CSE 484: Computer Security and Privacy

Anonymity + Usability

Spring 2024

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 ...

Career Panel May 21st 4-5pm, Room G0 Gates

Join us for an engaging panel of Allen School Alumni, presenting on working in tech for companies beyond the 'usual suspects: i.e. Microsoft, Google, etc' (Edstem Post: https://edstem.org/us/courses/488/discussion/4918007)

- **Please RSVP if you're interested** so you can let us know initial questions you want to see addressed. This will not be recorded so you do need to attend **in person** for this event.
- **Panelists:**
  - Erin Peach with Kraken, Software Engineer, BSMS and ugrad at Allen School, previously worked at Code.org and Obama Foundation (two non profits
  - Han Sarayli: Soft Dev Manager Blue Crew, previously at Zulily, Bellevue College Transfer Student, Allen School Ugrad
  - David Dawson: Co Founder and Head of Engineering, Ridwell, previously at Spruce Up, Inc and ShareGrid, Allen School Ugrad

Logistics

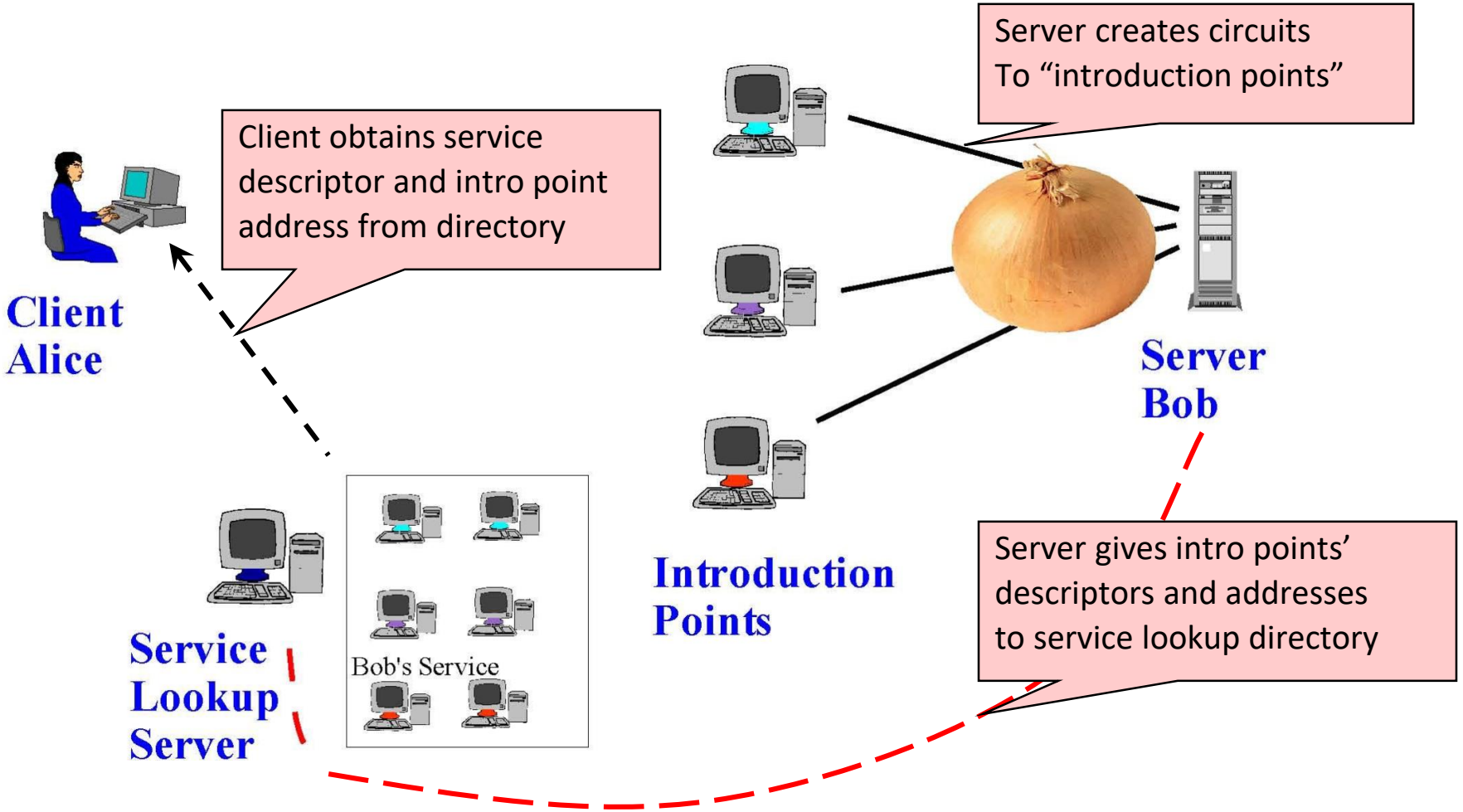
- Final Project Part A due Wednesday
  - Make sure your patch passes the gradescope autograder
  - Think about what your patch does with valid and invalid Host: headers
  - Consider what the range of valid Host: headers is
    - Note: you don't need to make tinyserv better than it was, just prevent exploitation
  - Please make your forks private!

- Double-check your patch: it is a human-readable file
  - We had a ton of groups with incorrect lab1b handins

