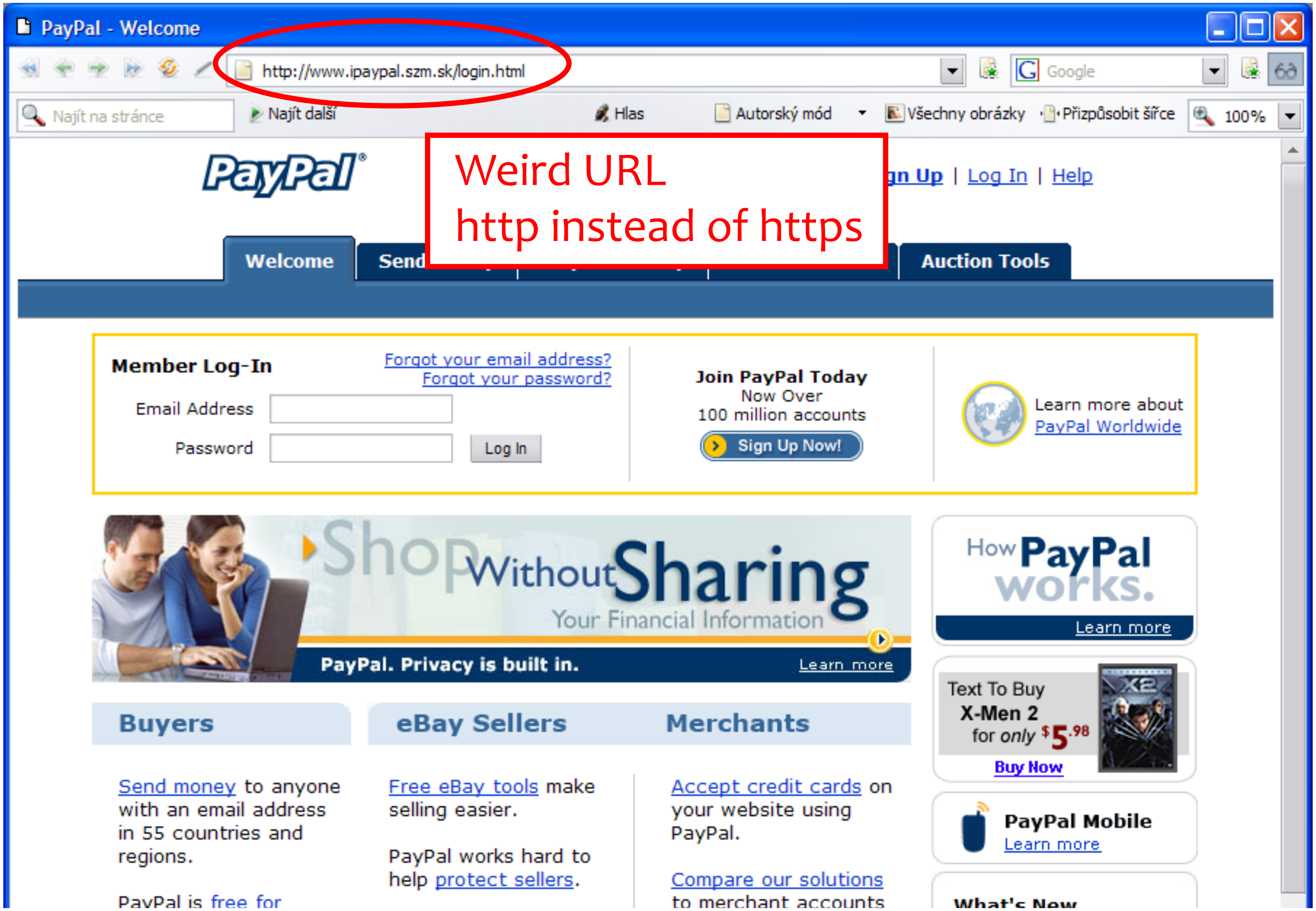
Usable Security Roadmap

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

Case Study #1: Phishing

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

A Typical Phishing Page



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

Weird URL
http instead of https

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

PayPal Mobile
Learn more

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.

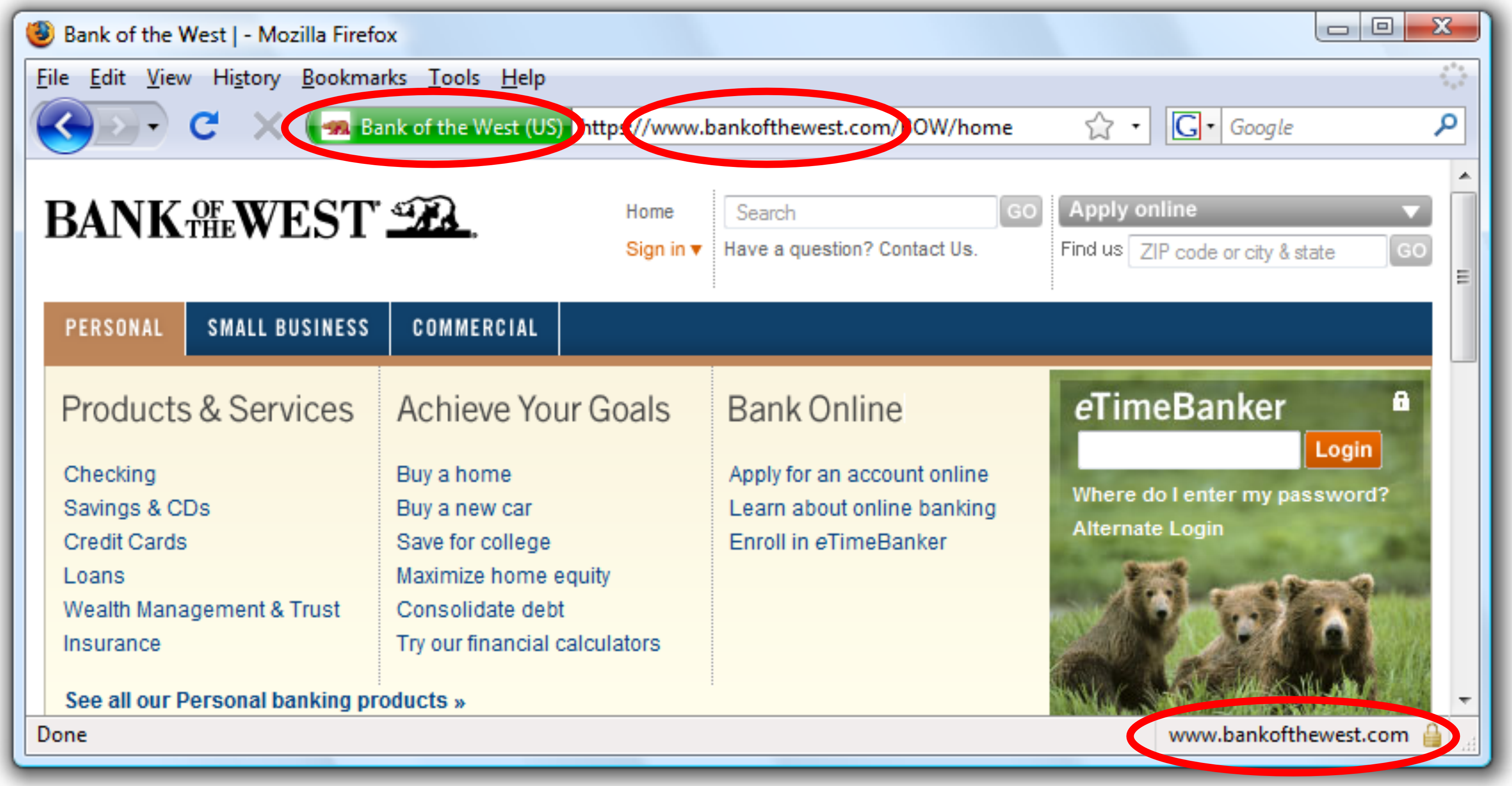
Merchants

Accept credit cards on your website using PayPal.

Compare our solutions to merchant accounts

What's New

Safe to Type Your Password?



Have a question? Contact Us.

