CSE 484: Computer Security and Privacy

Vulnerability Finding + Patching
Usability

Spring 2023

David Kohlbrenner

dkohlbre@cs

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

Exploit RCA and Patching

Root-Cause Analysis (RCA)

- Basically debugging, but you didn’t generate the input

- Consider:
  - What is different between a ‘normal’ interaction and the exploit?
  - What part(s) of the program are relevant to that interaction
    - Add logging/debugging here! But consider that it might affect the exploit…
  - What specifically happened that was ‘unusual’
  - Develop theories about what is happening
  - Test your theories!

The goals for RCAs

- Identify what the exploit accomplishes
- Identify the major steps the exploit takes
- Find the specific code components (if any exist) that are responsible
  - Aka: the vulnerability
  - Consider that an exploit might leverage *missing* features!
- Find ‘nearby’ bugs
  - Ie. If you fix the most-responsible line of code, is it still vulnerable?
- Plan out a patch

Project 0 (p0) RCAs

- Google Project 0 (aka p0) is the premiere publicly-disclosing bug hunting team
- They produce detailed writeups of many bugs, and work with Google's Threat Analysis Group (aka TAG) to produce RCAs of in-the-wild bugs.
- You should read some p0 RCAs!

Patch writing goals

- Break the *specific* exploit strategy the exploit uses
- Break *similar* exploit strategies
  - Consider how XSS filtering worked in Lab 2!

- Minimize breaking explicit features of the program

- Minimize breaking *implicit* features of the program

Public bug finding - Terminology

- “Zero Days” – 0 days (aka “o-days”)
  - Refers to a bug that is made publicly known at the same time as the vendor is told
  - The vendor has had ‘0 days’ of lead time to fix it
- CVE Number
  - Common Vulnerabilities and Exposures
  - E.g. CVE-2022-4135
- CVSS
  - Common Vulnerability Scoring System
  - Very limited utility, scores barely correlated with impact
- CWE
  - Common Weakness Enumeration
  - Standardized list of bug types

Public bug finding - Disclosure

- At some point, the vendor finds out about the bug
  - Either publicly revealed by finder (an 0-day)
  - Internally found by code auditing
  - Found being used in-the-wild
- If *you* find the bug:
  - When do you disclose?
  - How do you disclose?
  - “Full-disclosure” vs “Coordinated disclosure” vs “Responsible disclosure”
- Bug bounty programs offer incentives to disclose
  - But at a cost: you usually have to sign NDAs

Anonymity (Tor)

Tor

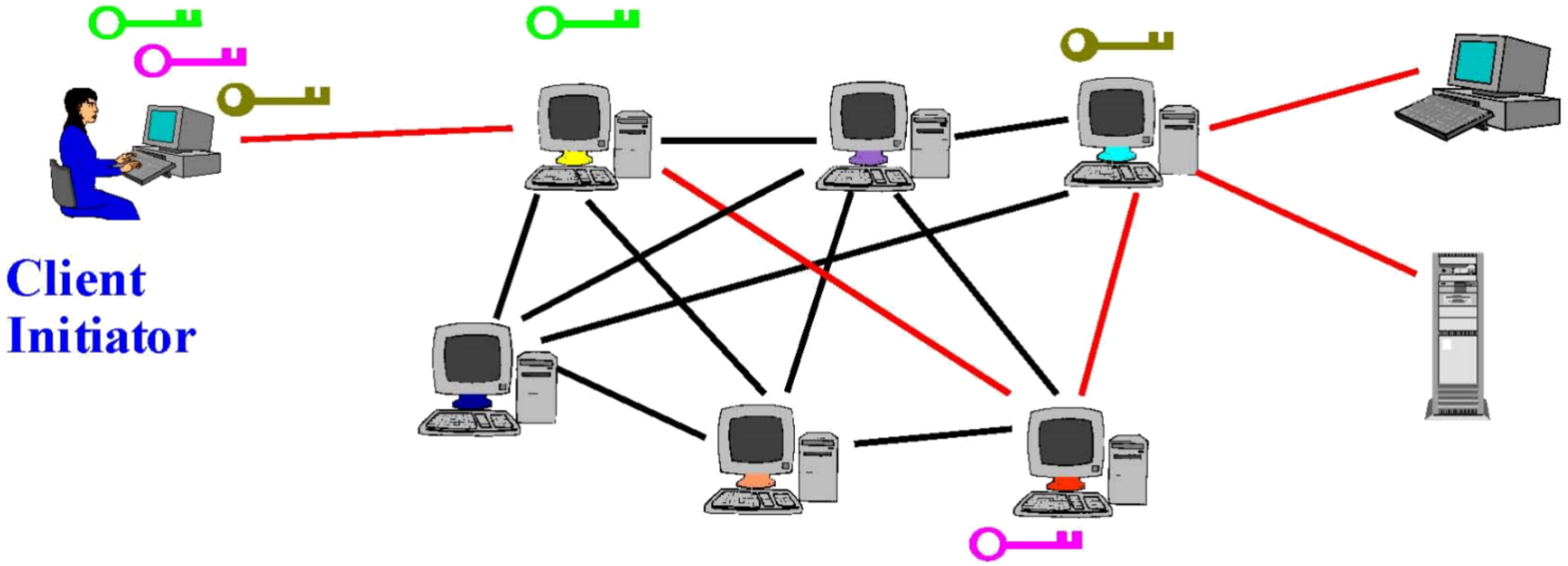
- Second-generation onion routing network
  - http://tor.eff.org
  - Developed by Roger Dingledine, Nick Mathewson and Paul Syverson
  - Specifically designed for low-latency anonymous Internet communications
- Running since October 2003
- “Easy-to-use” client proxy
  - Freely available, can use it for anonymous browsing

Issues and Notes of Caution

- Passive traffic analysis
  - Infer from network traffic who is talking to whom
  - To hide your traffic, must carry other people's traffic!
- Active traffic analysis
  - Inject packets or put a timing signature on packet flow
- Compromise of network nodes
  - Attacker may compromise some routers
    - Powerful adversaries may compromise "too many"
  - It is not obvious which nodes have been compromised
    - Attacker may be passively logging traffic
  - Better not to trust any individual router
    - Assume that some fraction of routers is good, don't know which

Issues and Notes of Caution

- Tor isn't completely effective by itself
  - Tracking cookies, fingerprinting, etc.
  - Exit nodes can see everything!



Issues and Notes of Caution

- The simple act of using Tor could make one a target for additional surveillance
- Hosting an exit node could result in illegal activity coming from your machine
- Tor not designed to protect against adversaries with the capabilities of a state (public statement by designers, at least in the past)

Usability and Security

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

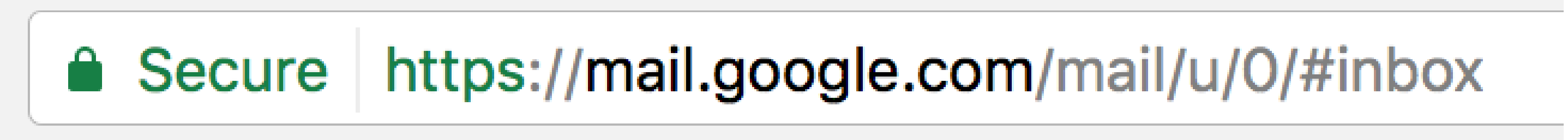
Usable Security Roadmap

- 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?
  - You discussed this in section a couple weeks ago

The Lock Icon

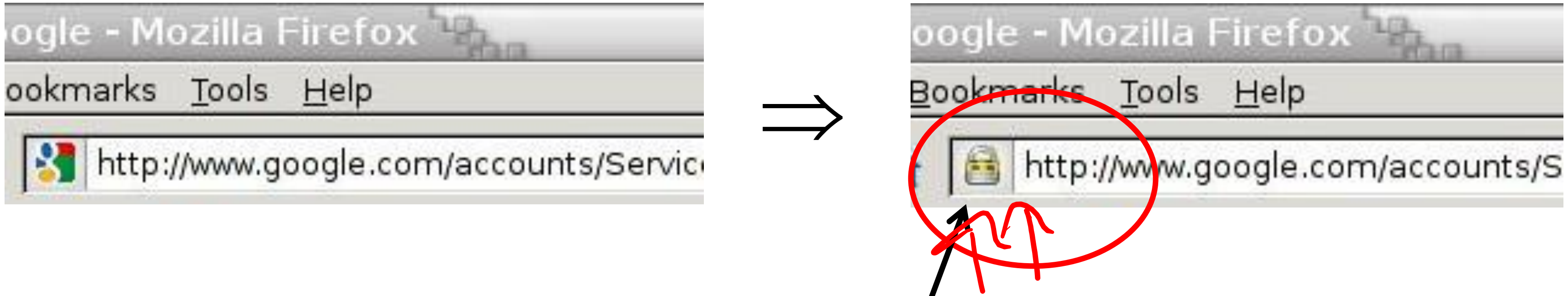


Secure https://mail.google.com/mail/u/0/#inbox

- 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]

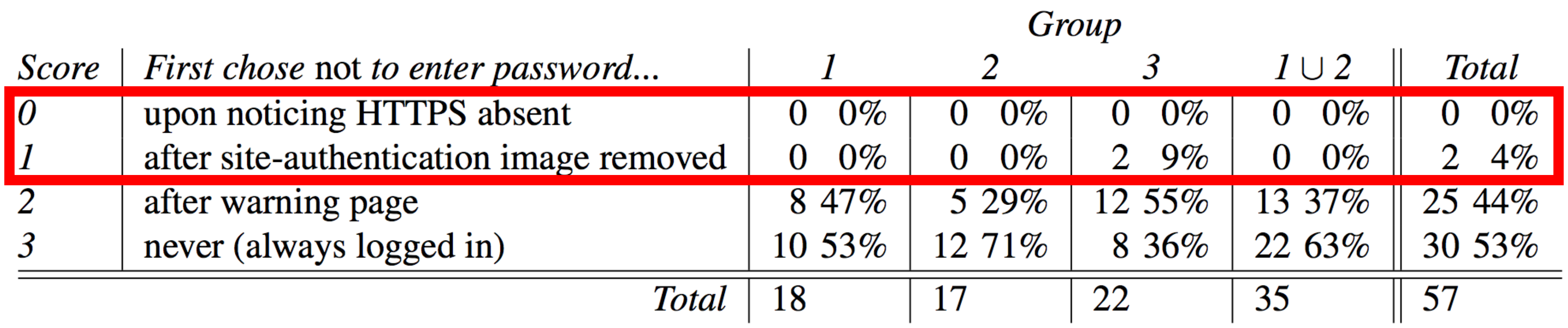
Will You Notice?



Clever favicon inserted by network attacker

Do These Indicators Help? (2007)

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



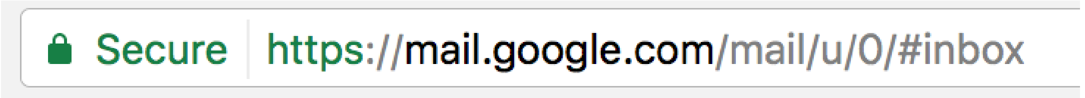
		Group				
Score	*First chose* not *to enter password...*	*1*	*2*	*3*	*1* ∪ *2*	*Total*
0	upon noticing HTTPS absent	0 0%	0 0%	0 0%	0 0%	0 0%
1	after site-authentication image removed	0 0%	0 0%	2 9%	0 0%	2 4%
2	after warning page	8 47%	5 29%	12 55%	13 37%	25 44%
3	never (always logged in)	10 53%	12 71%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

Lesson:

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

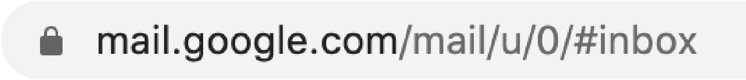
Newer Versions of Chrome

c. 2017

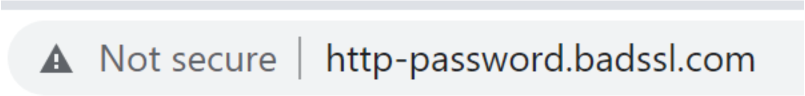


Secure https://mail.google.com/mail/u/0/#inbox

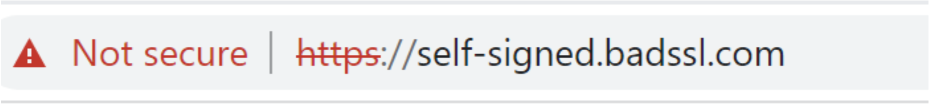
2022



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

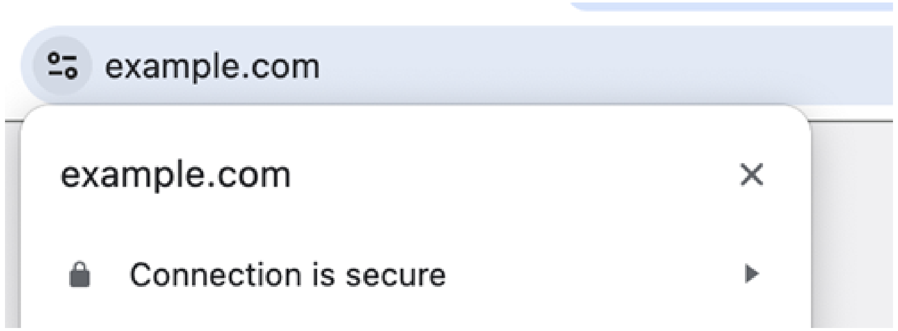


Not secure | http-password.badssl.com



Not secure | ~~https~~://self-signed.badssl.com

2023/2024



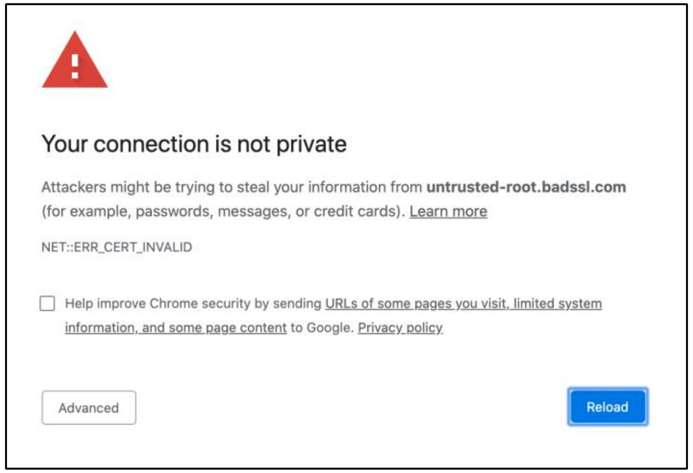
example.com

example.com

Connection is secure

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?