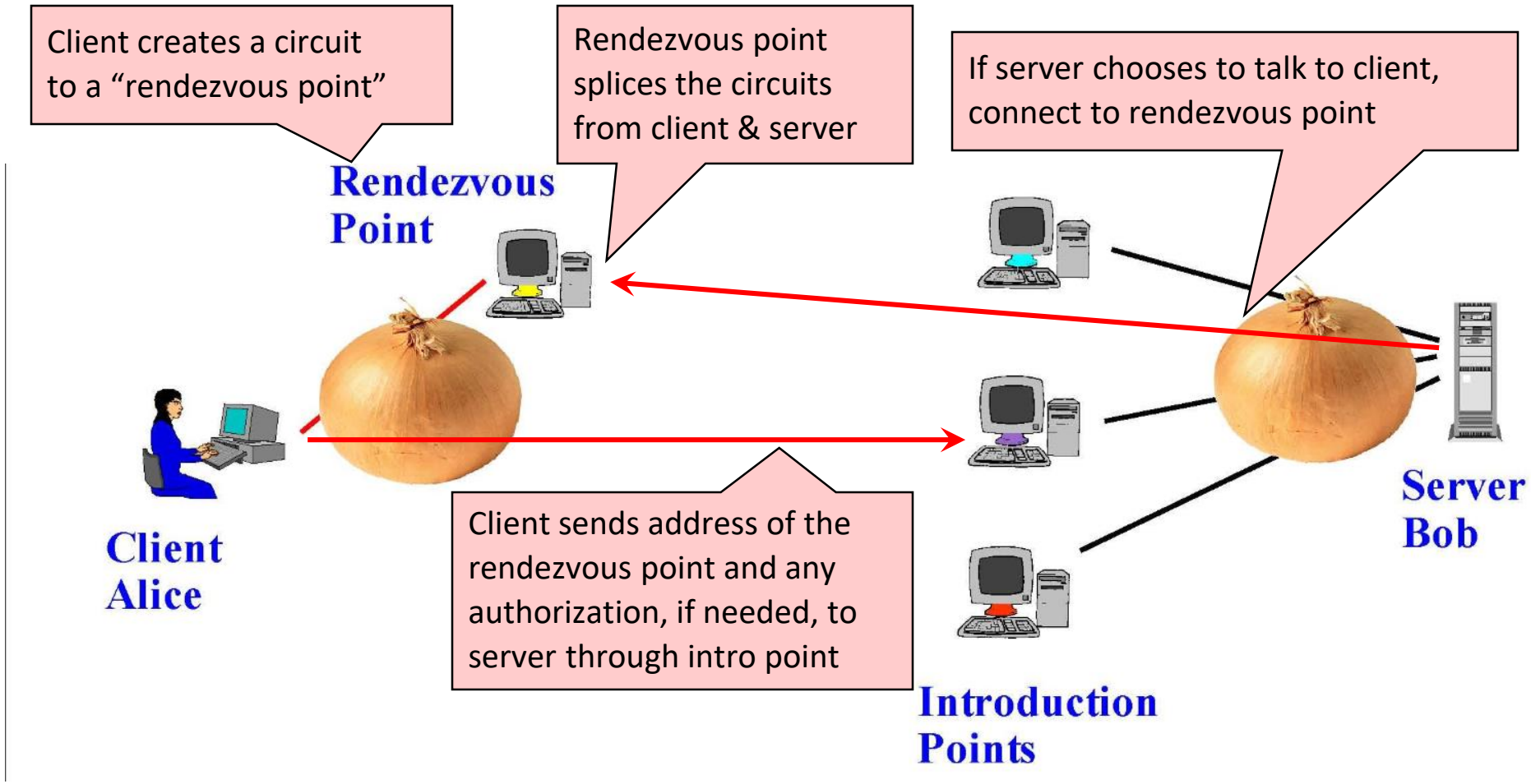
Location Hidden Service

- **Goal:** deploy a server on the Internet that anyone can connect to without knowing where it is or who runs it
- Accessible from anywhere
- Resistant to censorship
- Can survive a full-blown DoS attack
- Resistant to physical attack
  - Can't find the physical server!

Creating a Location Hidden Server



Using a Location Hidden Server

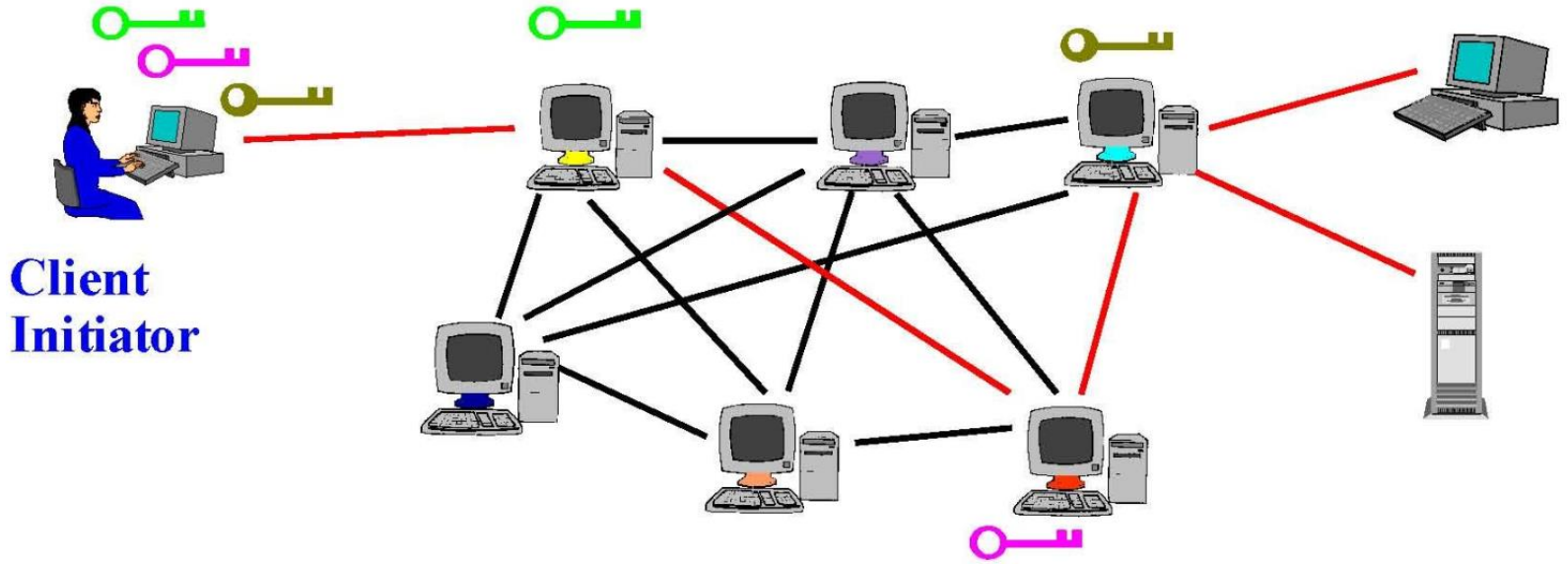


Issues and Notes of Caution

- 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)

Aside -- HDCP

Problem: People like copying movies!