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

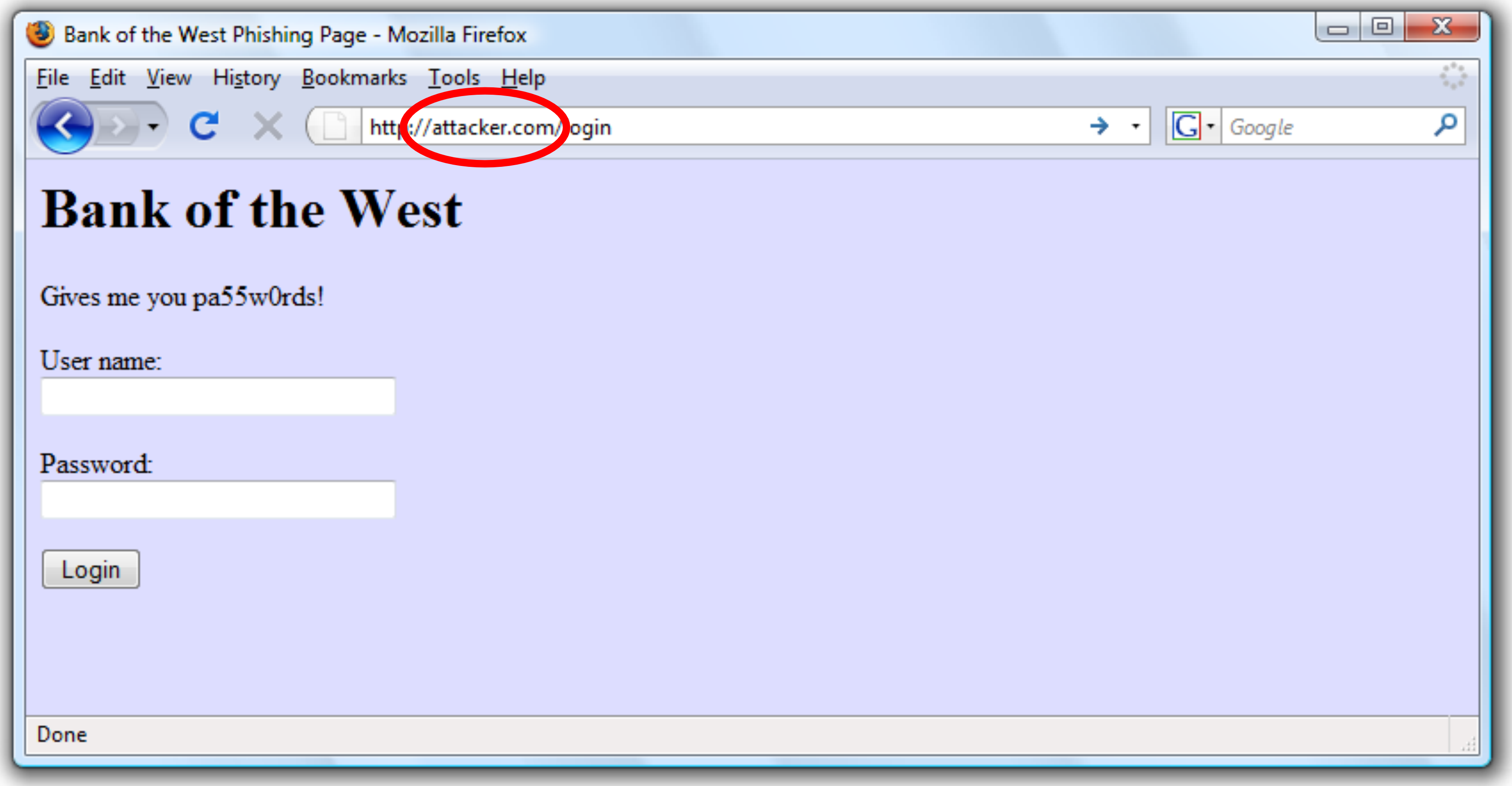
- Apply for an account online
- Learn about online banking
- Enroll in eTimeBanker

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

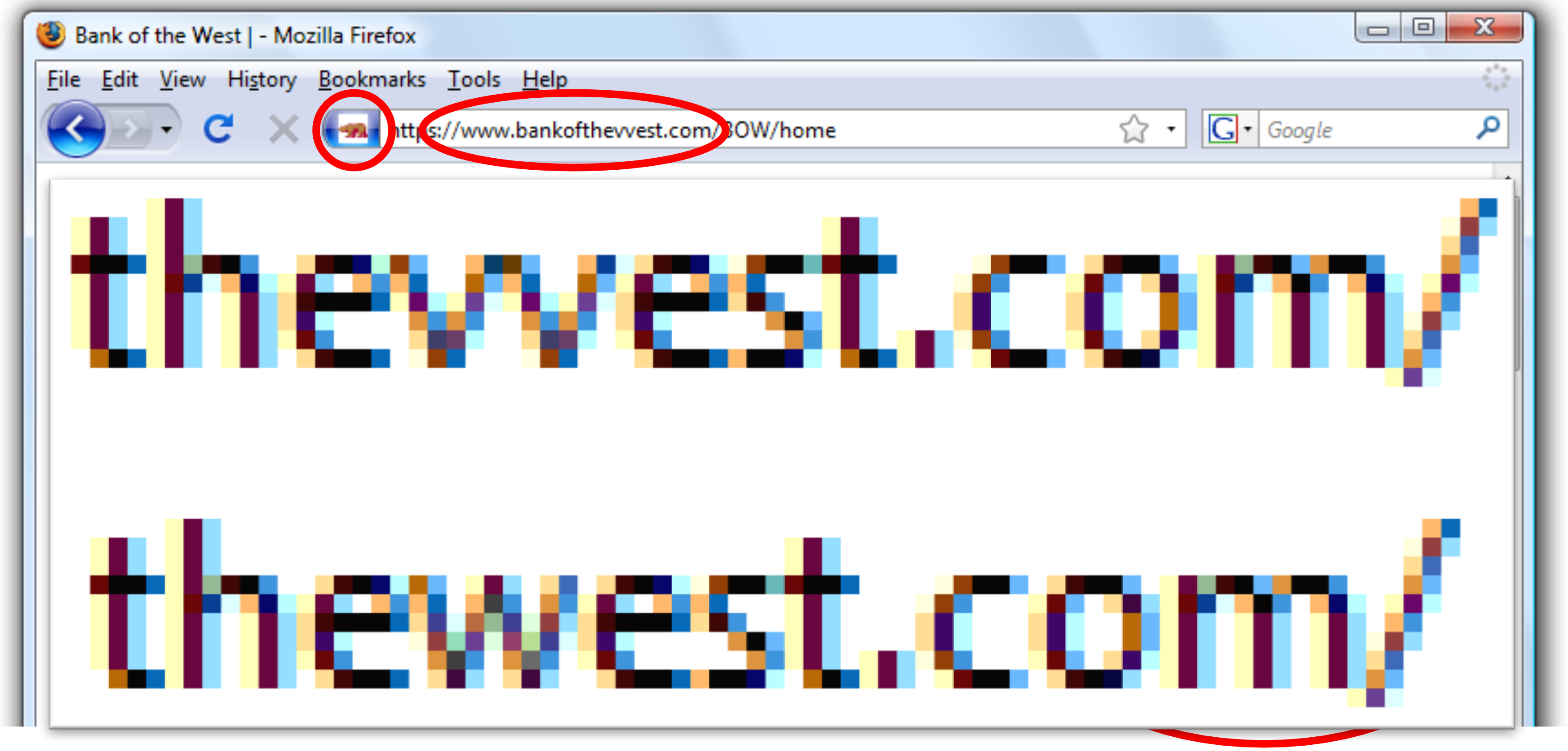
Bank of the West

Gives me you pa55w0rds!