Your connection is not private

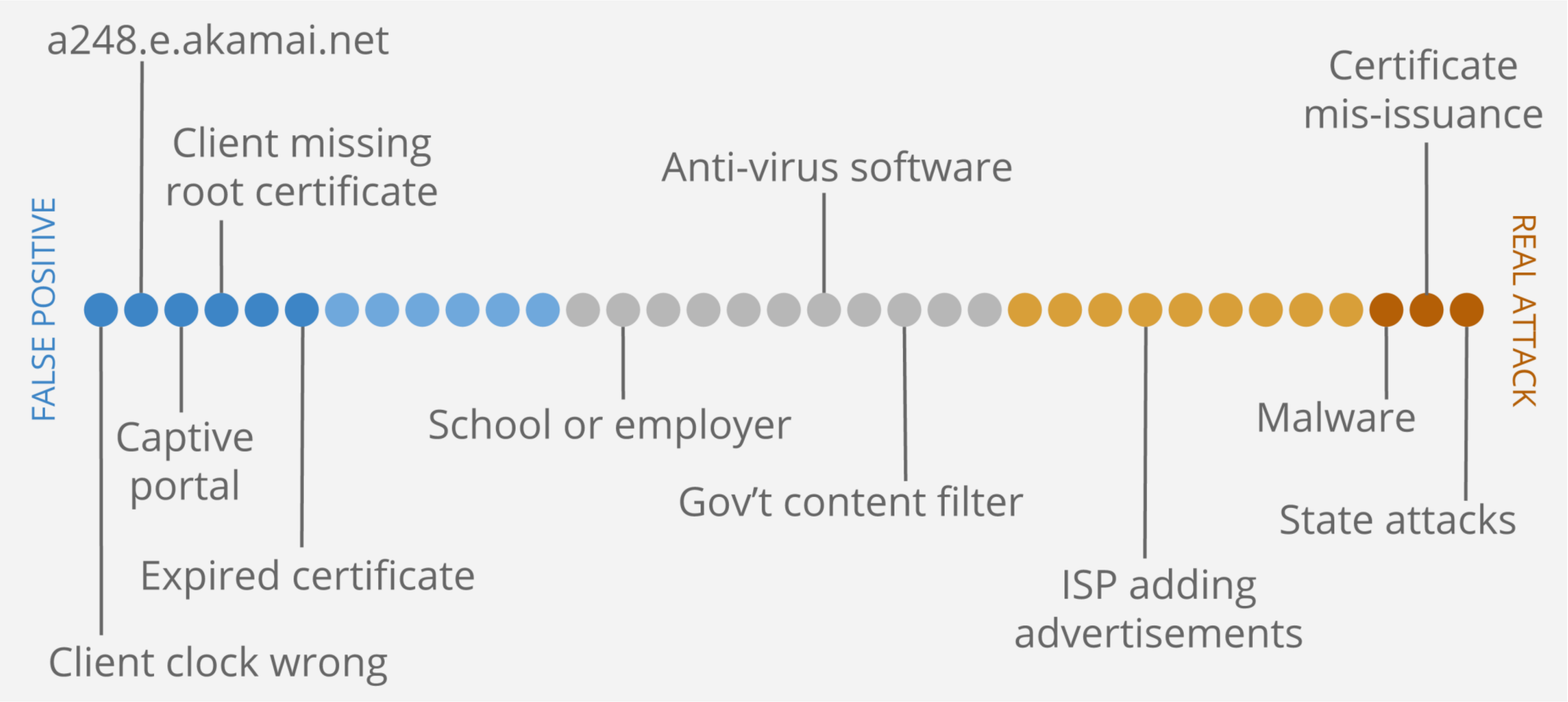
Attackers might be trying to steal your information from **untrusted-root.badssl.com** (for example, passwords, messages, or credit cards). Learn more

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

[Felt et al.]

Challenge: Meaningful Warnings

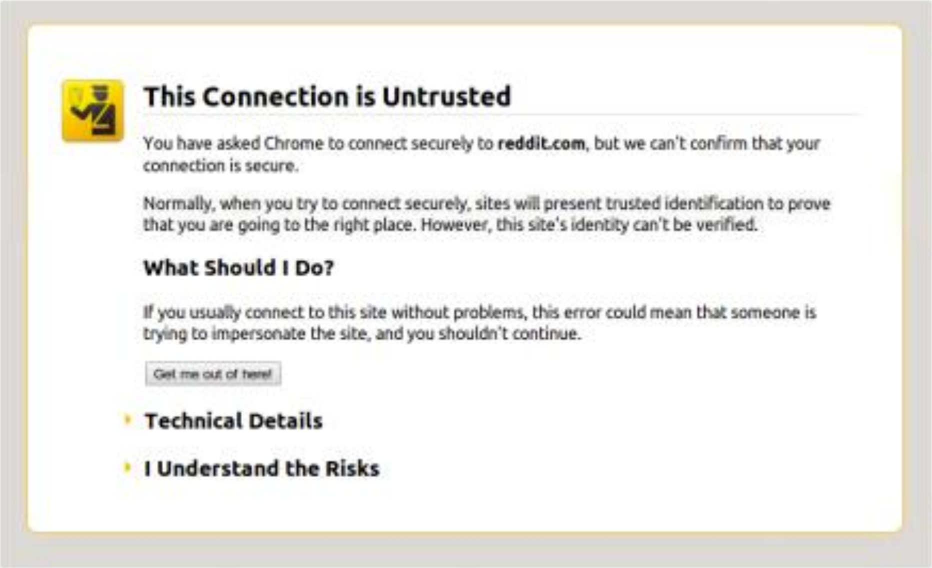


See current designs for different conditions at https://badssl.com/.

[Felt et al.]

Firefox vs. Chrome Warning

33% vs. 70% clickthrough rate



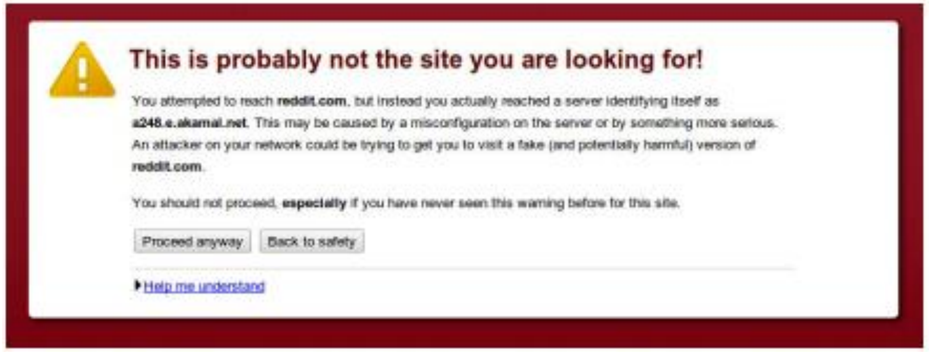
This Connection is Untrusted

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.



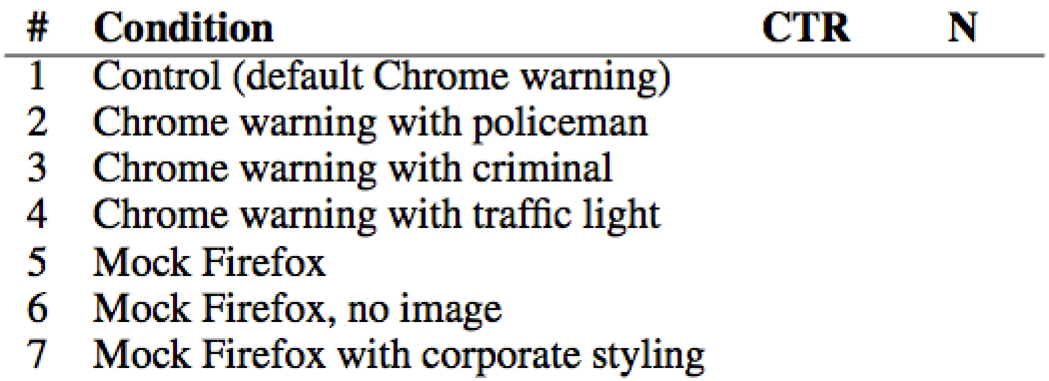
This is probably not the site you are looking for!

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		

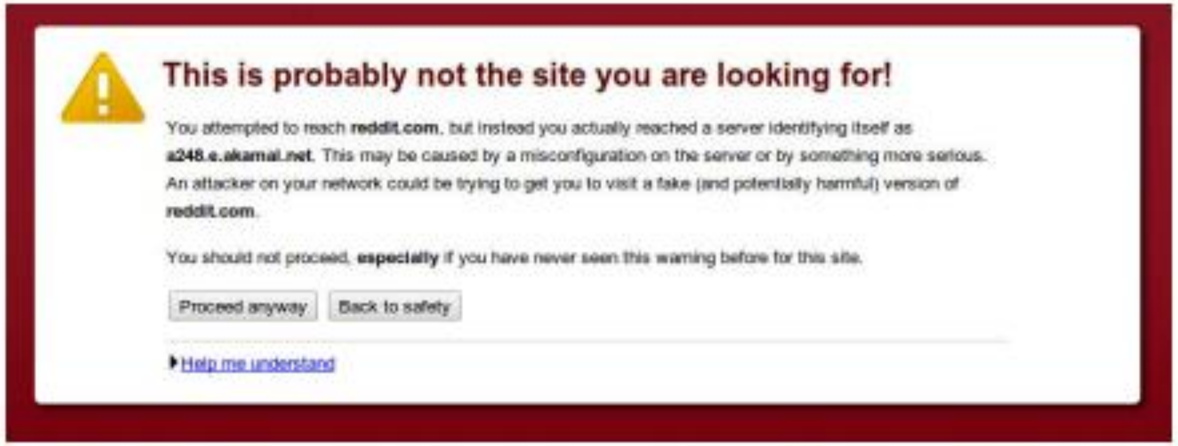
Table 1. Click-through rates and sample size for conditions.

[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.

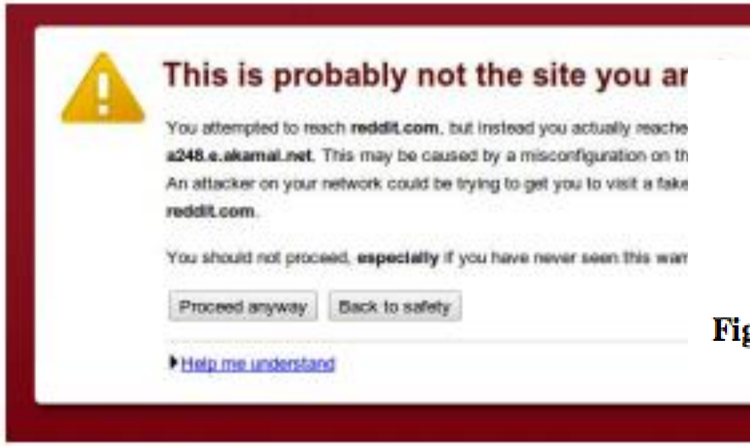
Figure 1. The default Chrome SSL warning (Condition 1).

[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

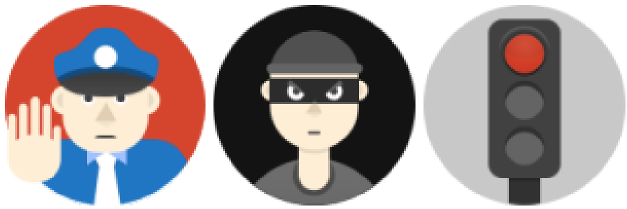
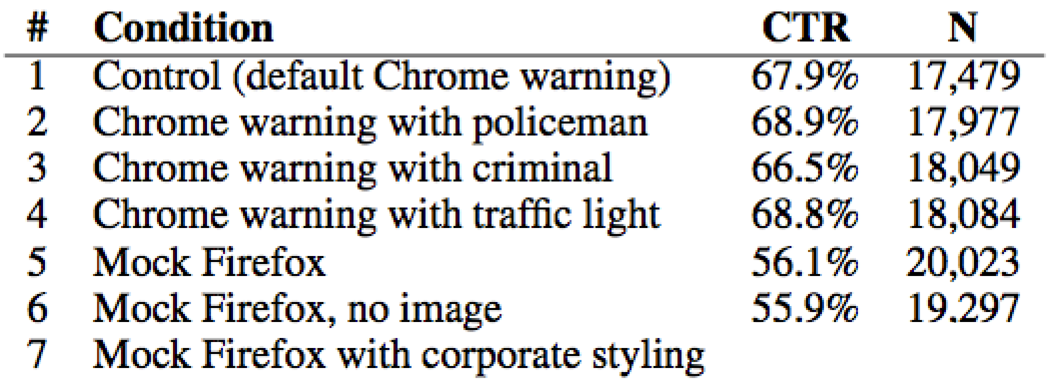


Figure 4. The three images used in Conditions 2-4.