- Solution: DRM (Digital Rights Management)
  - DVD players, Streaming service plugins, etc
  - Encrypt video in-transit, decrypt on device

Problem: People like copying movies!

- Solution: DRM (Digital Rights Management)
  - DVD players, Streaming service plugins, etc
  - Encrypt video in-transit, decrypt on device

- Problem: The *analog hole* – You have to display the context eventually

Problem: Analog Hole

- Solution: … The same thing again – DRM
  - HDCP -- High-bandwidth Digital Content Protection
  - Encrypt data on the wire between the computer output and the monitor
  - Just need to have a trusted chip on the sender (output) and the receiver (display)

Problem: Wait…

Usability and Security

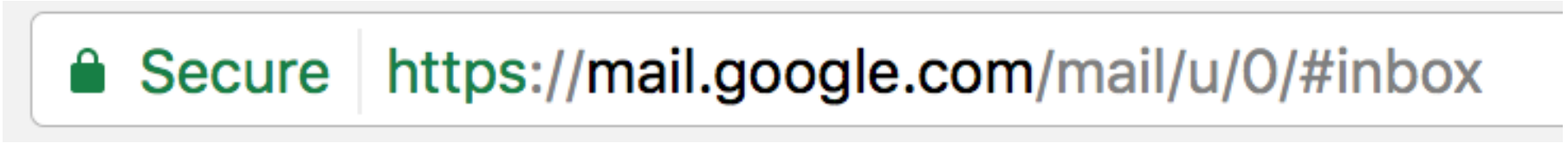
Importance of Usability in Security

- 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 – Done in section, will summarize
  - Phishing
- Step back: root causes of usability problems, and how to address

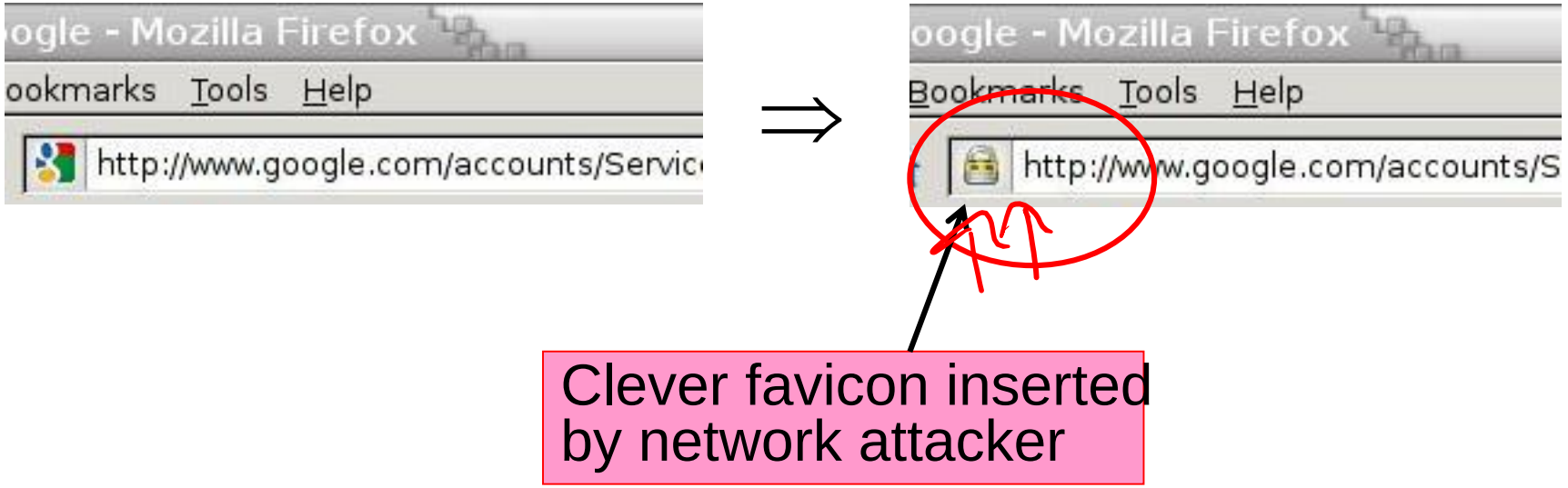
The Lock Icon



- 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

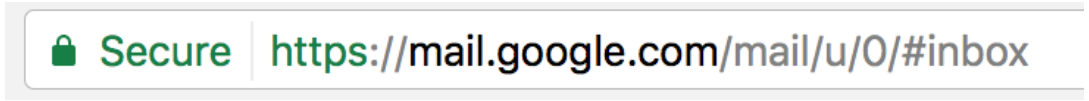
[Moxie Marlinspike]

Will You Notice?

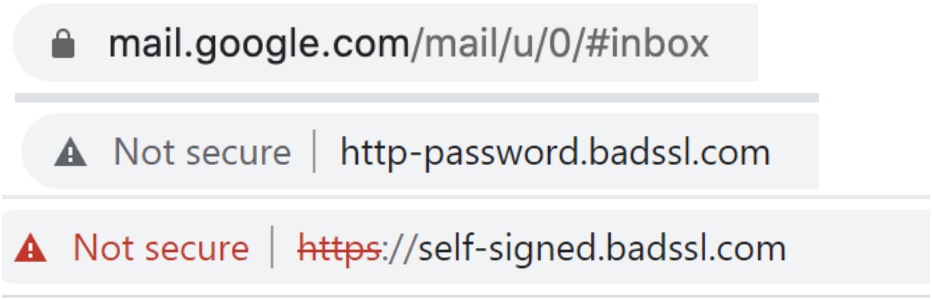


Newer Versions of Chrome

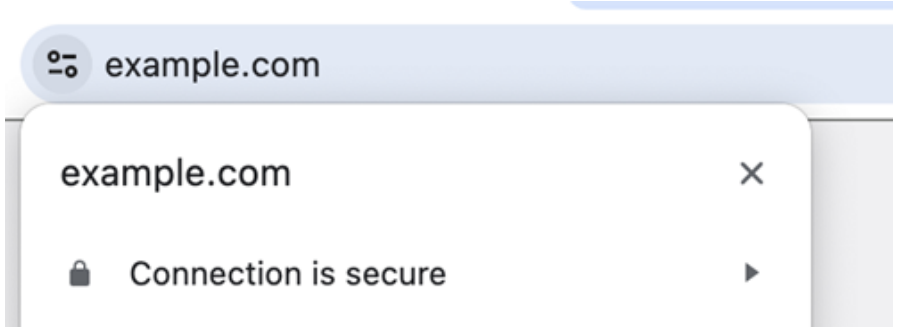
c. 2017



2022



2023/2024



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

Details

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...