User name:

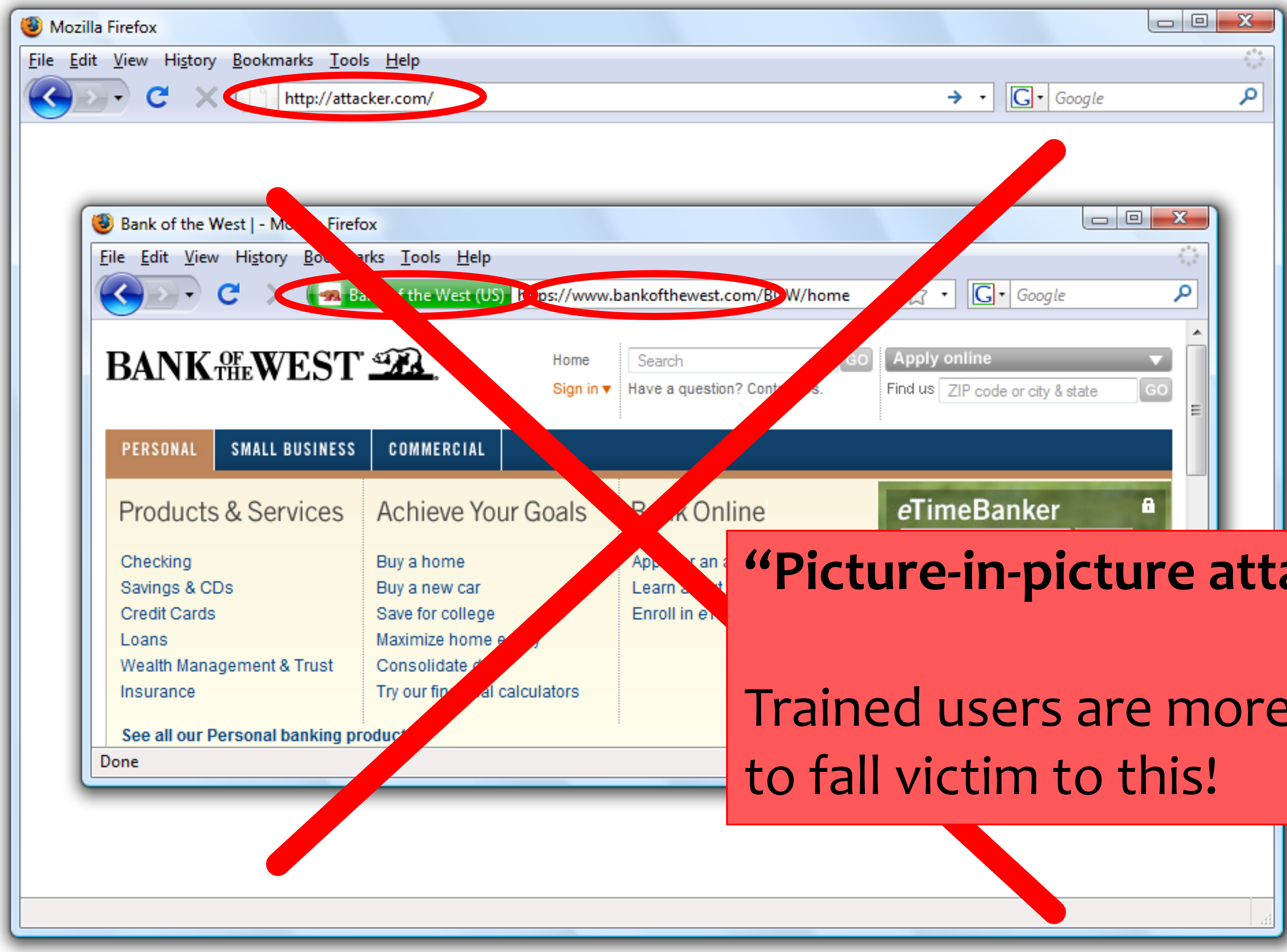
Password:

Safe to Type Your Password?



Bank of the West | - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://www.bankofthevvest.com/BOW/home
Google
thevvest.com/
thewest.com/

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

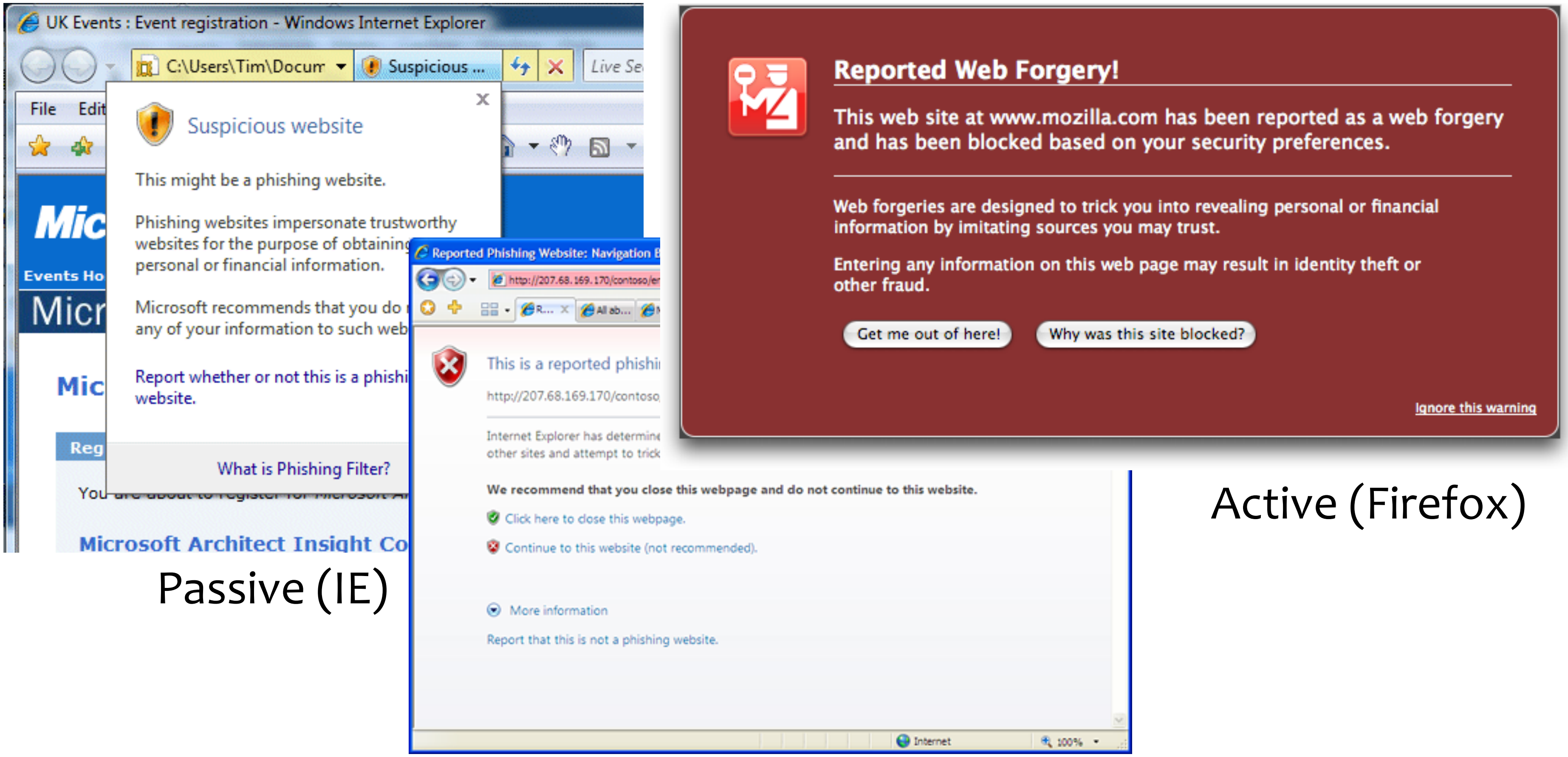
More Details

- 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 ...
Live Se
File
Edit
Mic
Events Ho
Micr
Mic
Reg
You are about to register for Microsoft A
Microsoft Architect Insight Co

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 n 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

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.]

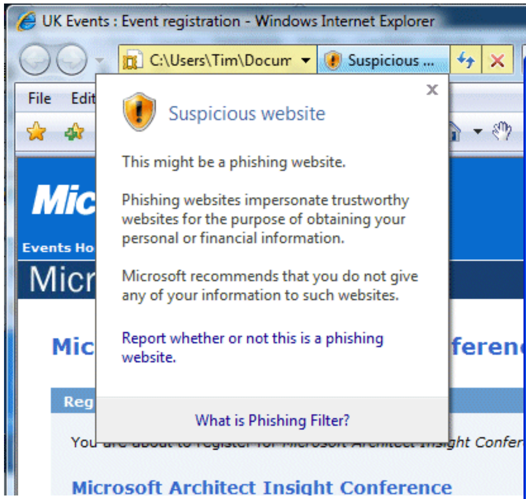
Are Phishing Warnings Effective?