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

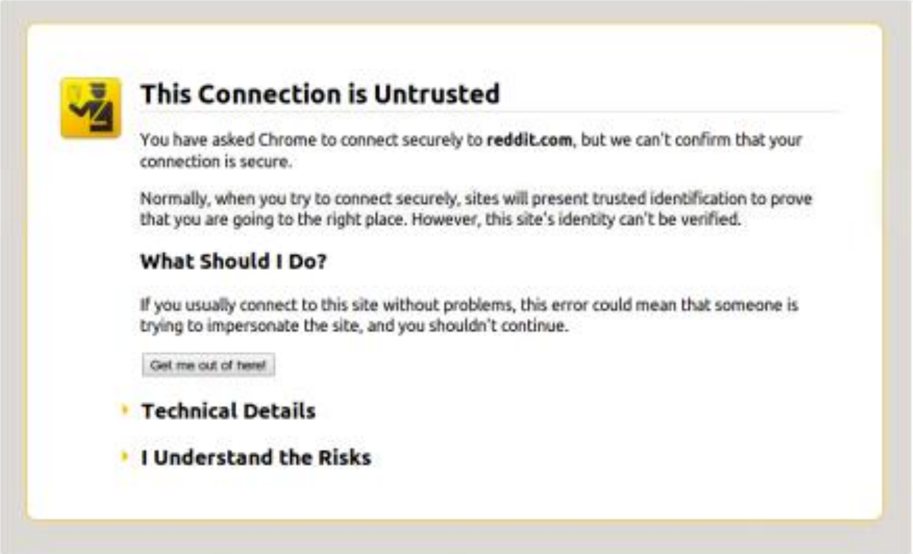
[Felt et al.]

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.

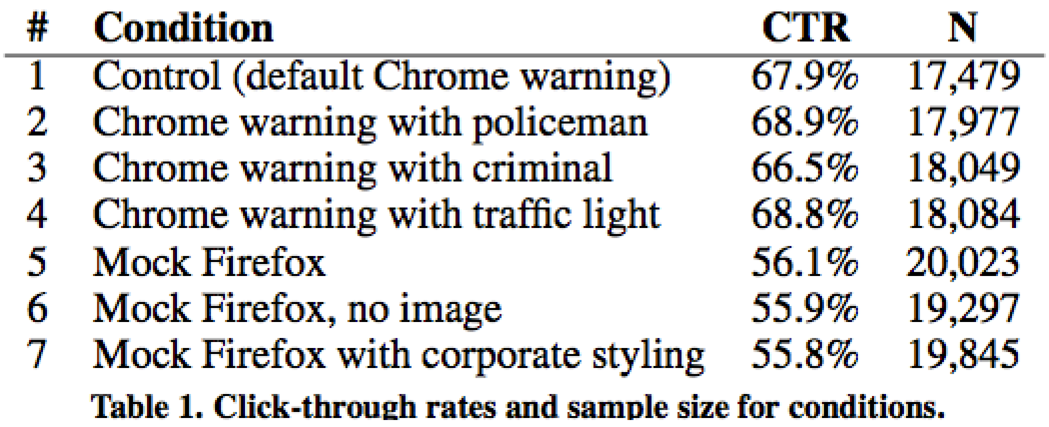
What Should I Do?

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).

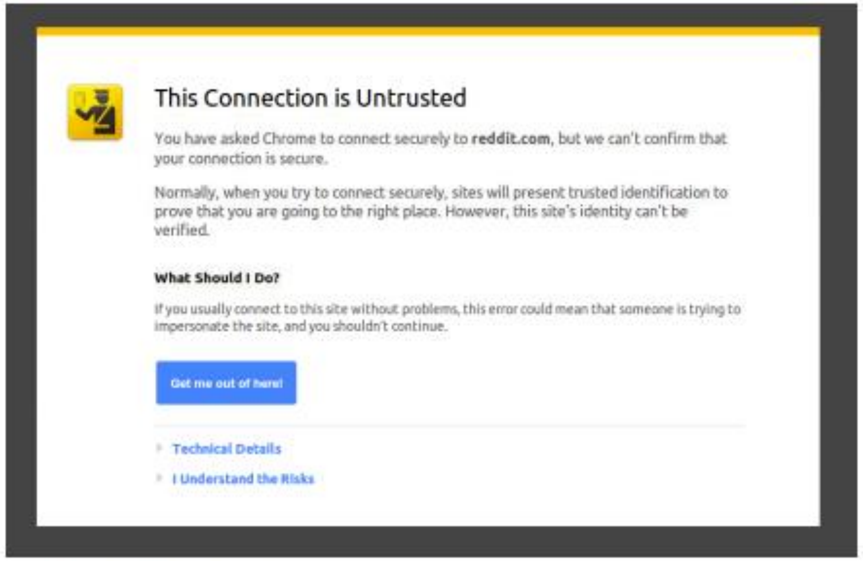
[Felt et al.]

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.

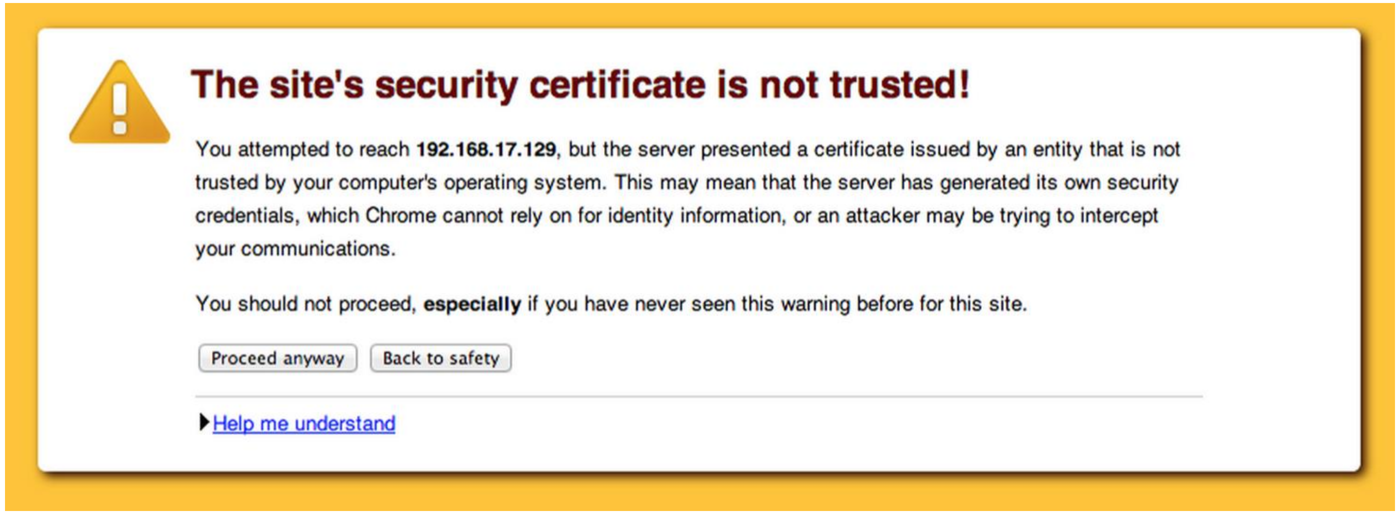
What Should I Do?

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!

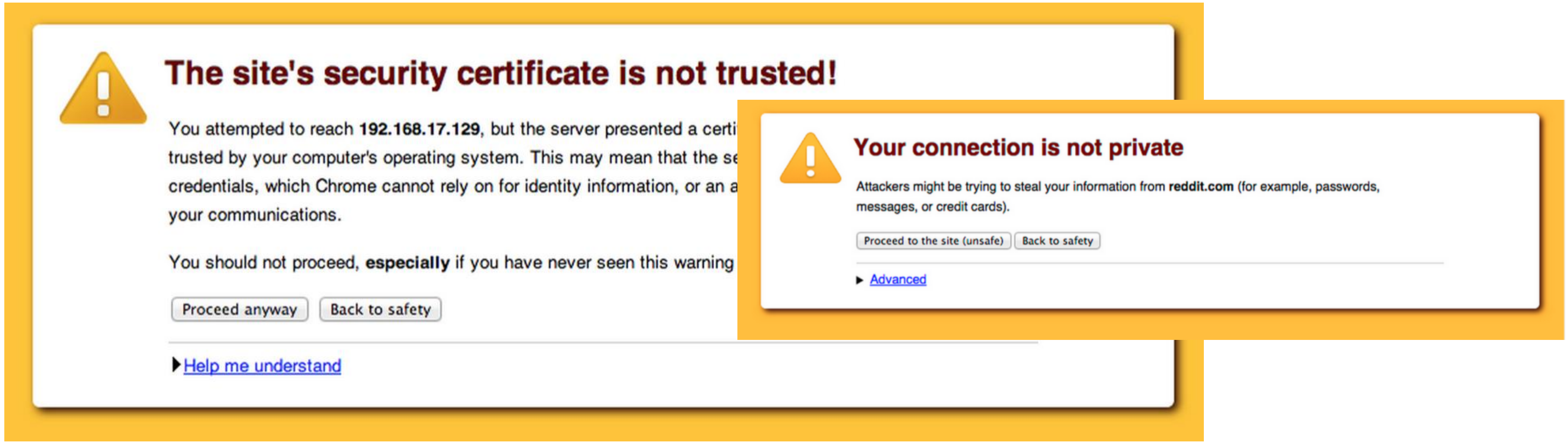
You attempted to reach **192.168.17.129**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Chrome cannot rely on for identity information, or an attacker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



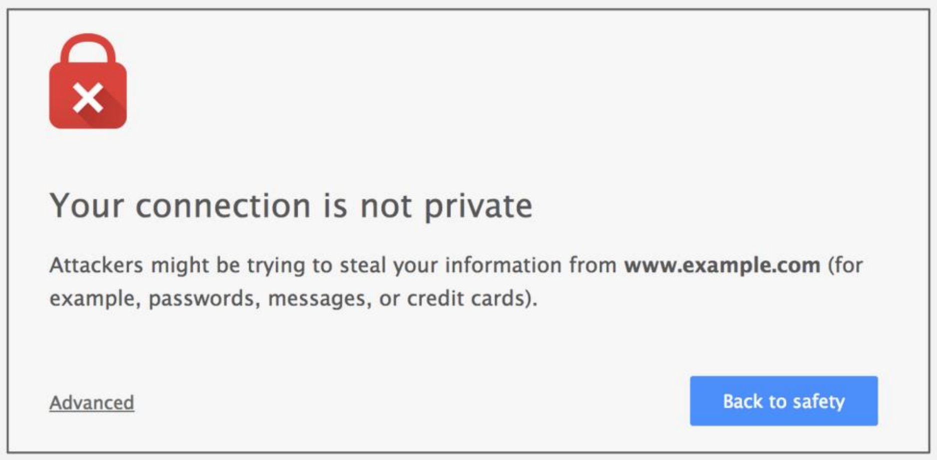
The site's security certificate is not trusted!

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).