Try Again

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

Advanced

Back to safety

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...

Go Back (Recommended)

Advanced...

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

Advanced

Back to safety

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...

Go Back (Recommended)

Advanced...

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

Advanced

Back to safety

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...

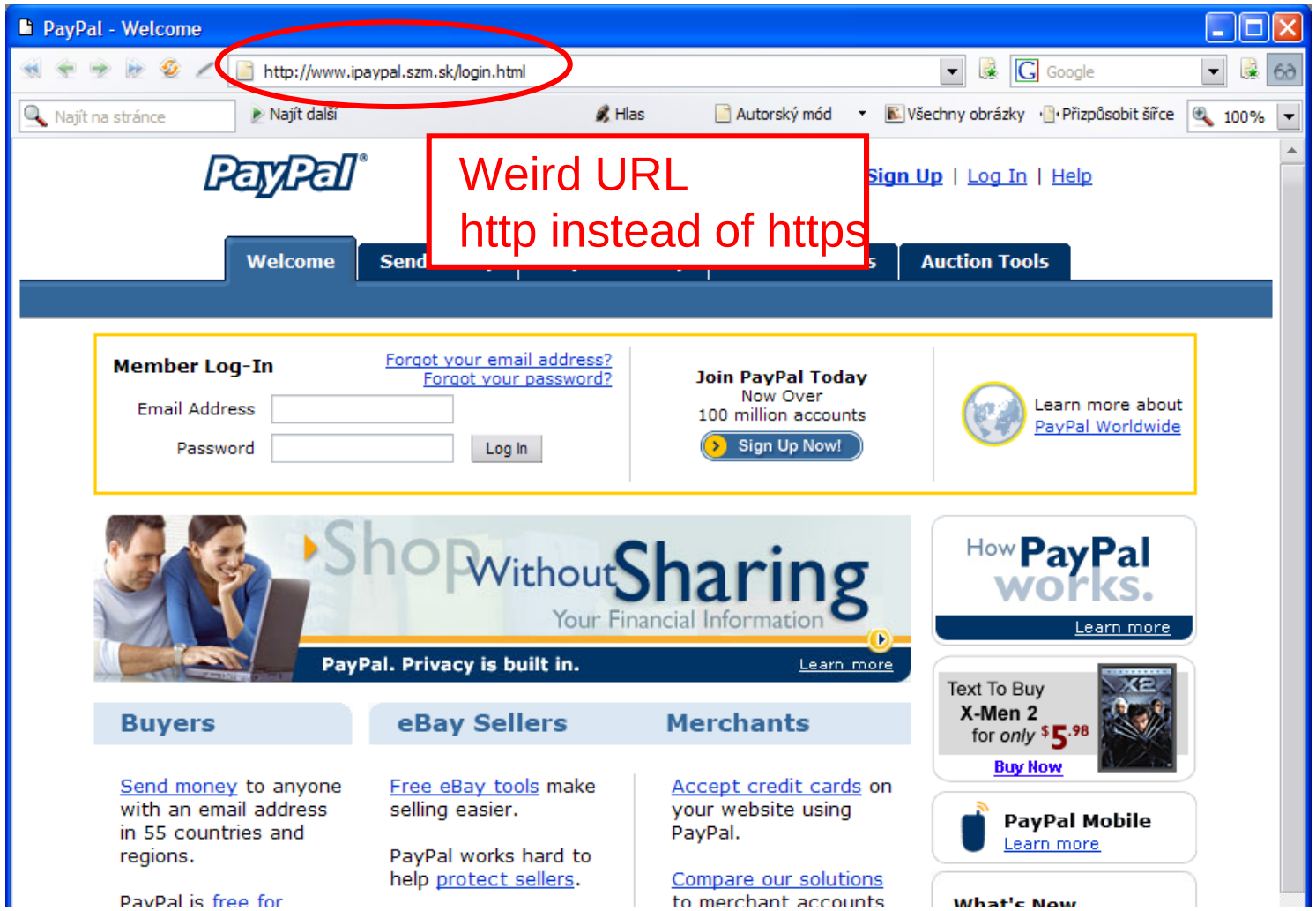
Go Back (Recommended)

Advanced...