- 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
C:\Users\Tim\Docum
Suspicious ...
File
Edit
Mic
Events Ho
Micr
Mic
ferenc
Reg
You are about to register for Microsoft Architect Insight Confer
Microsoft Architect Insight Conference

Suspicious website

This might be a phishing website.

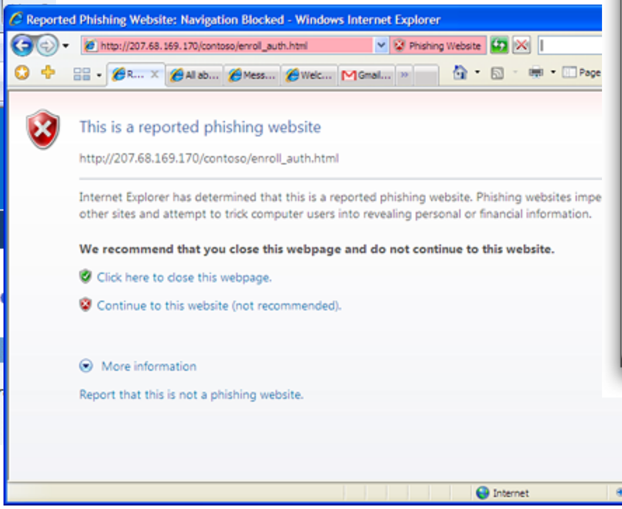
Phishing websites impersonate trustworthy websites for the purpose of obtaining your personal or financial information.

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?

Passive (IE)


Reported Phishing Website: Navigation Blocked - Windows Internet Explorer
http://207.68.169.170/contoso/enroll_auth.html
Phishing Website
R...
All ab...
Mess...
Welc...
Gmail...
Page
Internet
100%

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.

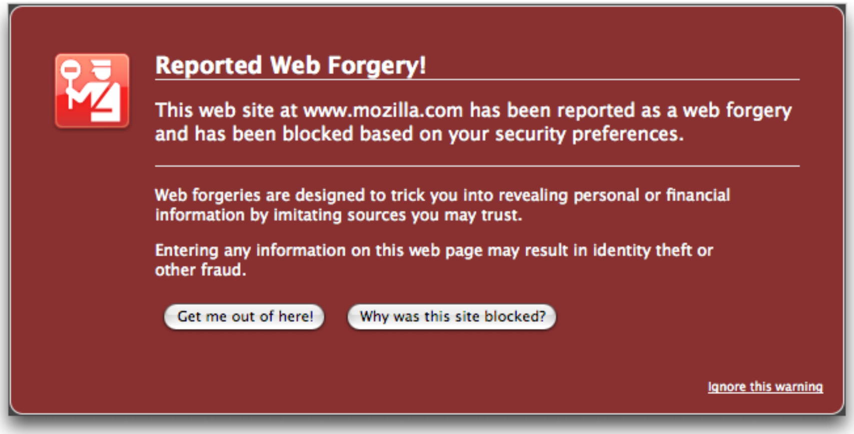
Click here to close this webpage.

Continue to this website (not recommended).

More information

Report that this is not a phishing website.

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.

Active (Firefox)

[Egelman et al.]

User Response to Warnings

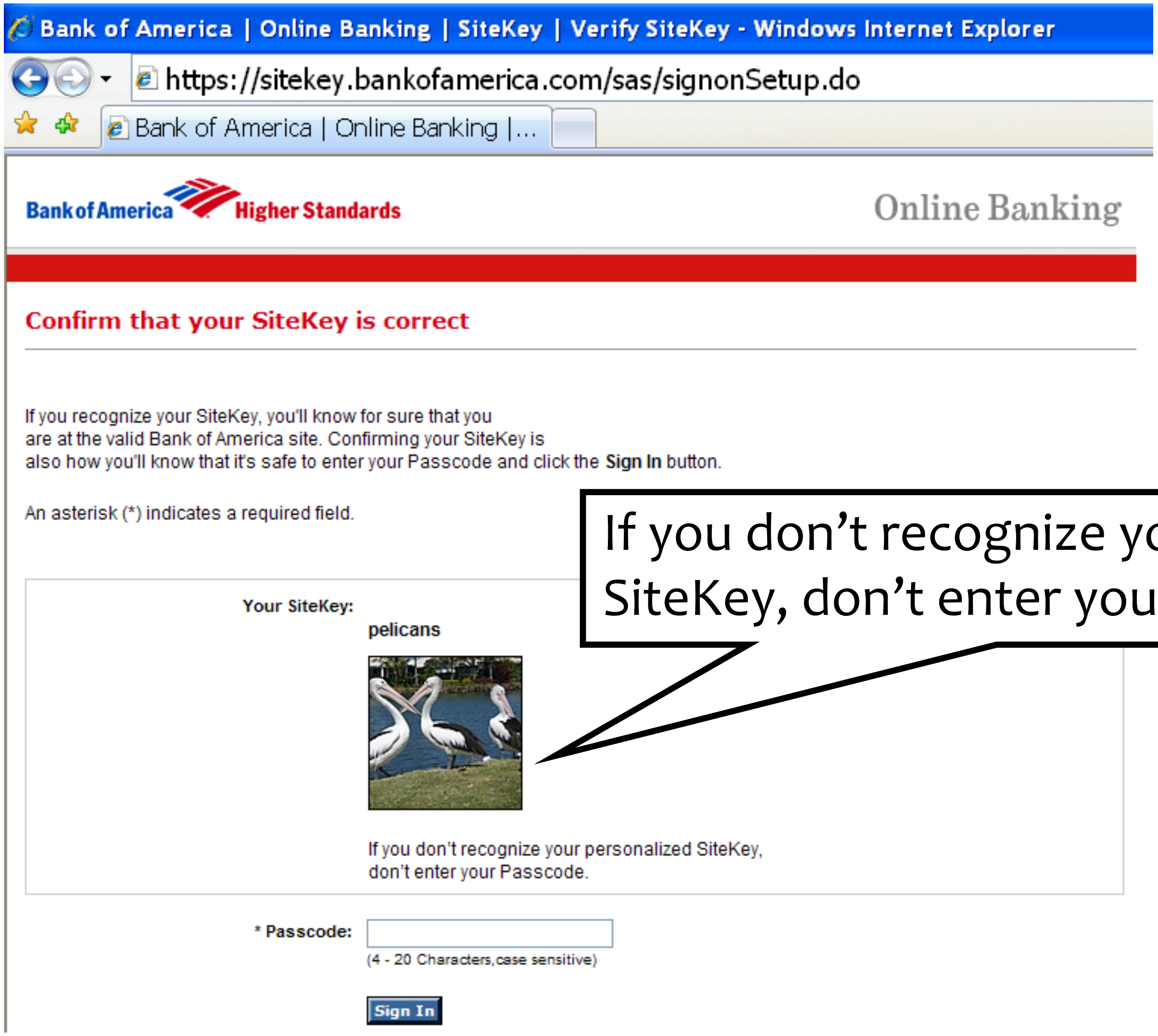
- Some fail to notice warnings entirely
  - Passive warning takes a couple of seconds to appear; if user starts typing, his keystrokes dismiss the warning
- Some saw the warning, closed the window, went back to email, clicked links again, were presented with the same warnings… repeated 4-5 times
  -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

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:

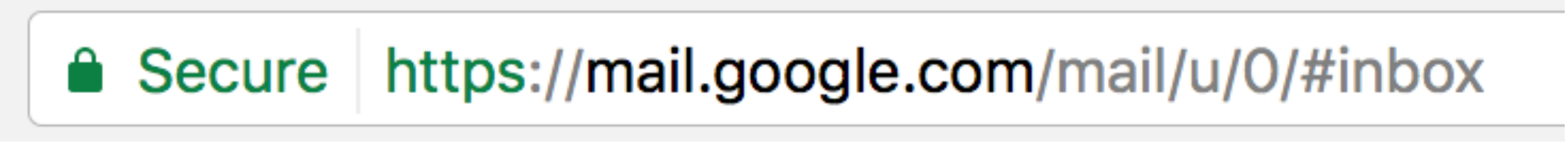
(4 - 20 Characters,case sensitive)