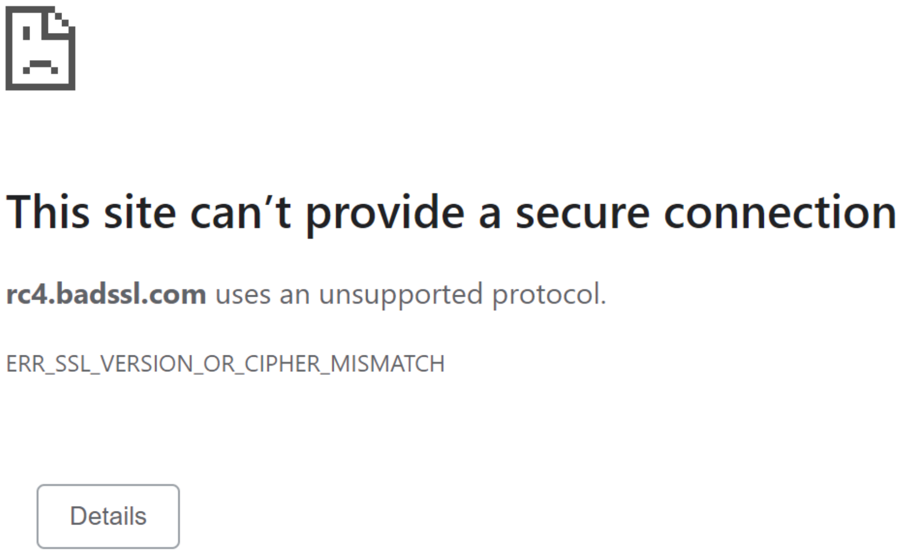
Your connection is not private

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**

Today’s warnings (2022)

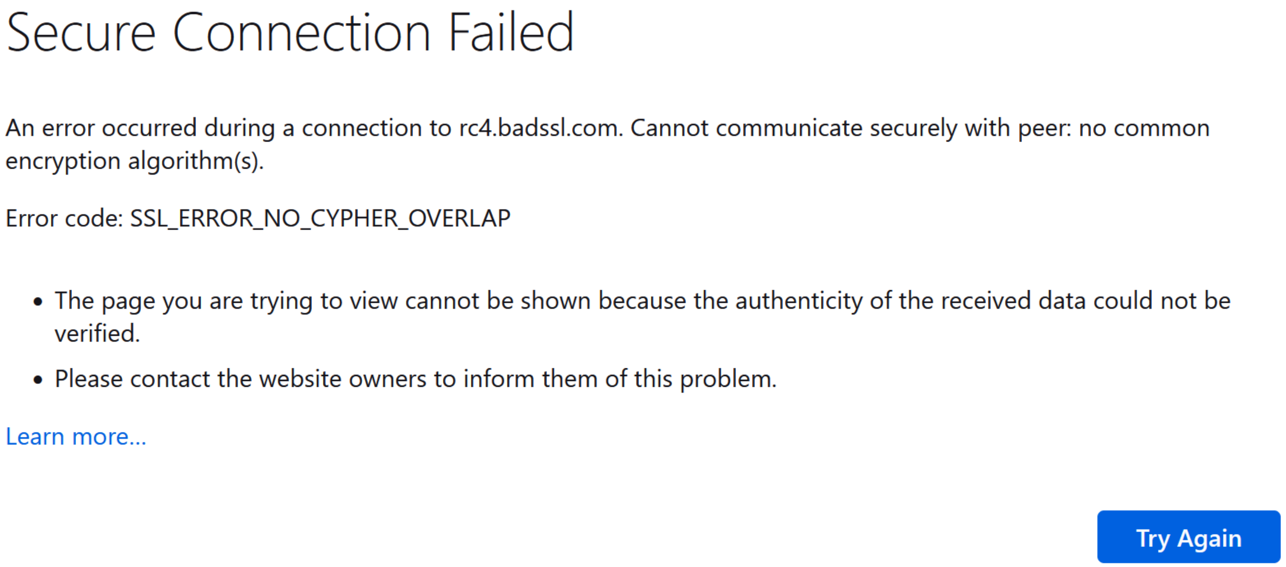
Deprecated encryption schemes



This site can’t provide a secure connection

rc4.badssl.com uses an unsupported protocol.

ERR_SSL_VERSION_OR_CIPHER_MISMATCH



Secure Connection Failed

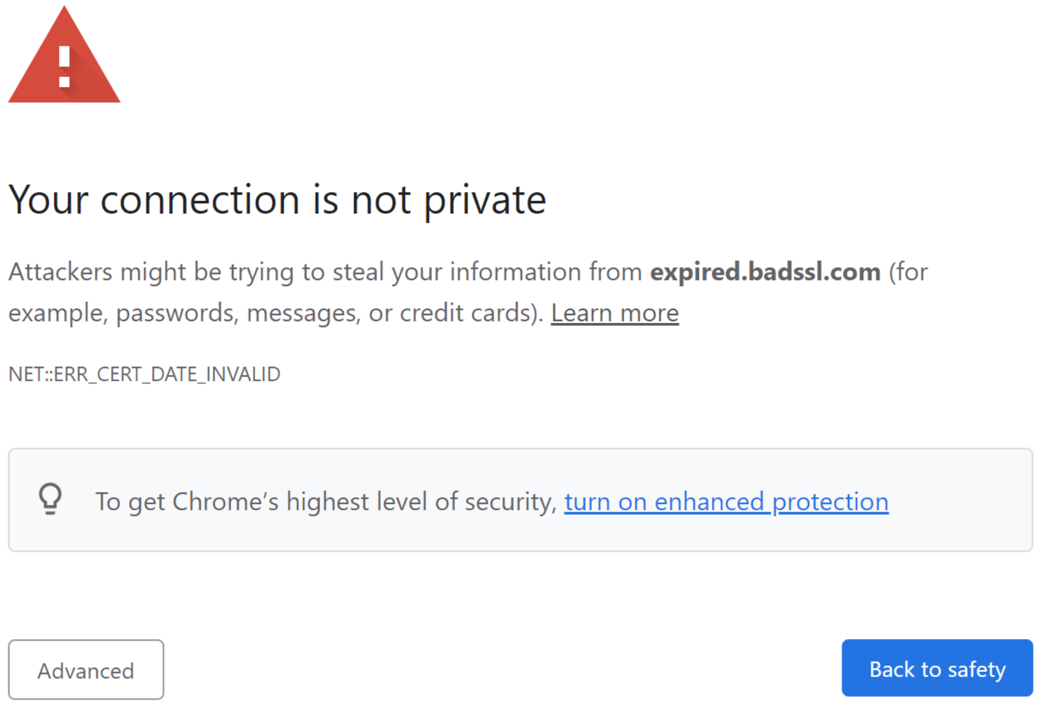
An error occurred during a connection to rc4.badssl.com. Cannot communicate securely with peer: no common encryption algorithm(s).

Error code: SSL_ERROR_NO_CYPHER_OVERLAP

- The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.
- Please contact the website owners to inform them of this problem.

Learn more…

Expired certificates

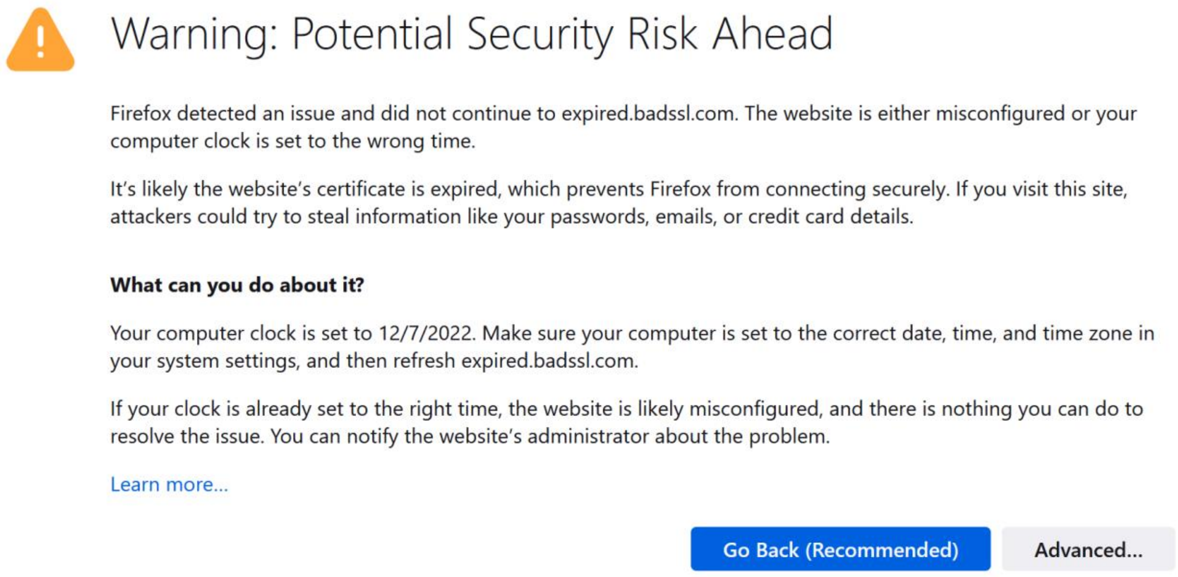


Your connection is not private

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

NET::ERR_CERT_DATE_INVALID

To get Chrome's highest level of security, turn on enhanced protection



Warning: Potential Security Risk Ahead

Firefox detected an issue and did not continue to expired.badssl.com. The website is either misconfigured or your computer clock is set to the wrong time.

It's likely the website's certificate is expired, which prevents Firefox from connecting securely. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

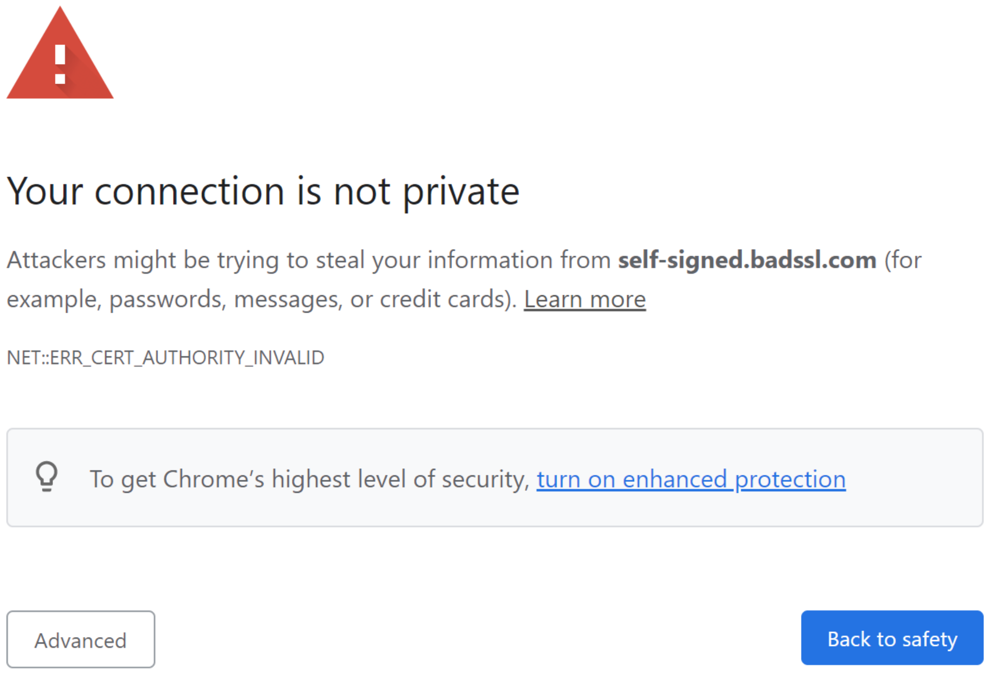
What can you do about it?

Your computer clock is set to 12/7/2022. Make sure your computer is set to the correct date, time, and time zone in your system settings, and then refresh expired.badssl.com.

If your clock is already set to the right time, the website is likely misconfigured, and there is nothing you can do to resolve the issue. You can notify the website's administrator about the problem.

Learn more...

Self-signed certificates

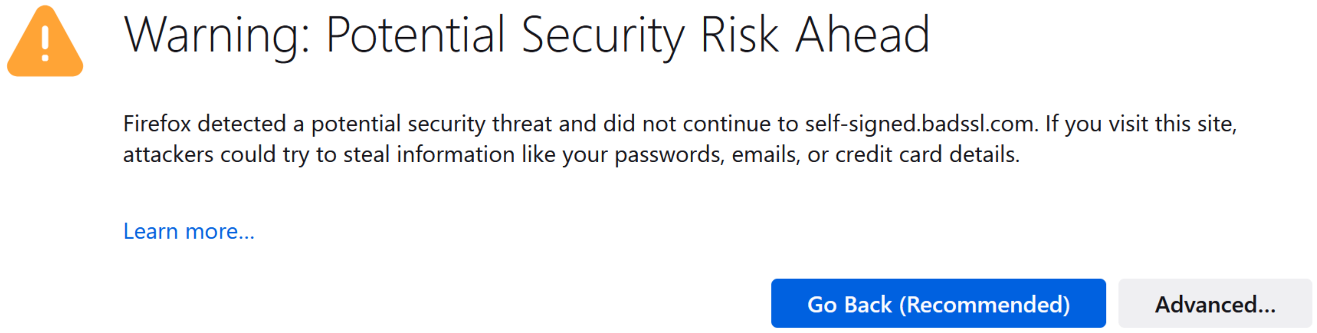


Your connection is not private

Attackers might be trying to steal your information from **self-signed.badssl.com** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