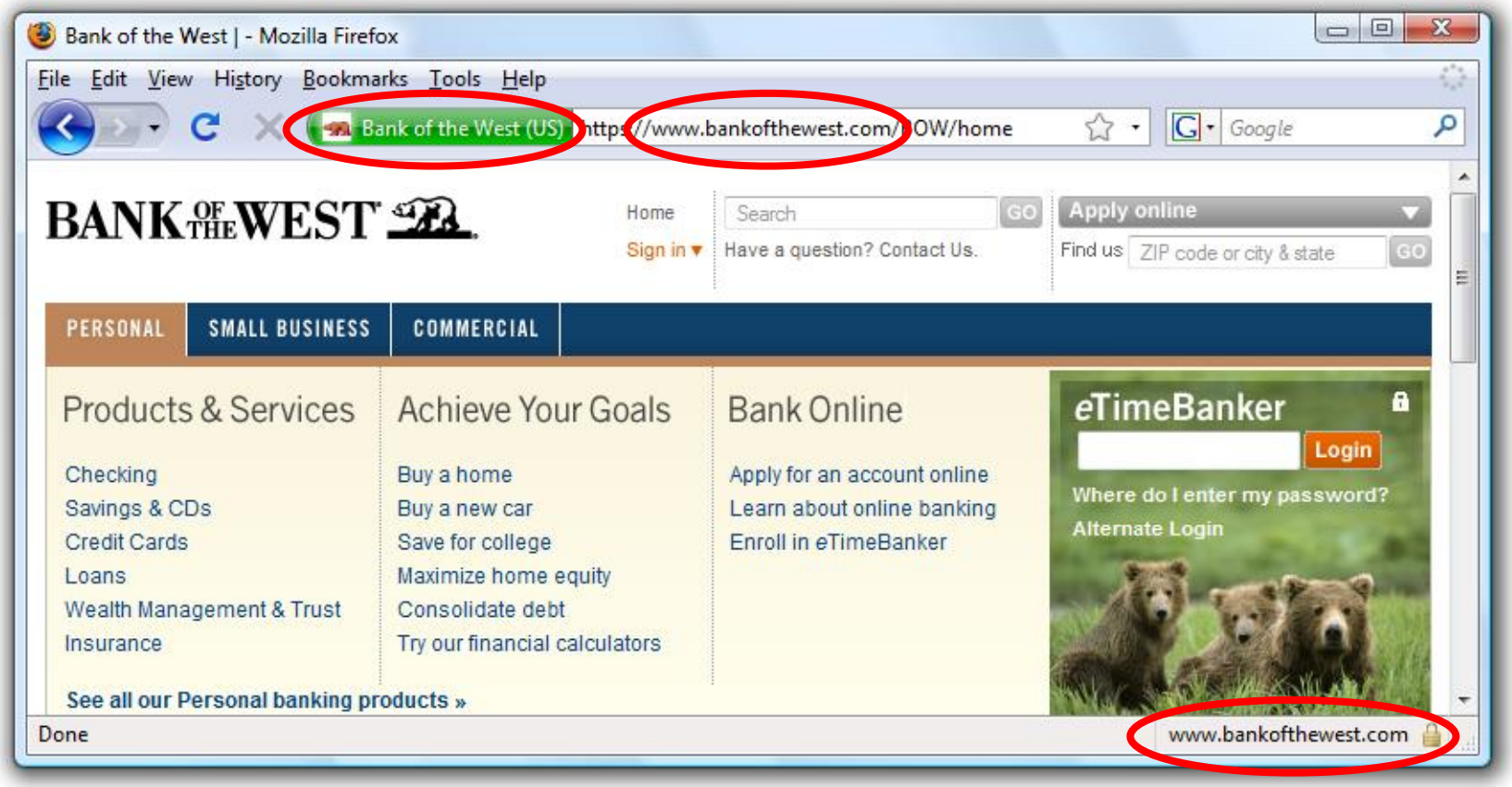
Case Study #2: Phishing

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

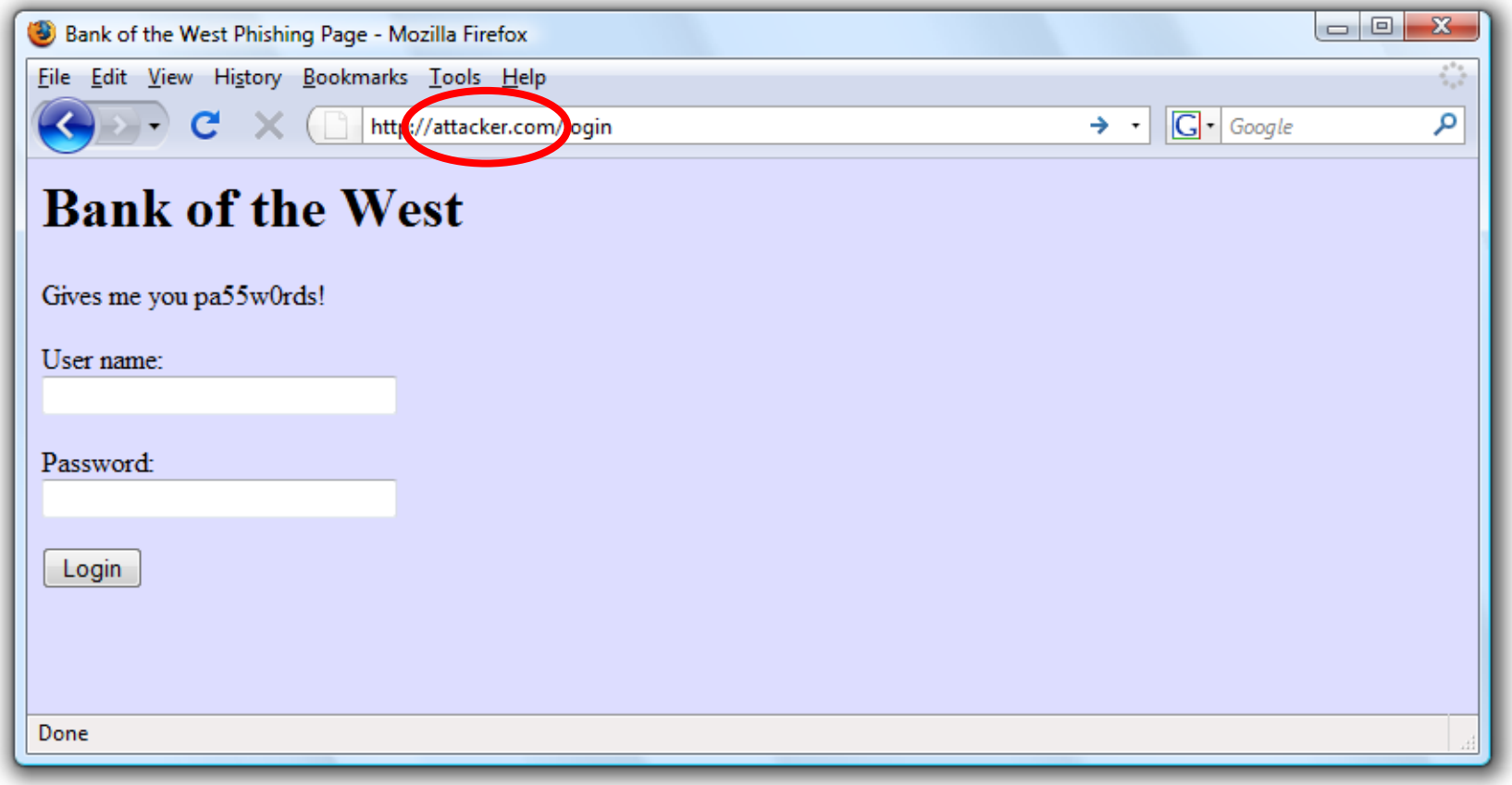
A Typical Phishing Page



Safe to Type Your Password?