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

Case Study #2: Browser SSL Warnings

- **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

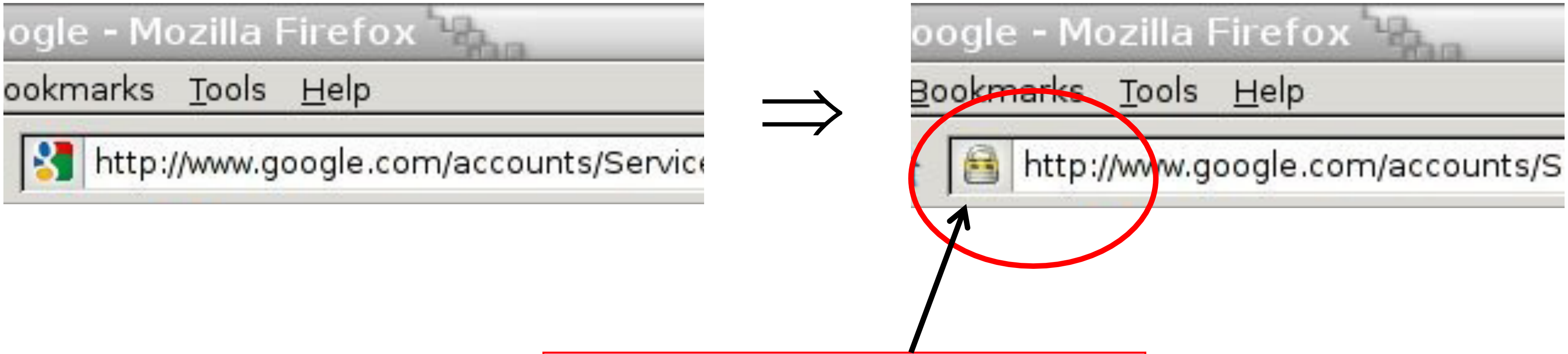


🔒 Secure | https://mail.google.com/mail/u/0/#inbox

- 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?



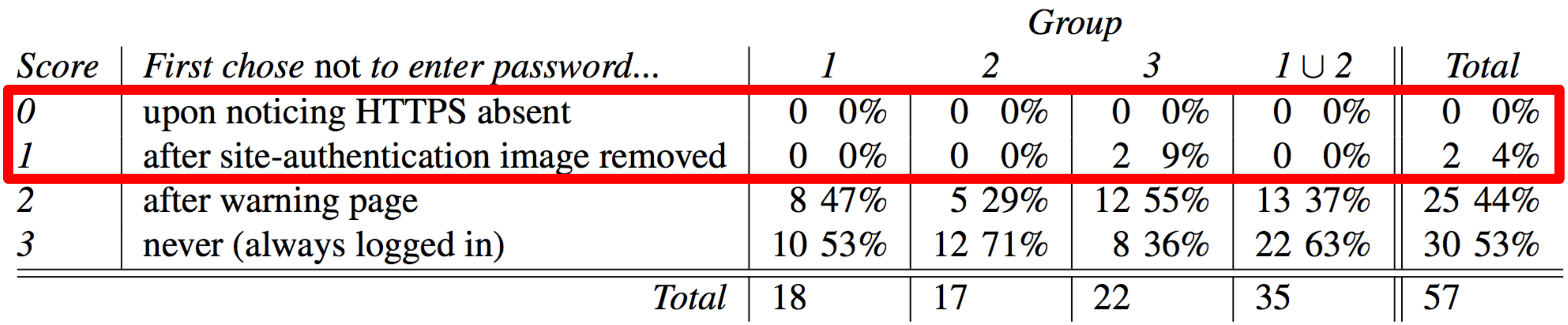
http://www.google.com/accounts/Servic

http://www.google.com/accounts/S

Clever favicon inserted by network attacker

Do These Indicators Help?

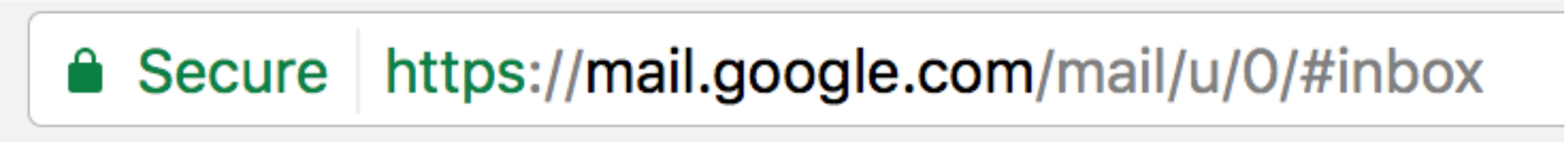
- “The Emperor’s New Security Indicators”
  - http://www.usablesecurity.org/emperor/emperor.pdf

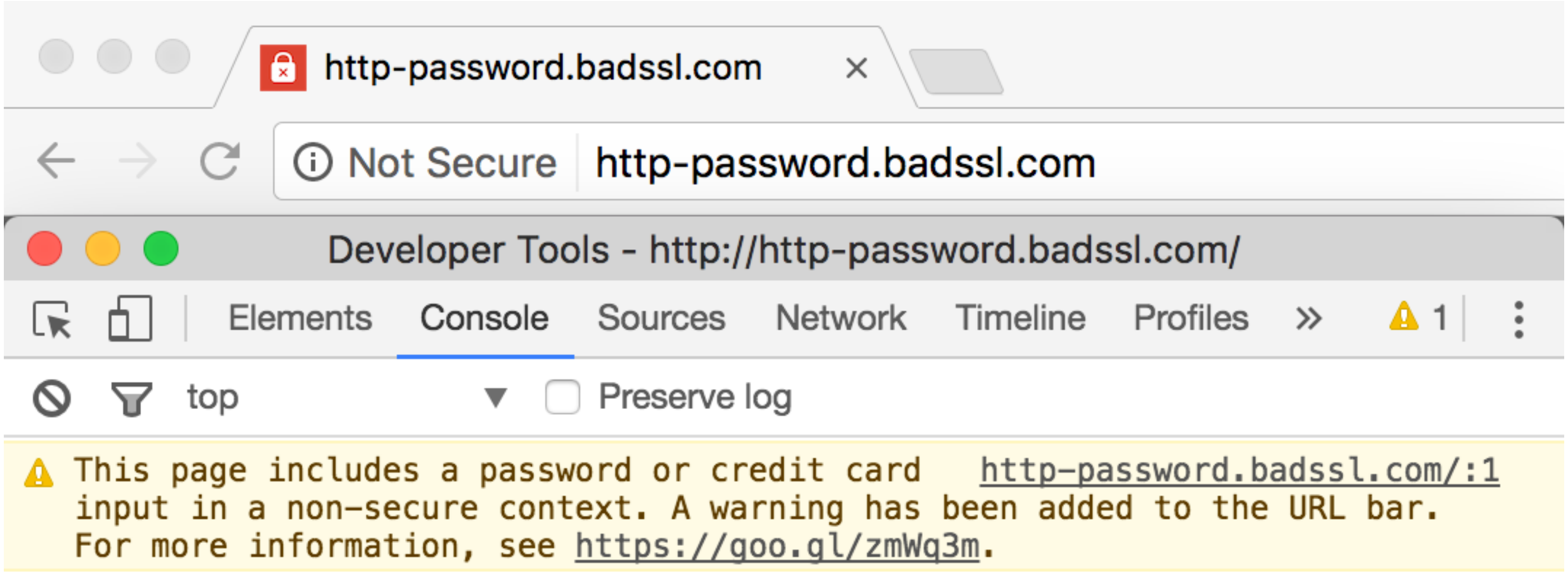


		Group				
Score	*First chose* not *to enter password...*	*1*	*2*	*3*	*1 ∪ 2*	*Total*
0	upon noticing HTTPS absent	0 0%	0 0%	0 0%	0 0%	0 0%
1	after site-authentication image removed	0 0%	0 0%	2 9%	0 0%	2 4%
2	after warning page	8 47%	5 29%	12 55%	13 37%	25 44%
3	never (always logged in)	10 53%	12 71%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