To get Chrome's highest level of security, turn on enhanced protection

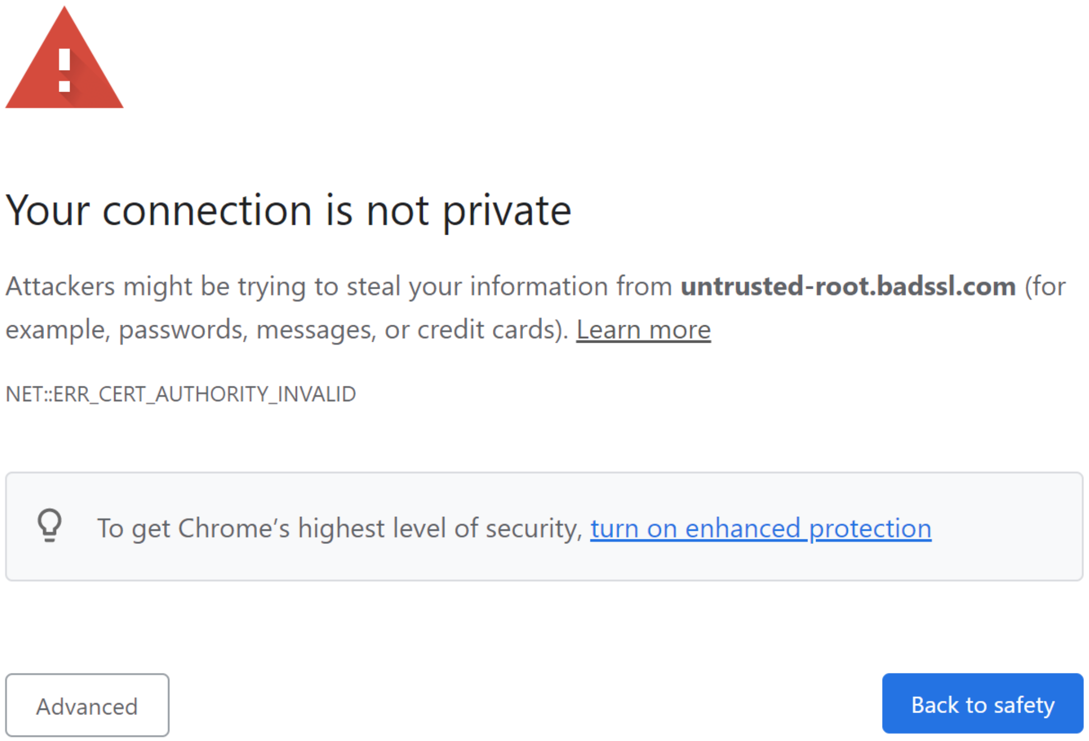


Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to self-signed.badssl.com. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

Learn more…

Untrusted Root certificate

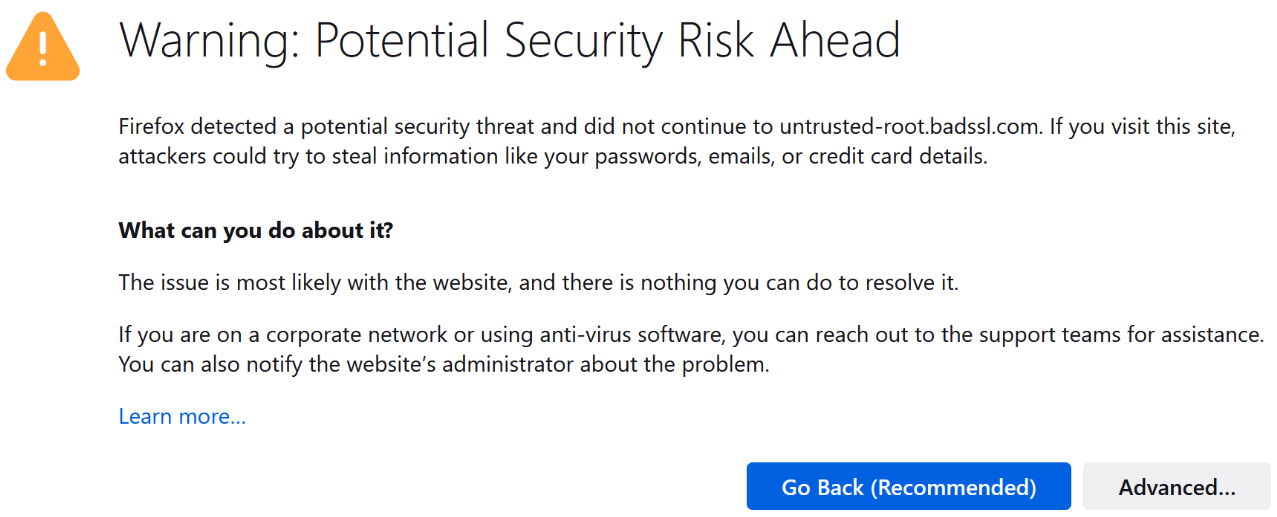


Your connection is not private

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_AUTHORITY_INVALID

To get Chrome's highest level of security, turn on enhanced protection



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to untrusted-root.badssl.com. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

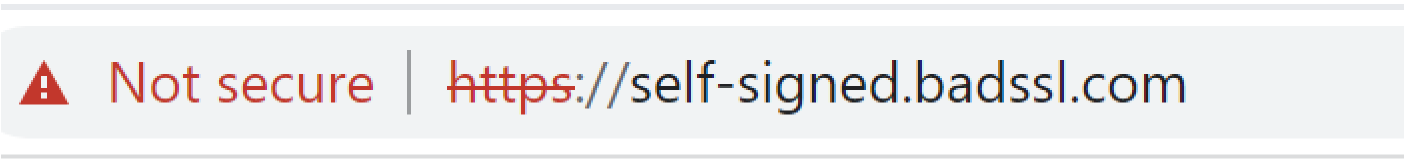
What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it.

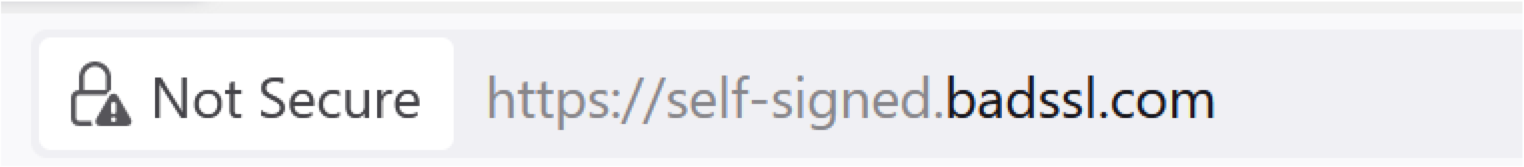
If you are on a corporate network or using anti-virus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

Learn more...

Address Bar behaviors (2022)



⚠ Not secure | ~~https~~://self-signed.badssl.com



Not Secure https://self-signed.badssl.com

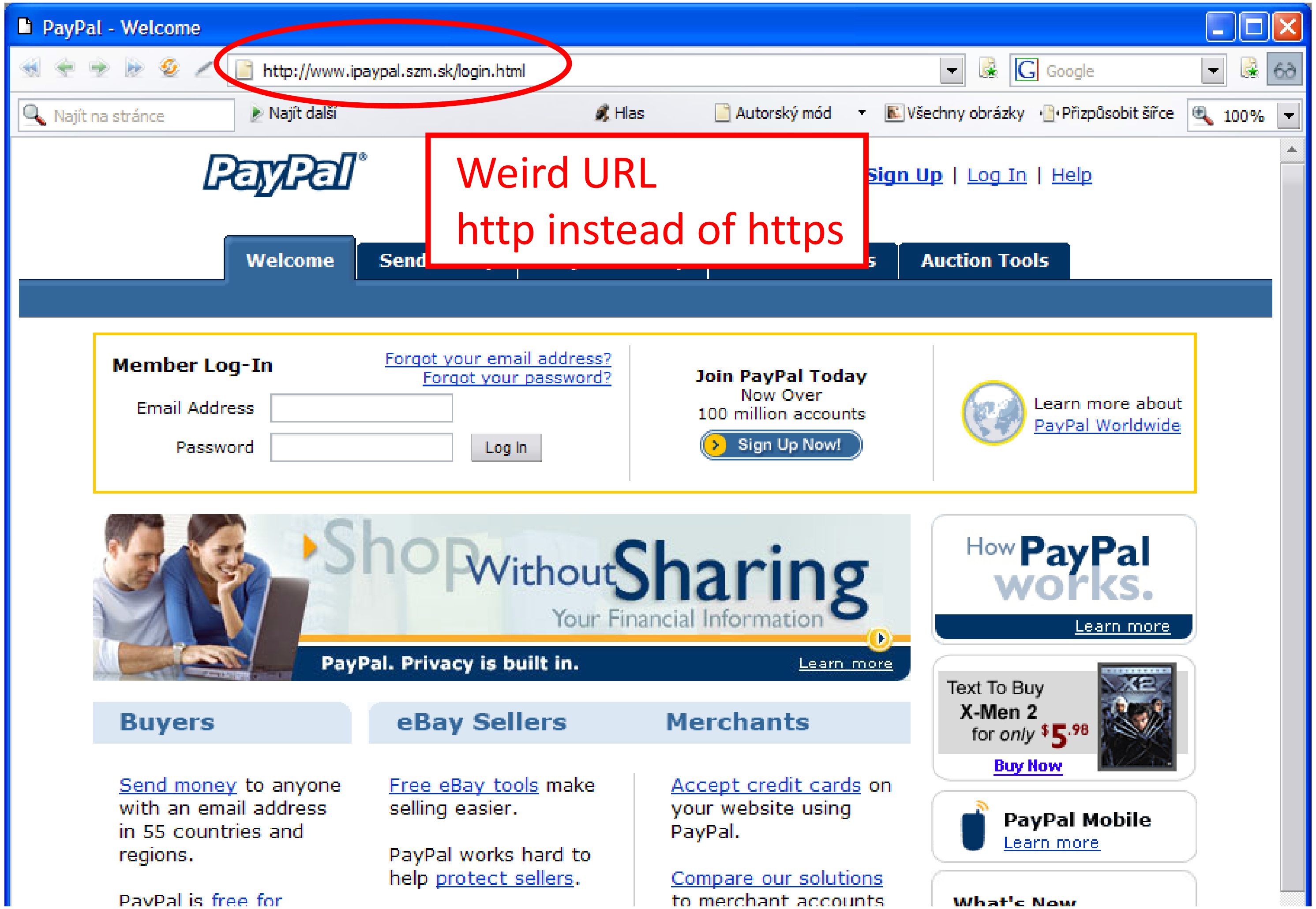
Does anything stand out?

- Pollev
- What makes warnings hard, especially over time?
- Why do Firefox and Chrome make different warning designs?

Case Study #2: Phishing

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

A Typical Phishing Page



Weird URL

http instead of https

PayPal - Welcome

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

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

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.

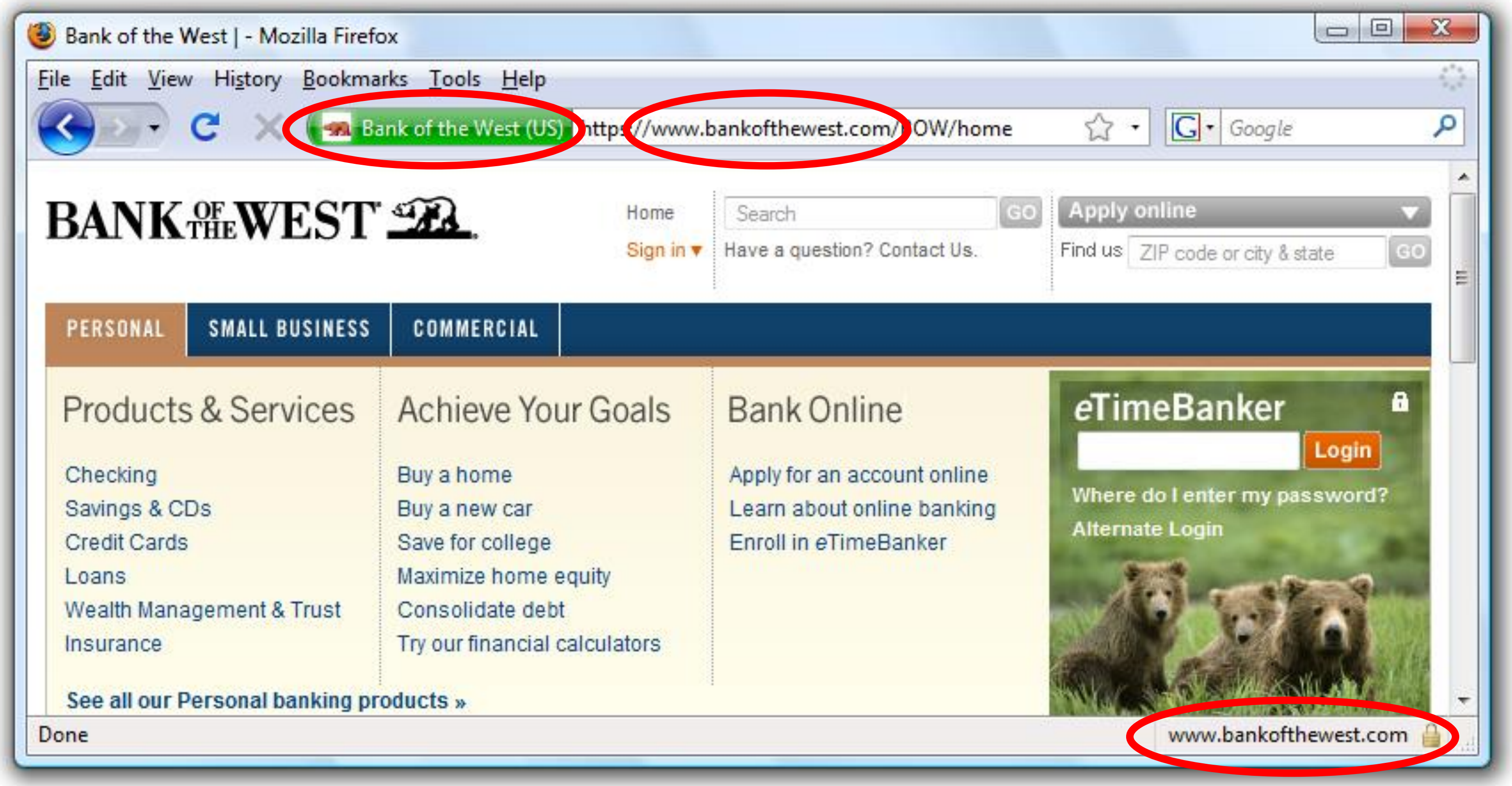
PayPal works hard to help protect sellers.