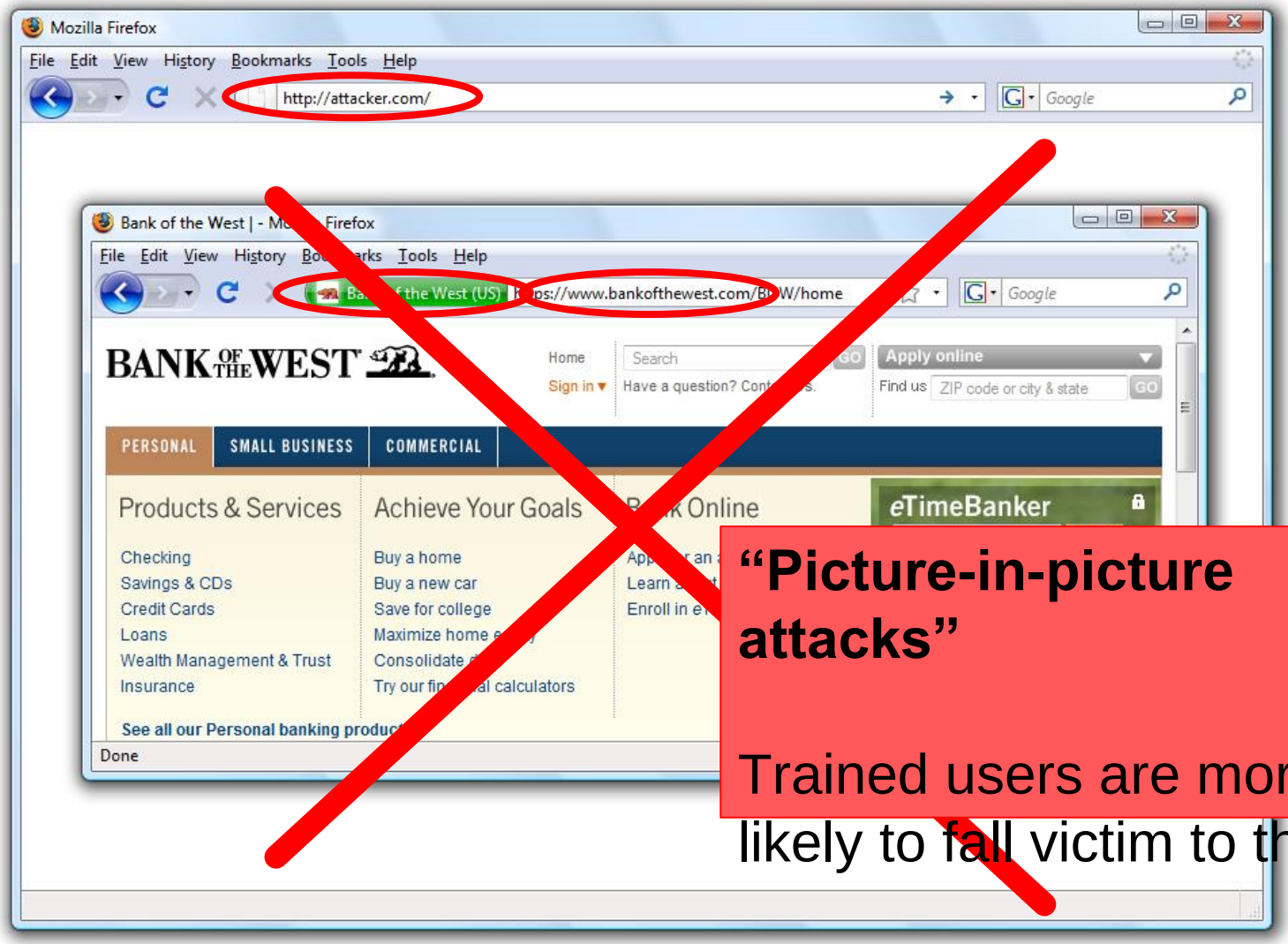


Safe to Type Your Password?



Safe to Type Your Password?

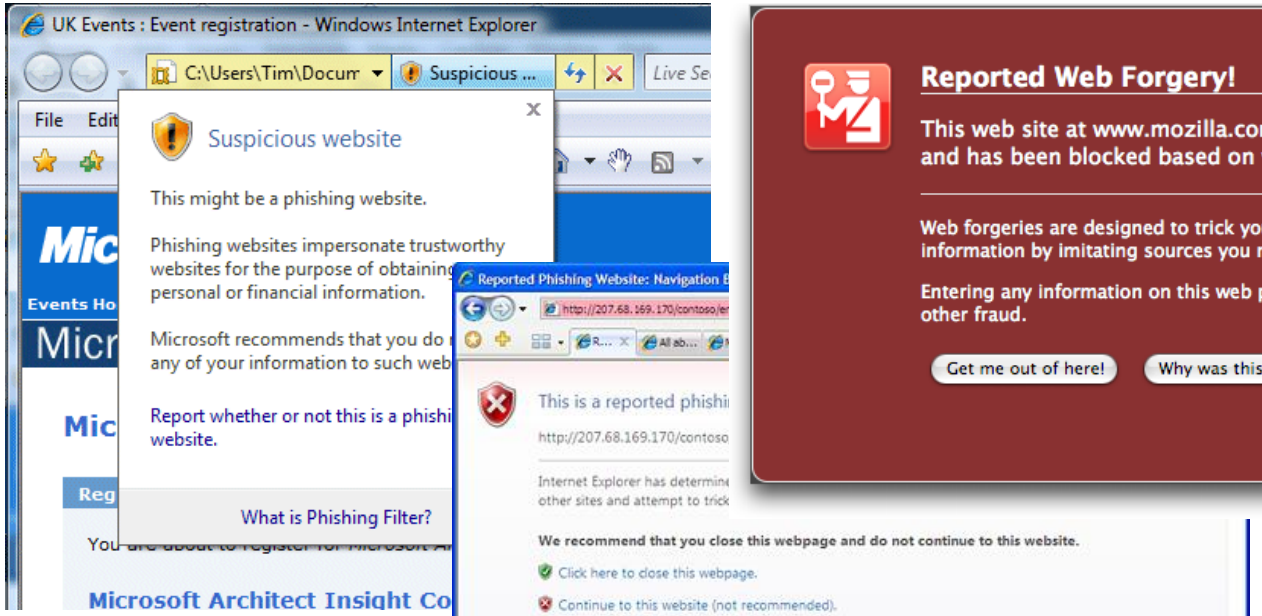
Safe to Type Your Password?