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

Latest Design in Chrome



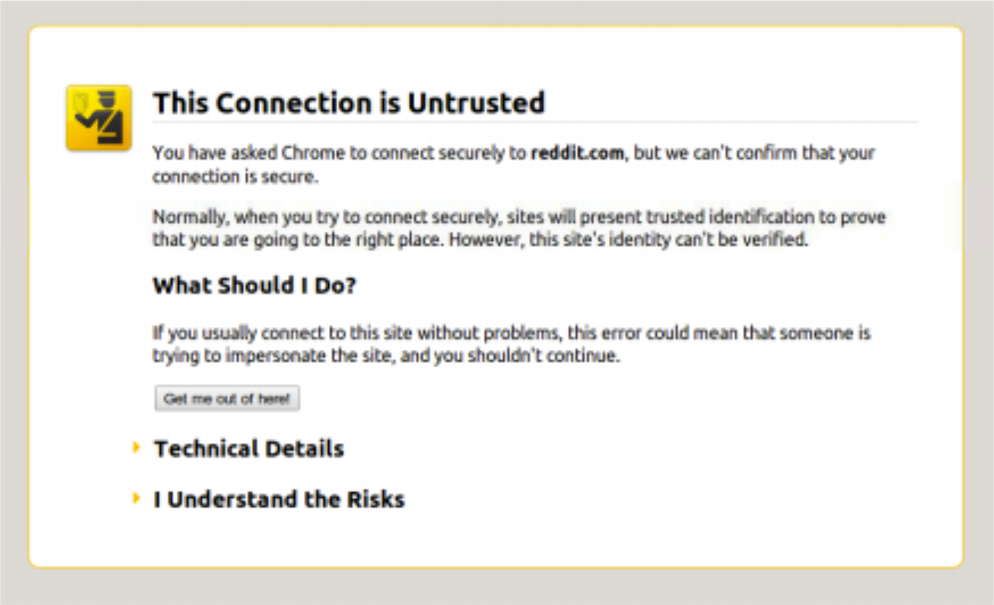


```
⚠ This page includes a password or credit card   http-password.badssl.com/:1
  input in a non-secure context. A warning has been added to the URL bar.
  For more information, see https://goo.gl/zmWq3m.
```

[Felt et al.]

Firefox vs. Chrome Warning

33% vs. 70% clickthrough rate



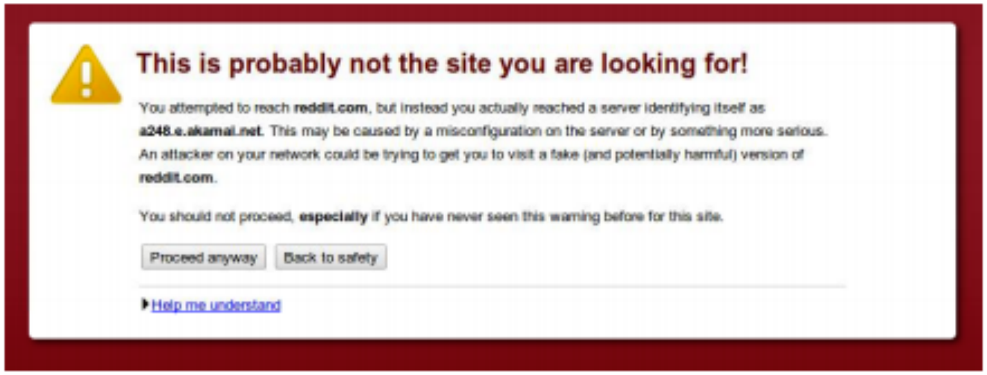
This Connection is Untrusted

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.



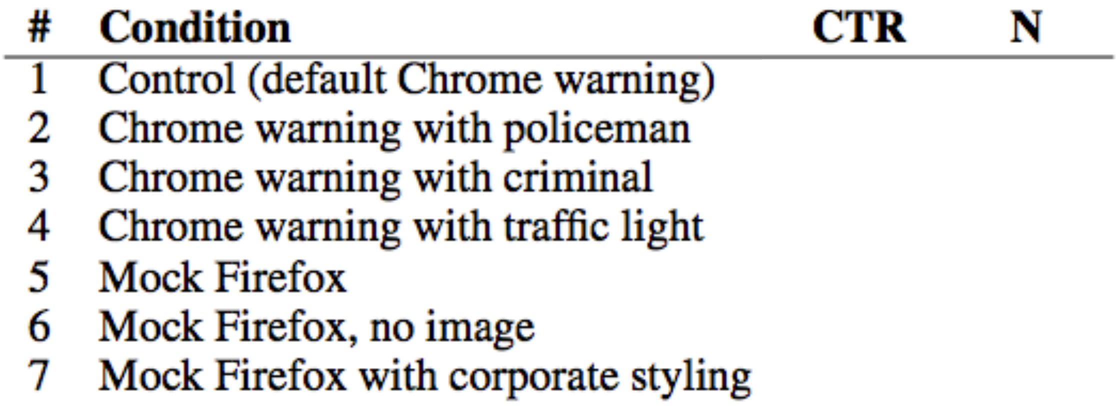
This is probably not the site you are looking for!

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		

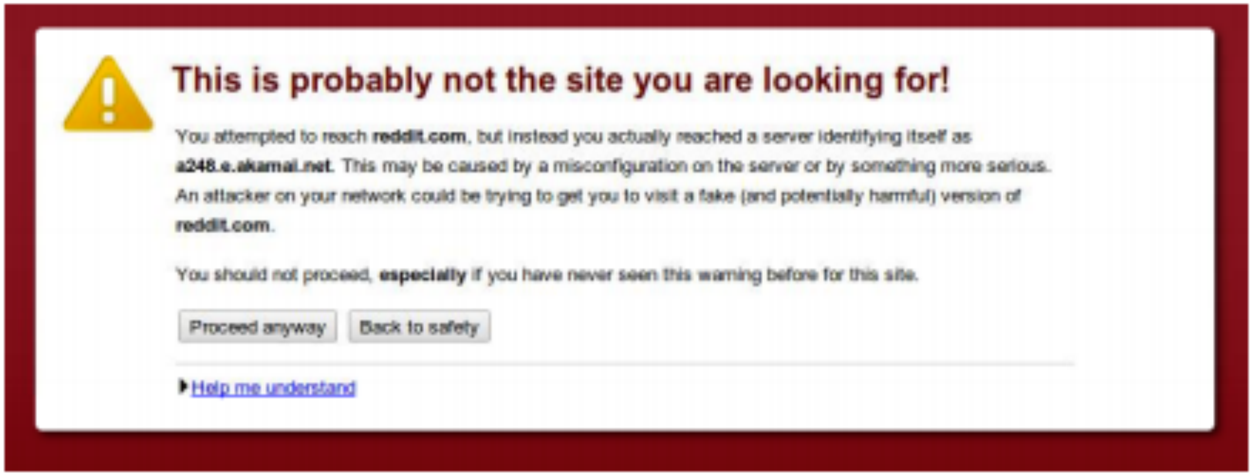
Table 1. Click-through rates and sample size for conditions.

[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.

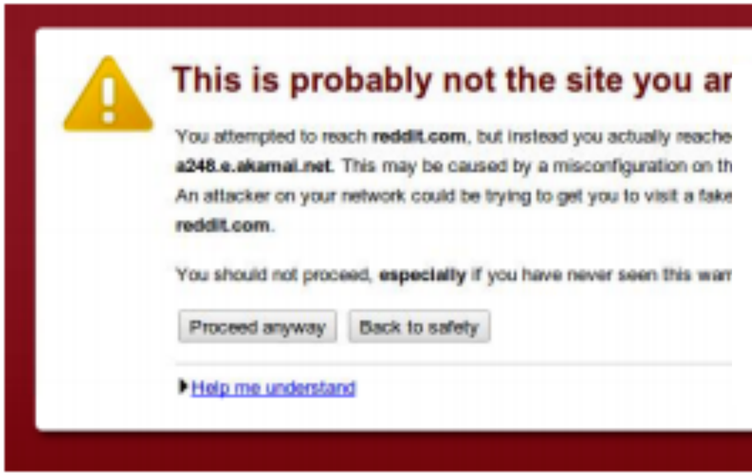
Figure 1. The default Chrome SSL warning (Condition 1).