Merchants

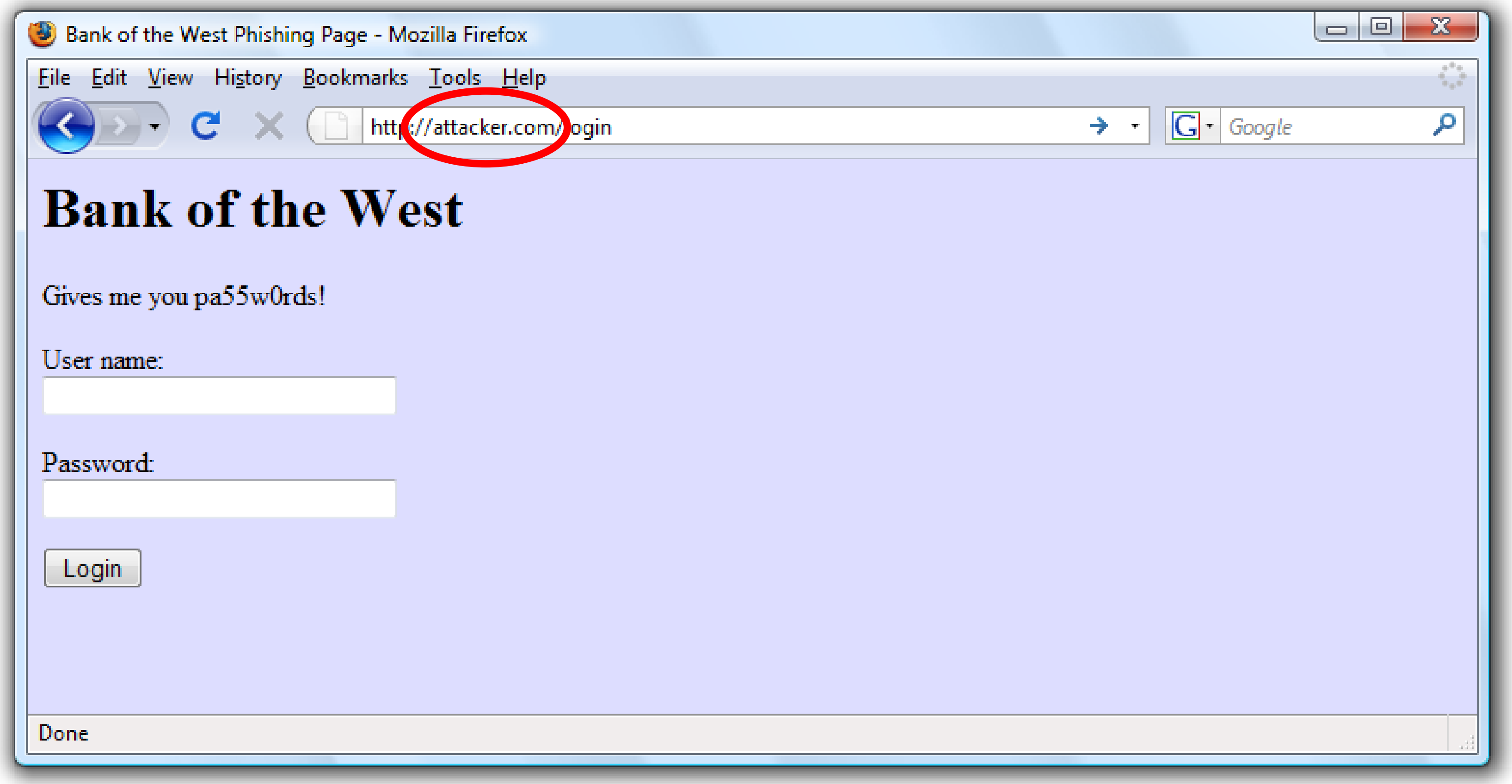
Accept credit cards on your website using PayPal.

Compare our solutions to merchant accounts

Safe to Type Your Password?



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
Done

Bank of the West

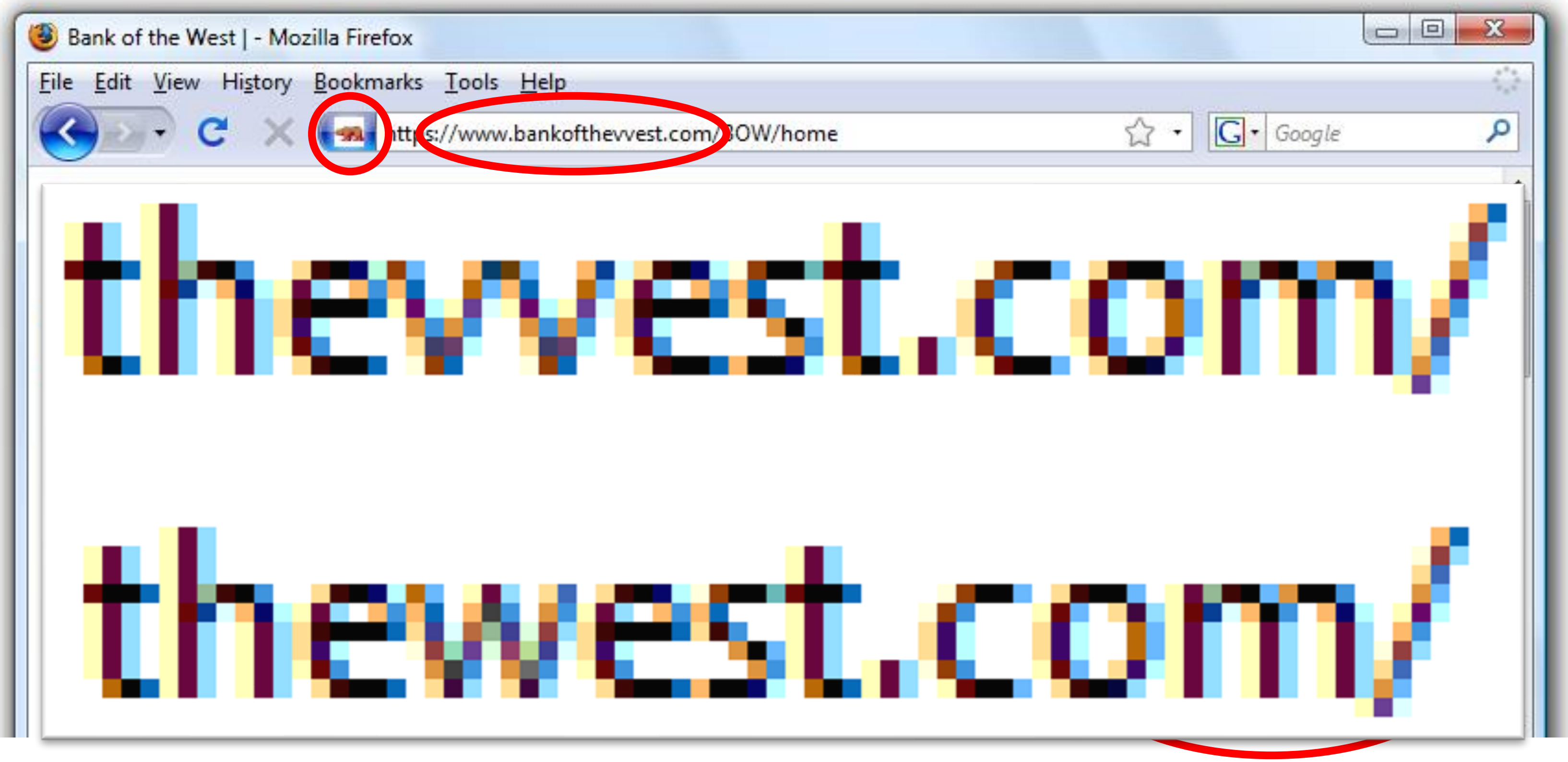
Gives me you pa55w0rds!

User name:

Password:

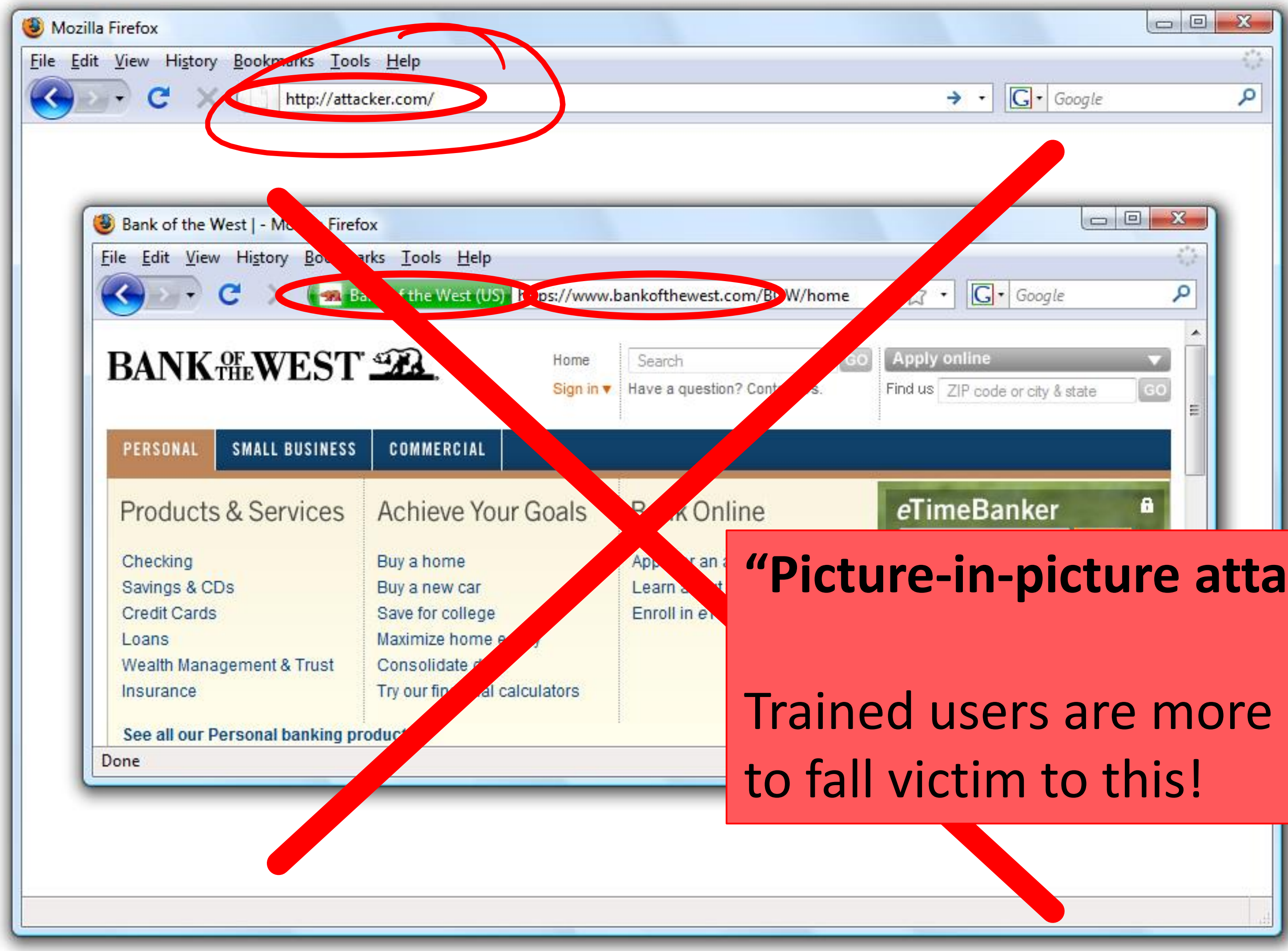
Login

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/

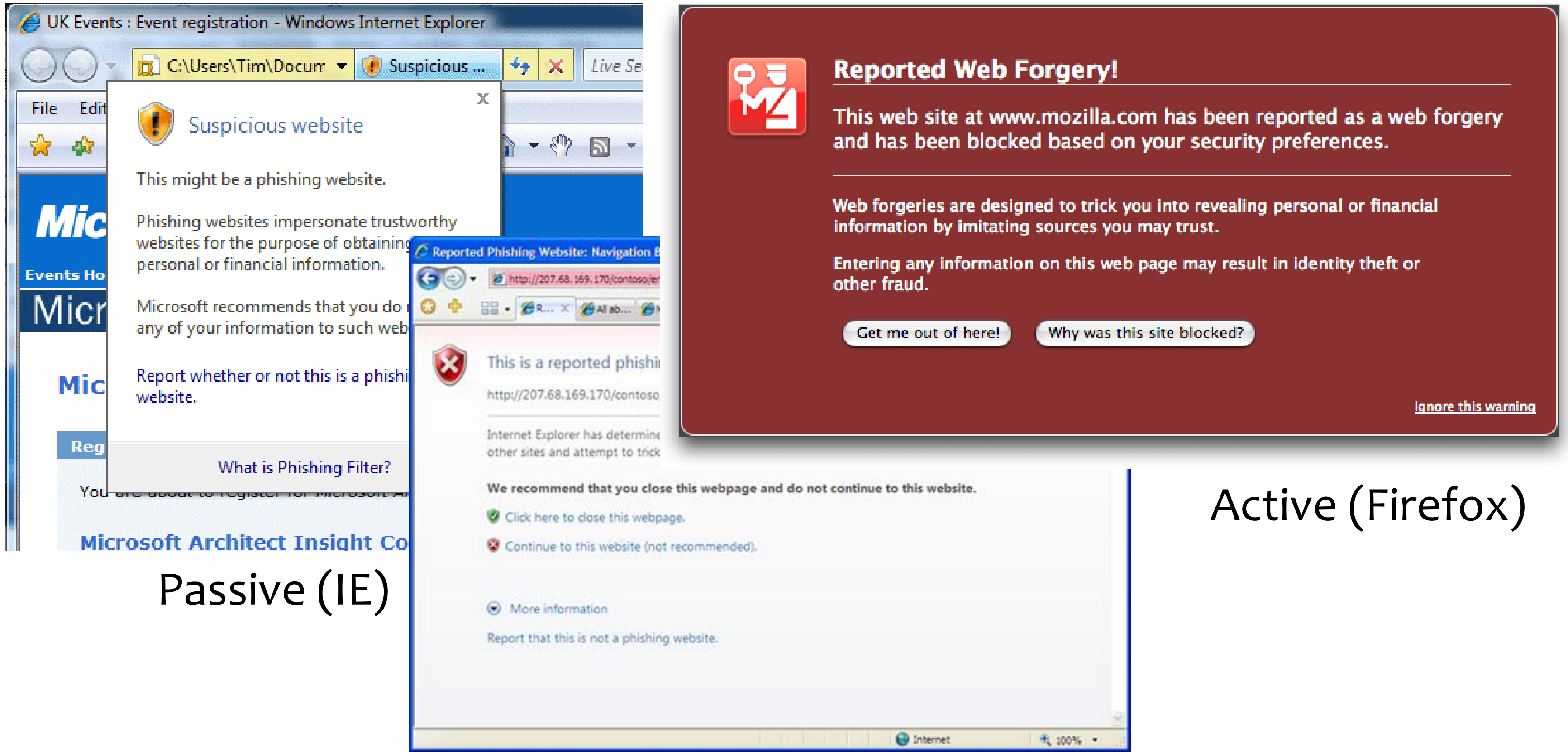
Safe to Type Your Password?



“Picture-in-picture attacks”

Trained users are more likely to fall victim to this!

Phishing Warnings (2008)



UK Events : Event registration - Windows Internet Explorer

Suspicious website

This might be a phishing website.

Phishing websites impersonate trustworthy websites for the purpose of obtainin 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?

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

Passive (IE)

Reported Phishing Website: Navigation B

This is a reported phishi

http://207.68.169.170/contoso

Internet Explorer has determin 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.

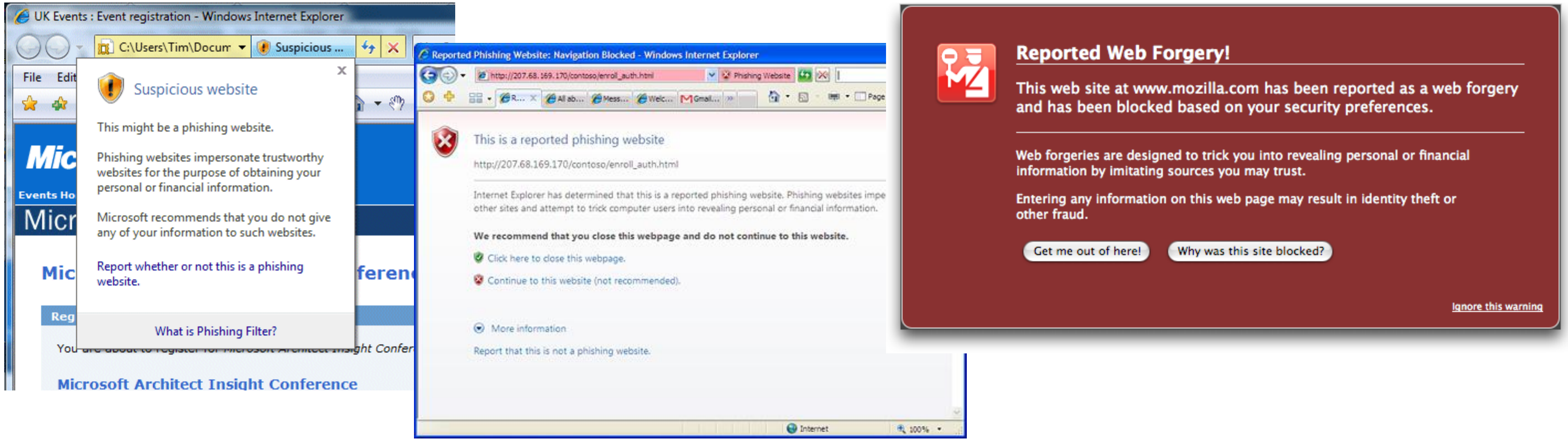
Entering any information on this web page may result in identity theft or other fraud.

Active (Firefox)

[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?

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.

Reported Web Forgery!

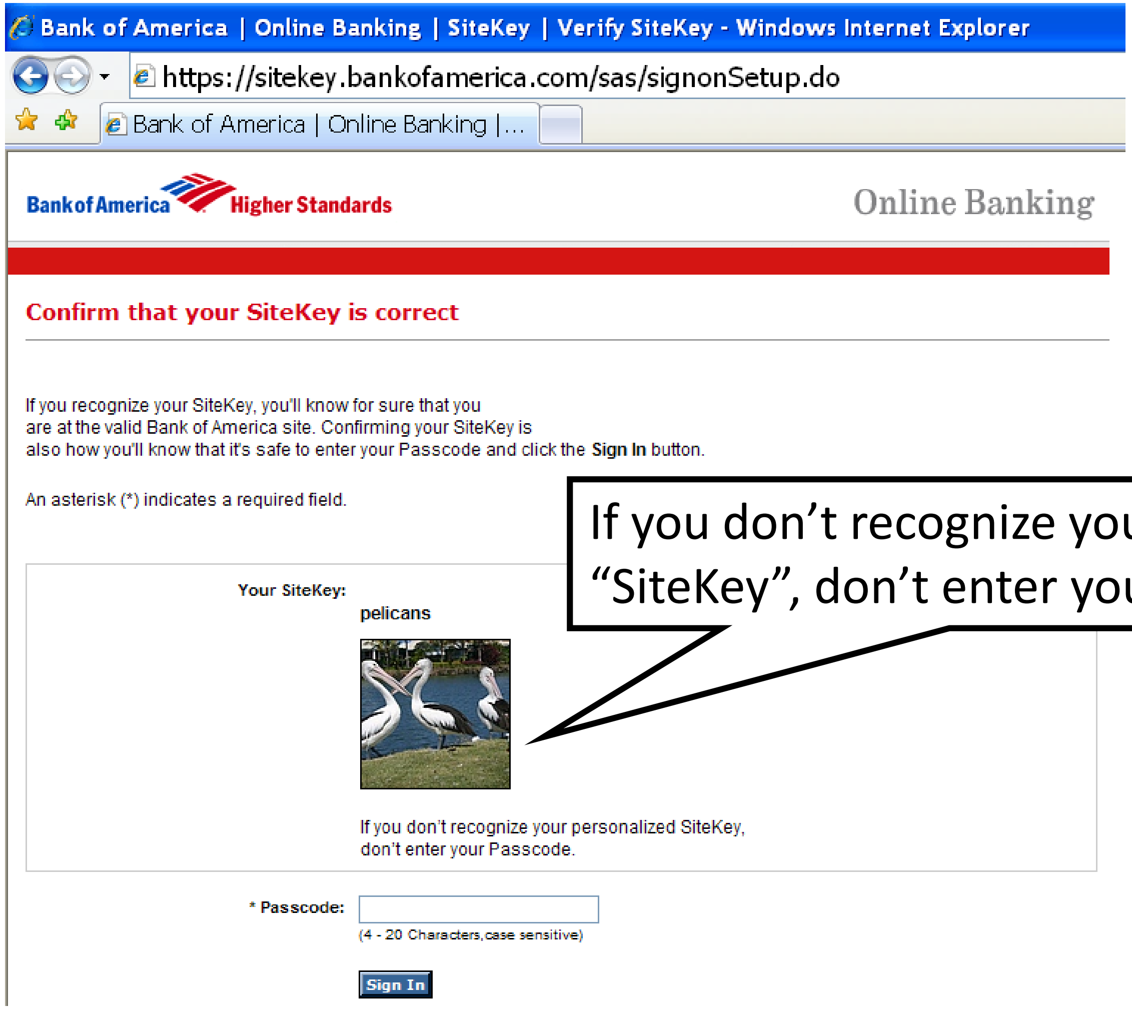
This web site at www.mozilla.com has been reported as a web forgery and has been blocked based on your security preferences.

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)

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)