"Picture-in-picture attacks"

Trained users are more likely to fall victim to this!

Phishing Warnings (2008)



Passive (IE)

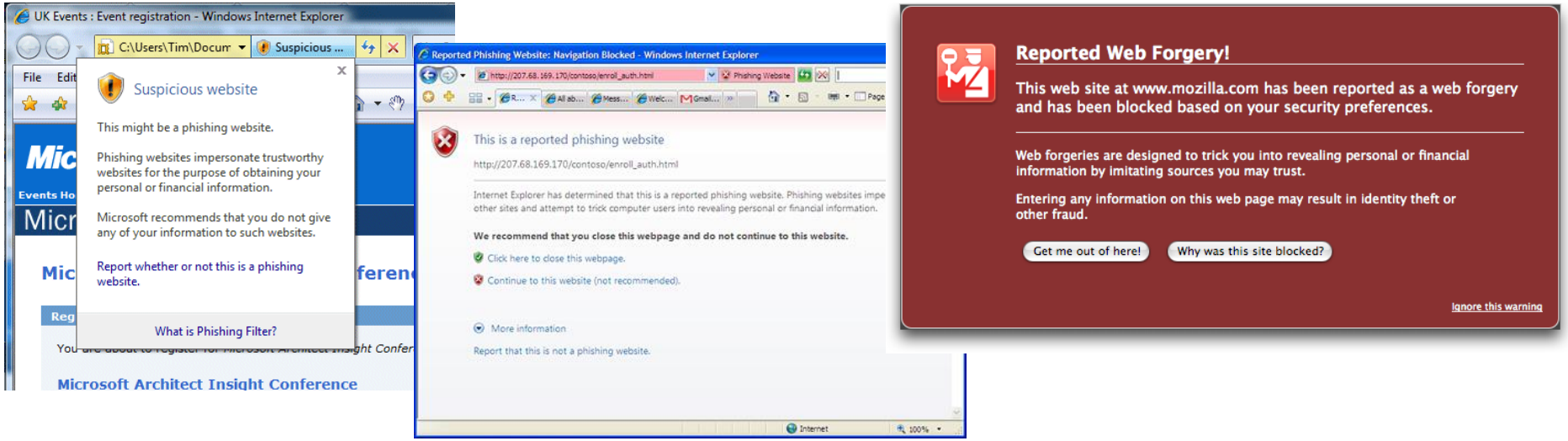
Active (Firefox)

Active (IE)

[Egelman et al.]

Active vs. Passive Warnings

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



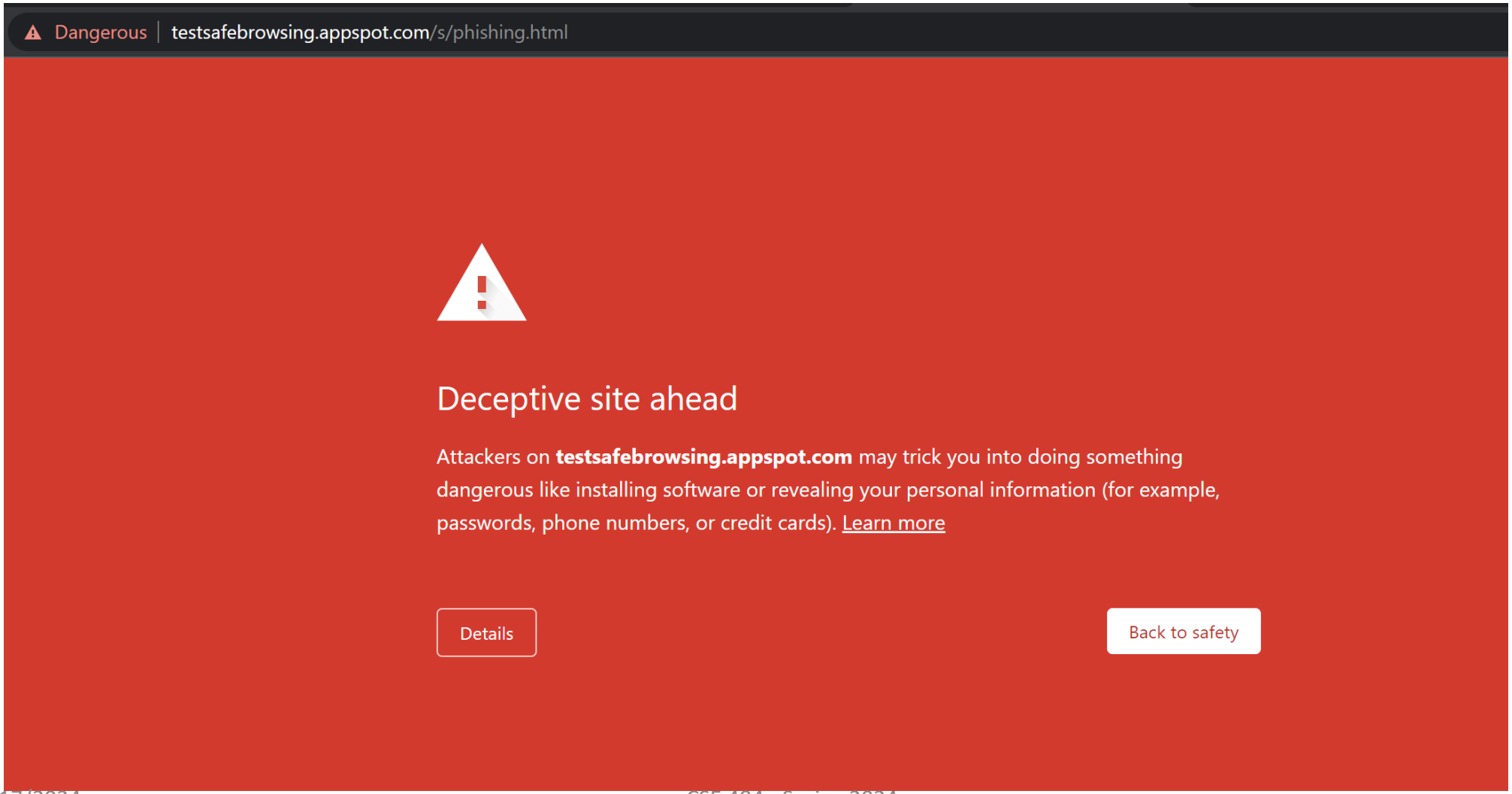
Passive (IE) Active (IE) Active (Firefox)