[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

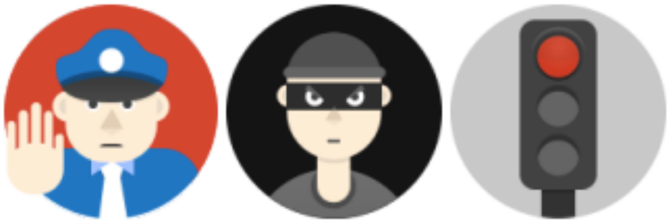


Figure 4. The three images used in Conditions 2-4.

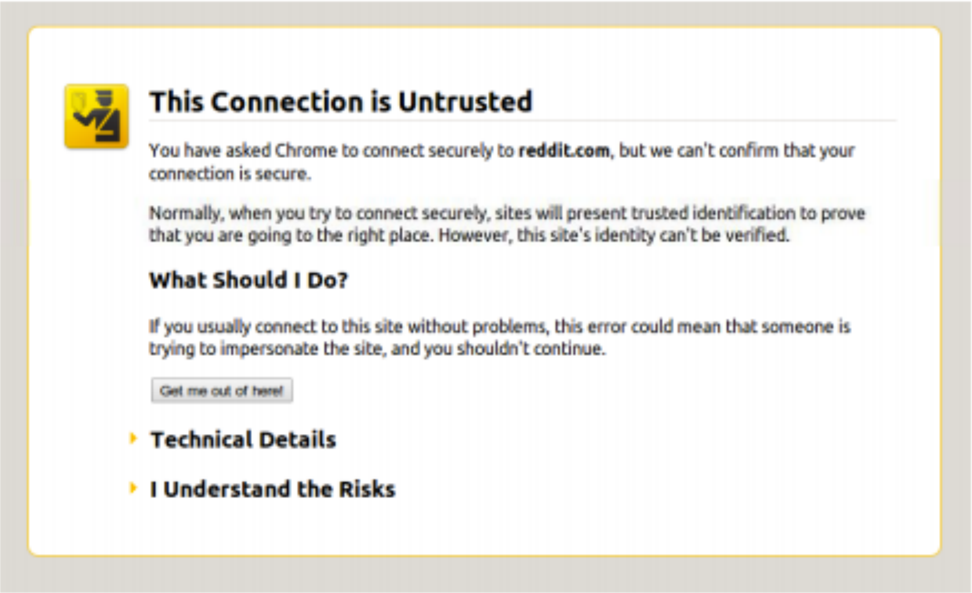
Figure 1. The default Chrome SSL warning (Condition 1).

[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.

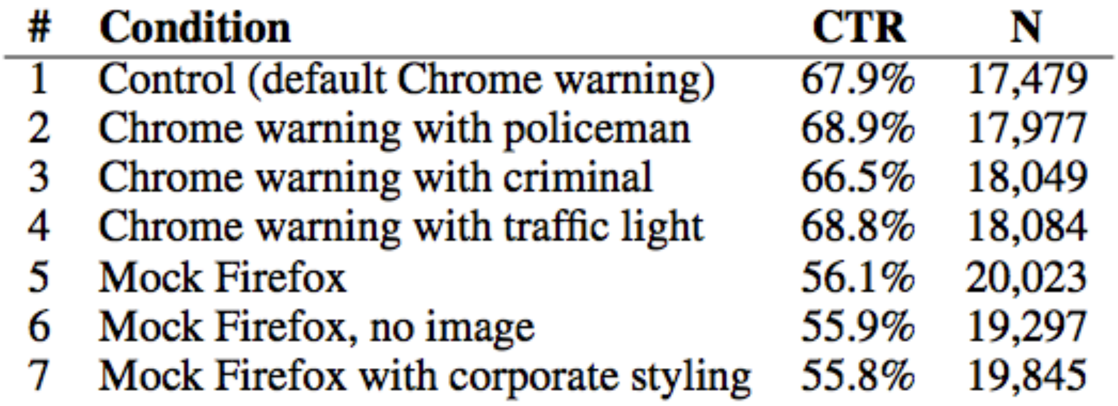
What Should I Do?

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.

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

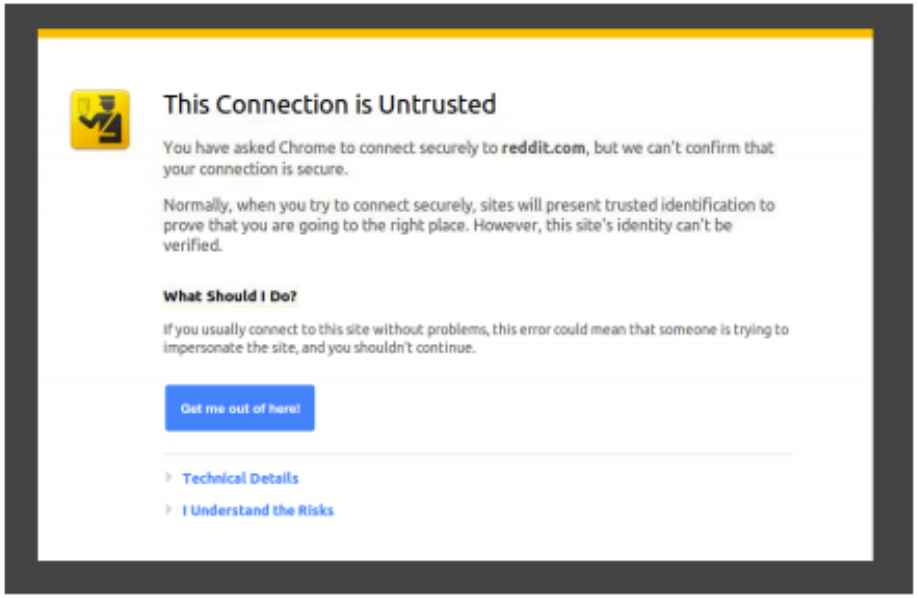
[Felt et al.]

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.

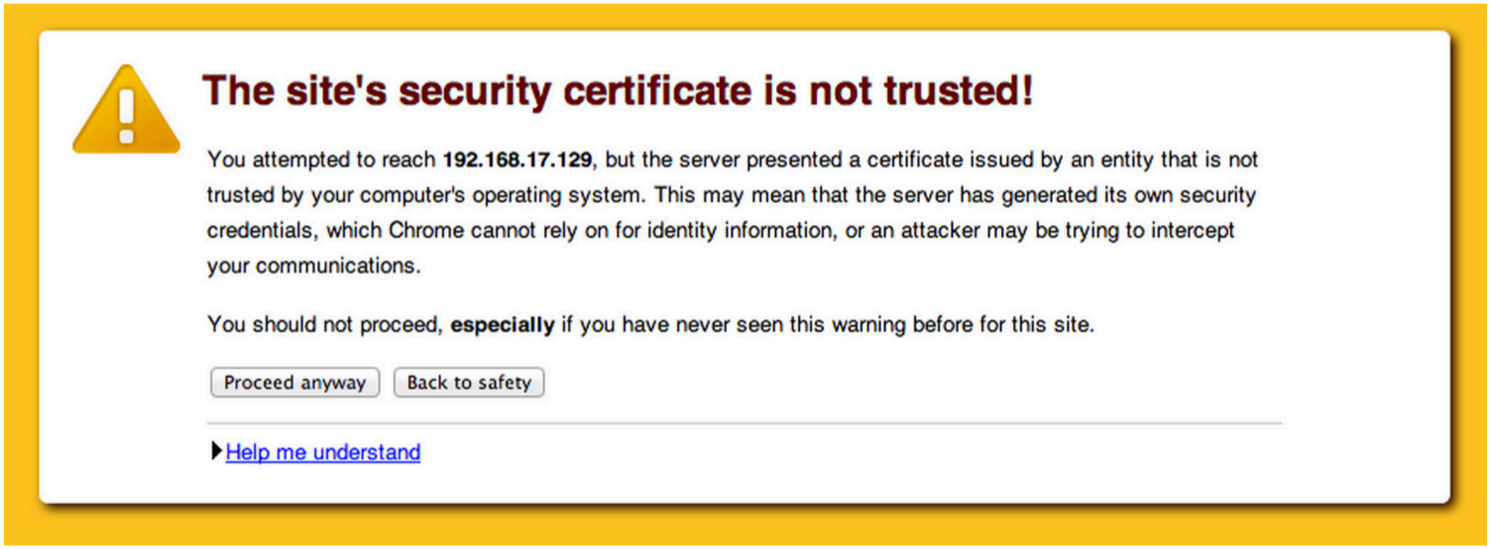
What Should I Do?