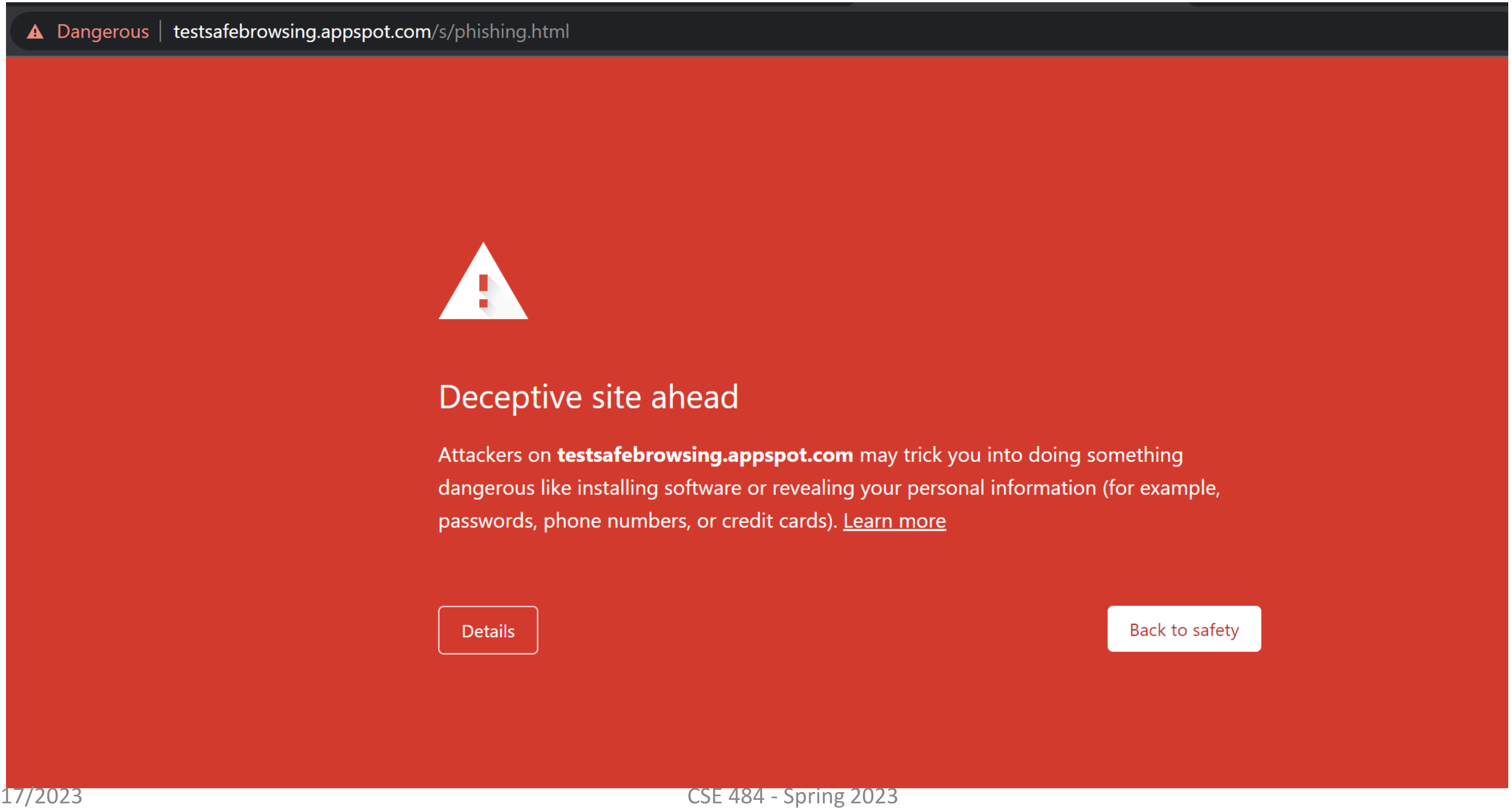
Sign In

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

Modern anti-phishing

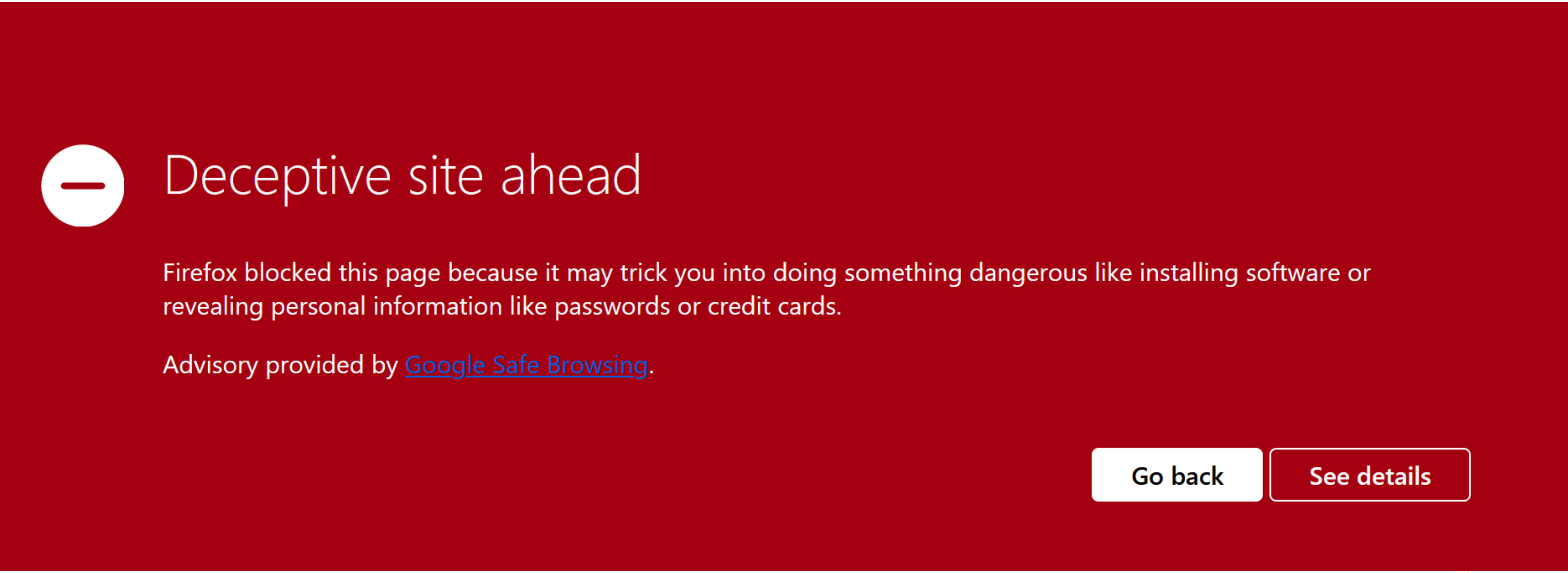
- Largely driven by Google Safe Browsing
  - Browser sends 32-bit prefix of hash(url)
  - API says: good or bad

Modern warnings



Deceptive site ahead

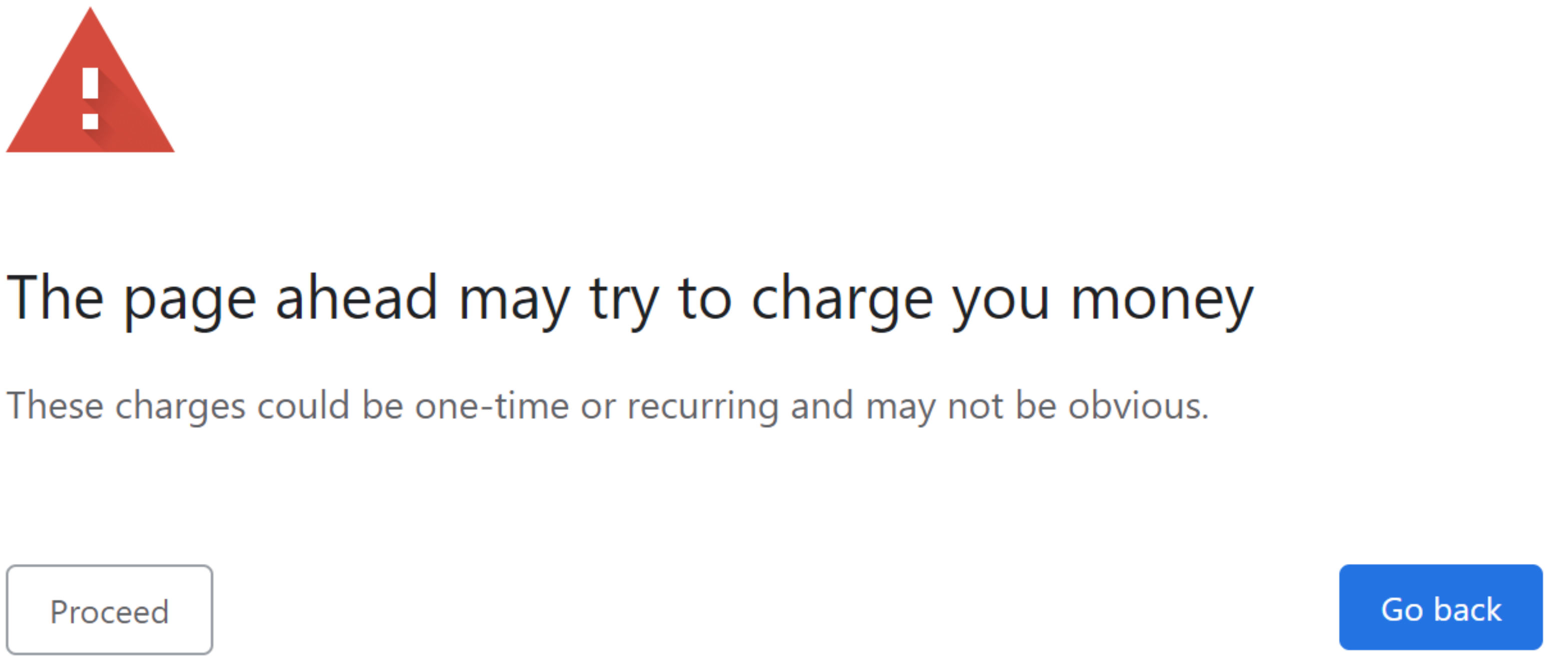
Attackers on **testsafebrowsing.appspot.com** may trick you into doing something dangerous like installing software or revealing your personal information (for example, passwords, phone numbers, or credit cards). Learn more



Deceptive site ahead

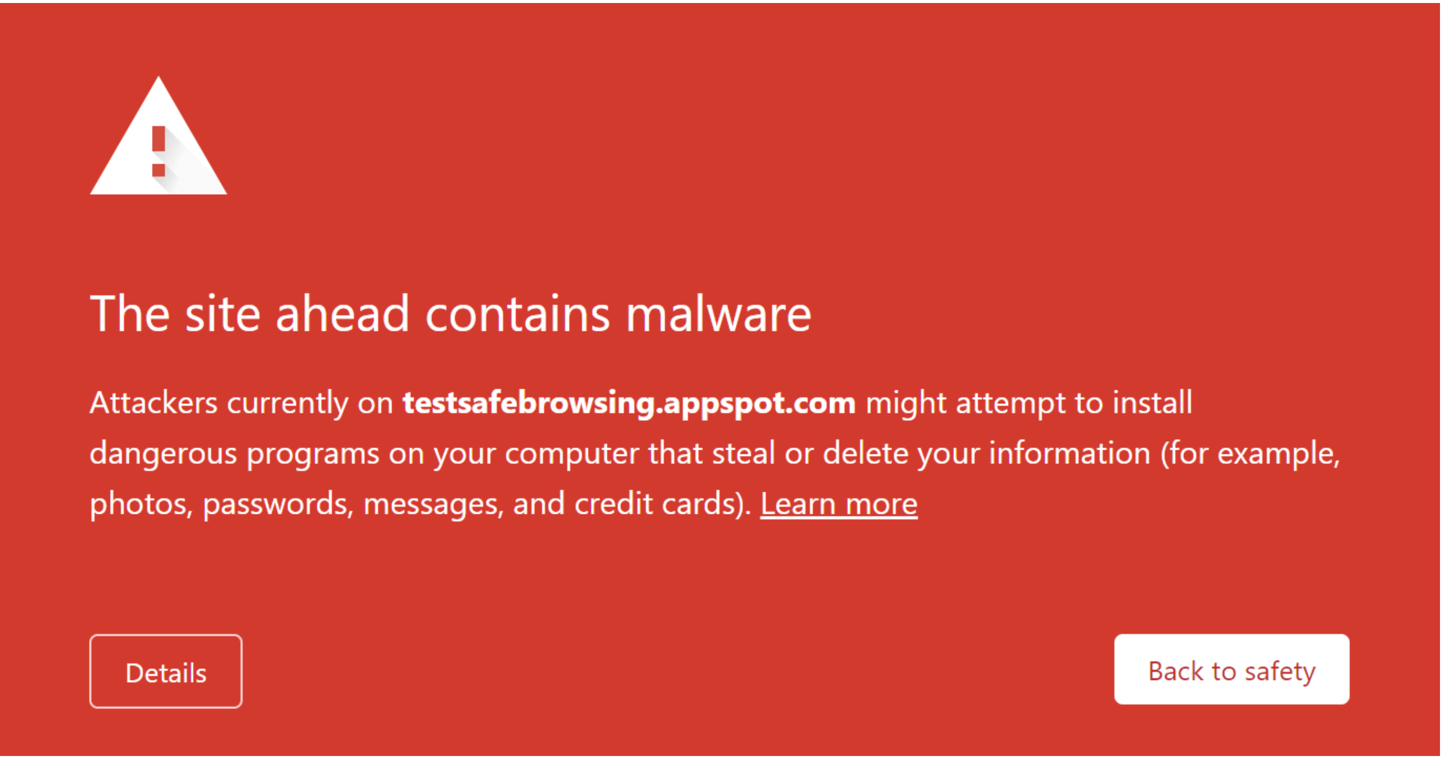
Firefox blocked this page because it may trick you into doing something dangerous like installing software or revealing personal information like passwords or credit cards.

Advisory provided by Google Safe Browsing.



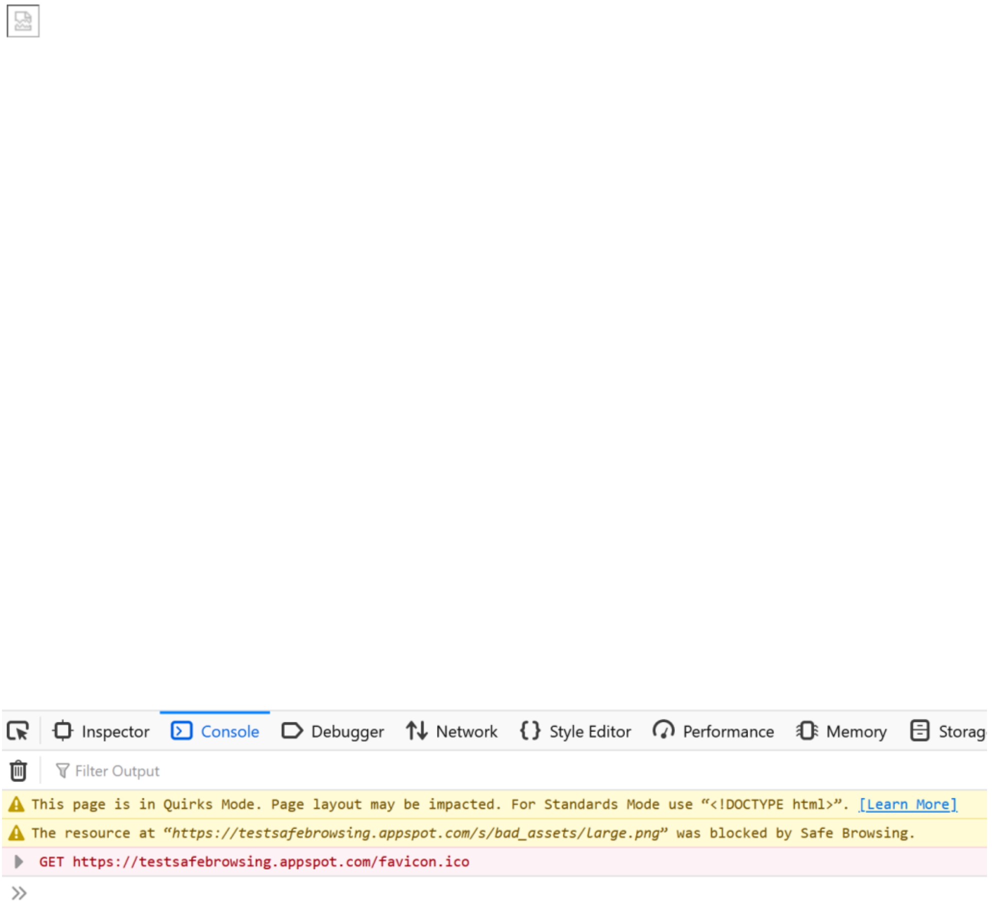
The page ahead may try to charge you money

These charges could be one-time or recurring and may not be obvious.



The site ahead contains malware

Attackers currently on **testsafebrowsing.appspot.com** might attempt to install dangerous programs on your computer that steal or delete your information (for example, photos, passwords, messages, and credit cards). Learn more



```
This page is in Quirks Mode. Page layout may be impacted. For Standards Mode use “<!DOCTYPE html>”. [Learn More]
The resource at “https://testsafebrowsing.appspot.com/s/bad_assets/large.png” was blocked by Safe Browsing.
GET https://testsafebrowsing.appspot.com/favicon.ico
»
```

Which warning is ‘better’?

- For user security?
- For user agency?
- For user understanding?
- For… what?