Modern anti-phishing

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

- (Also Microsoft SafeScreen)

Modern warnings



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.

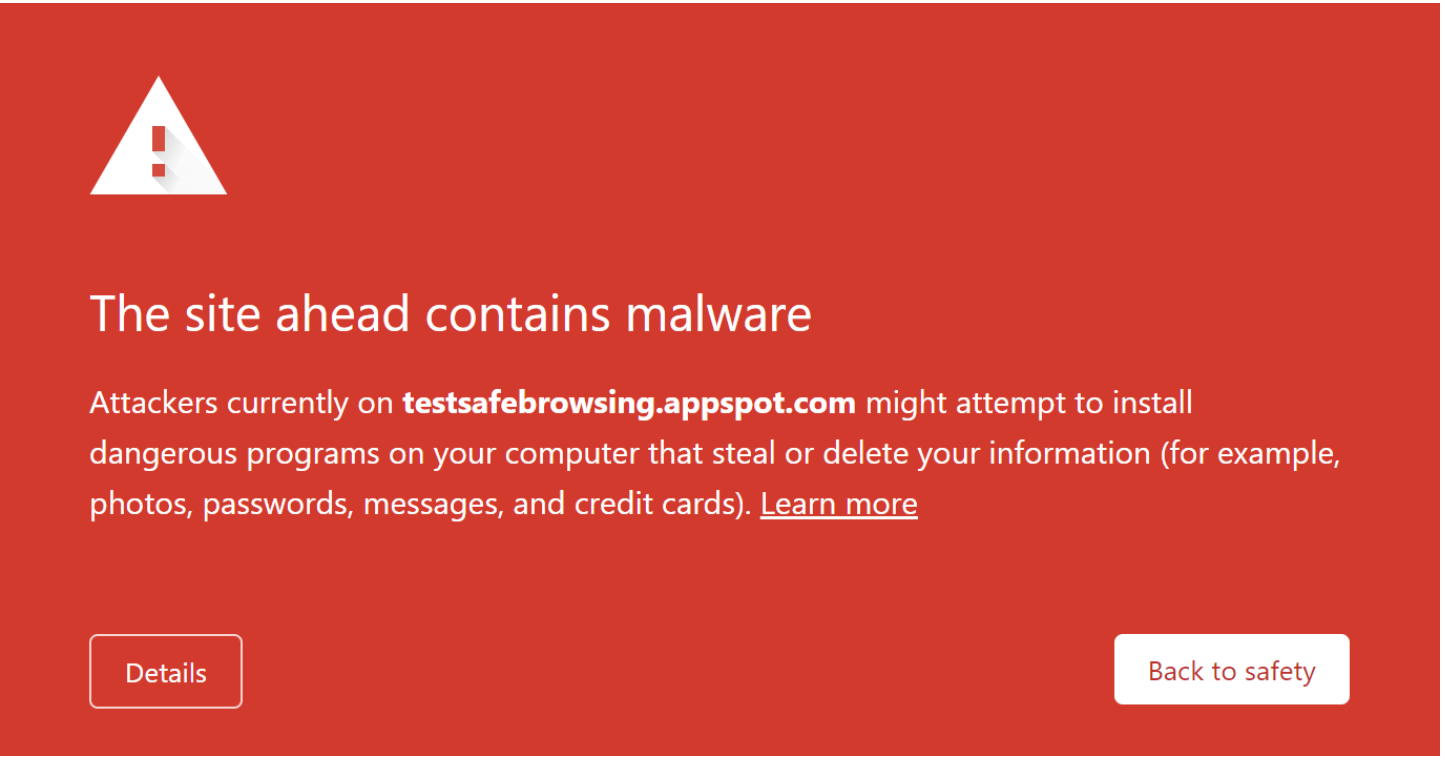
Go back | See details

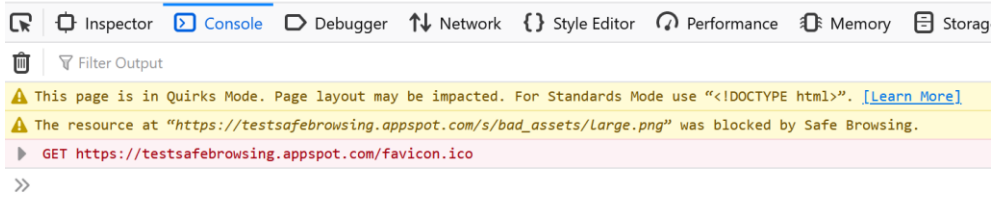
The page ahead may try to charge you money

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

Proceed

Go back


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
Details
Back to safety


Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storag
Filter Output
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?