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!

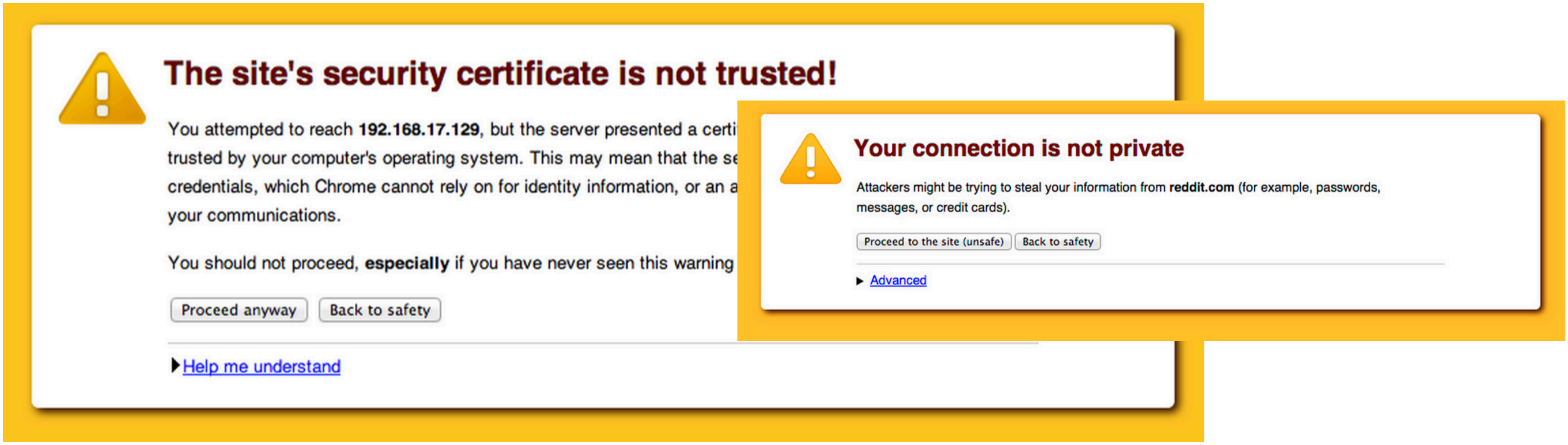
You attempted to reach **192.168.17.129**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Chrome cannot rely on for identity information, or an attacker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



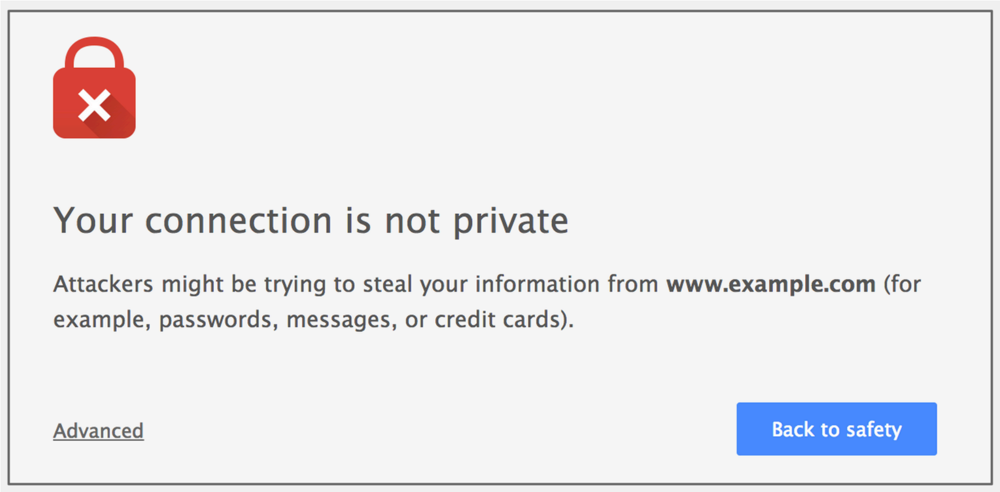
The site's security certificate is not trusted!

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).



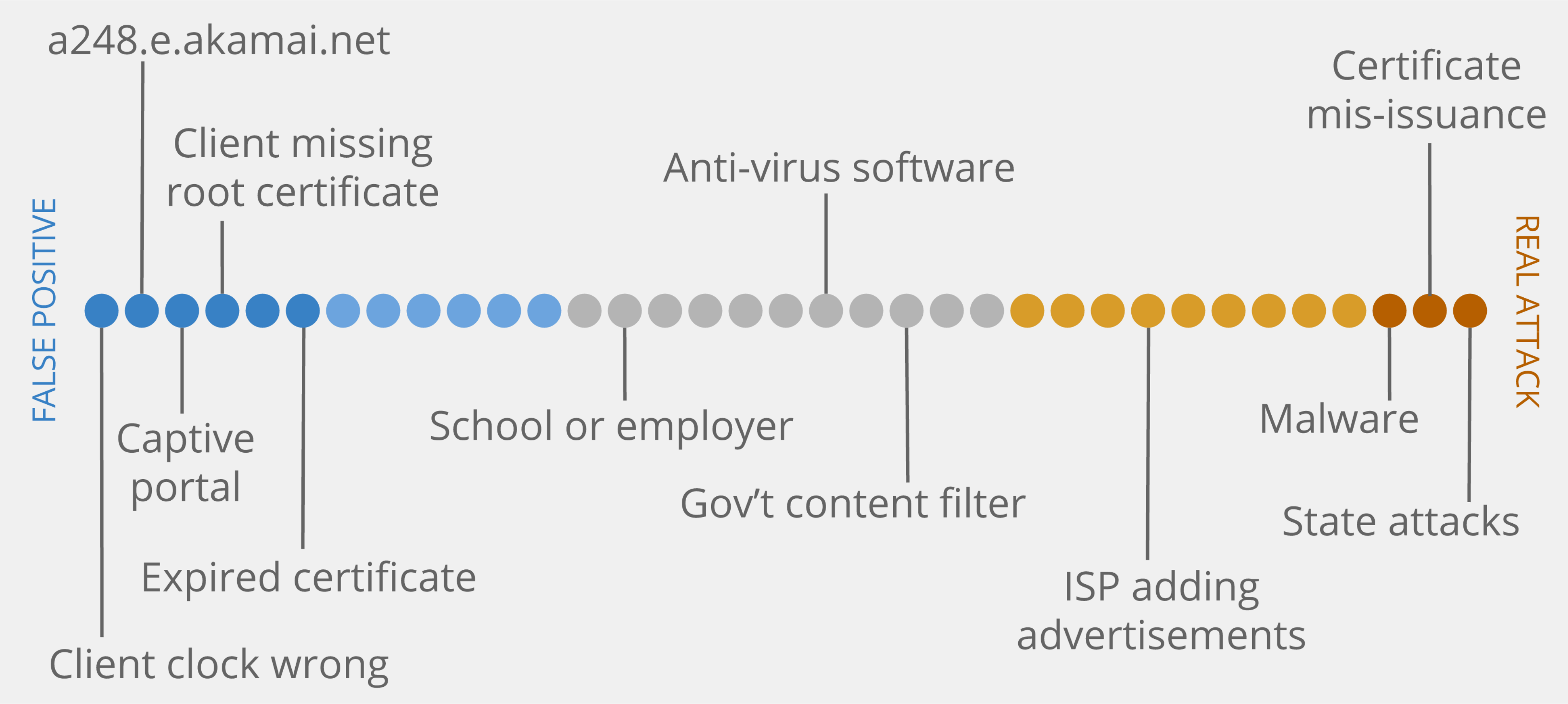
Your connection is not private

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



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
- …?