CSE 484/M584: Computer Security (and Privacy)

Spring 2025

David Kohlbrenner
dkohlbre@cs

UW Instruction Team: David Kohlbrenner, Yoshi Kohno, Franziska Roesner, Nirvan Tyagi. Thanks to Dan Boneh, Dieter Gollmann, Dan Halperin, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials

Admin

- Lab 3 Weblab due today
- HW2 goes out today
  - Some reading and writing
  - Some using security tools (reading documentation)

Authentication

But mostly passwords

“New” (2017) NIST Guidelines ☺

- Remove requirement to periodically change passwords
- Screen for commonly used passwords
- Allow copy-paste into password fields
  - But concern: what apps have access to clipboard?
- Allow but don’t require arbitrary special characters
- Etc.

https://pages.nist.gov/800-63-3/sp800-63b.html

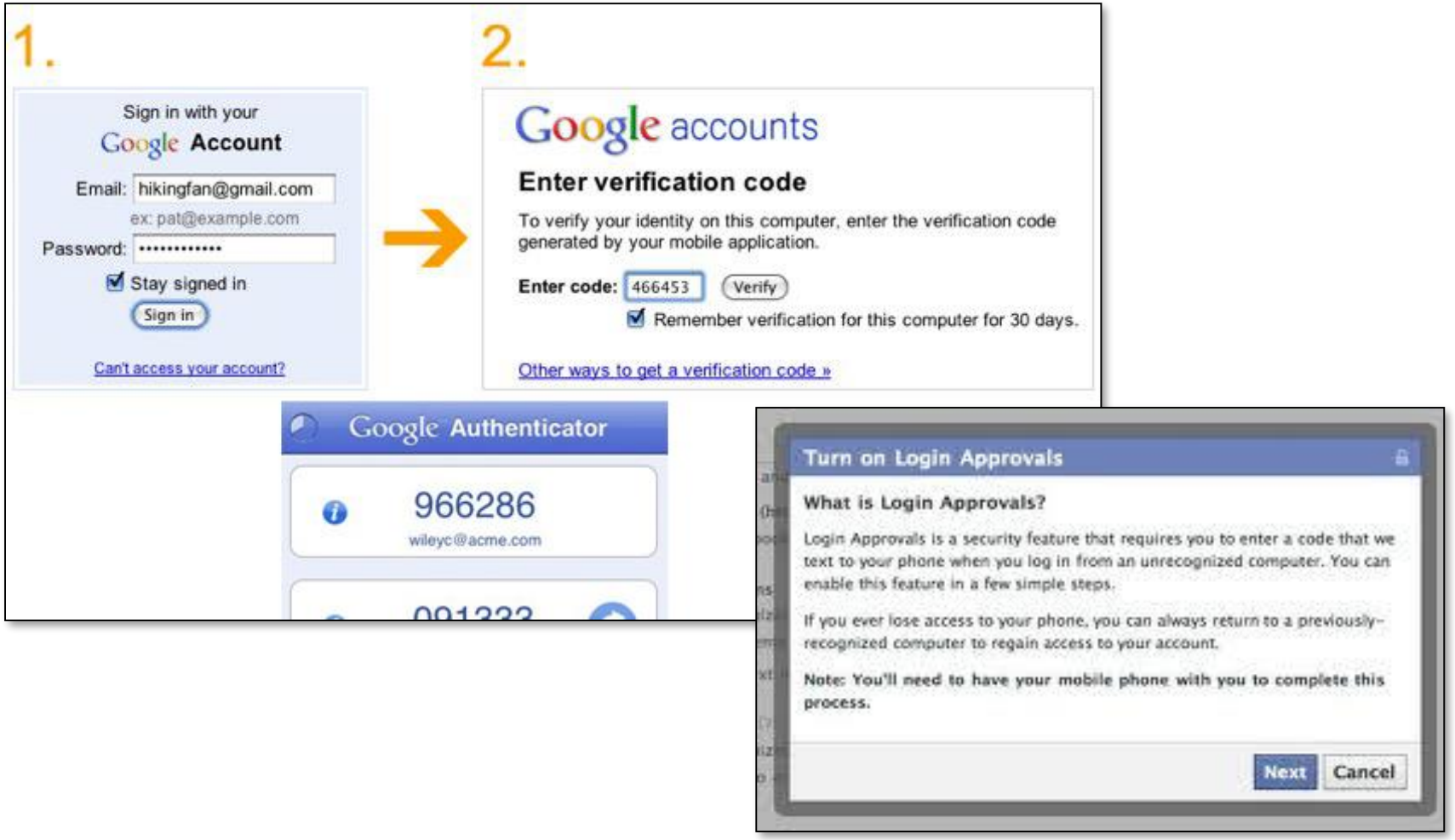
Improving(?) Passwords

- Add biometrics
  - For example, keystroke dynamics or voiceprint
- Graphical passwords
  - Goal: easier to remember? no need to write down?
- Password managers
  - Examples: LastPass, KeePass, built into browsers
  - Can have security vulnerabilities…
- Two-factor authentication
  - Leverage phone (or other device) for authentication

Password managers

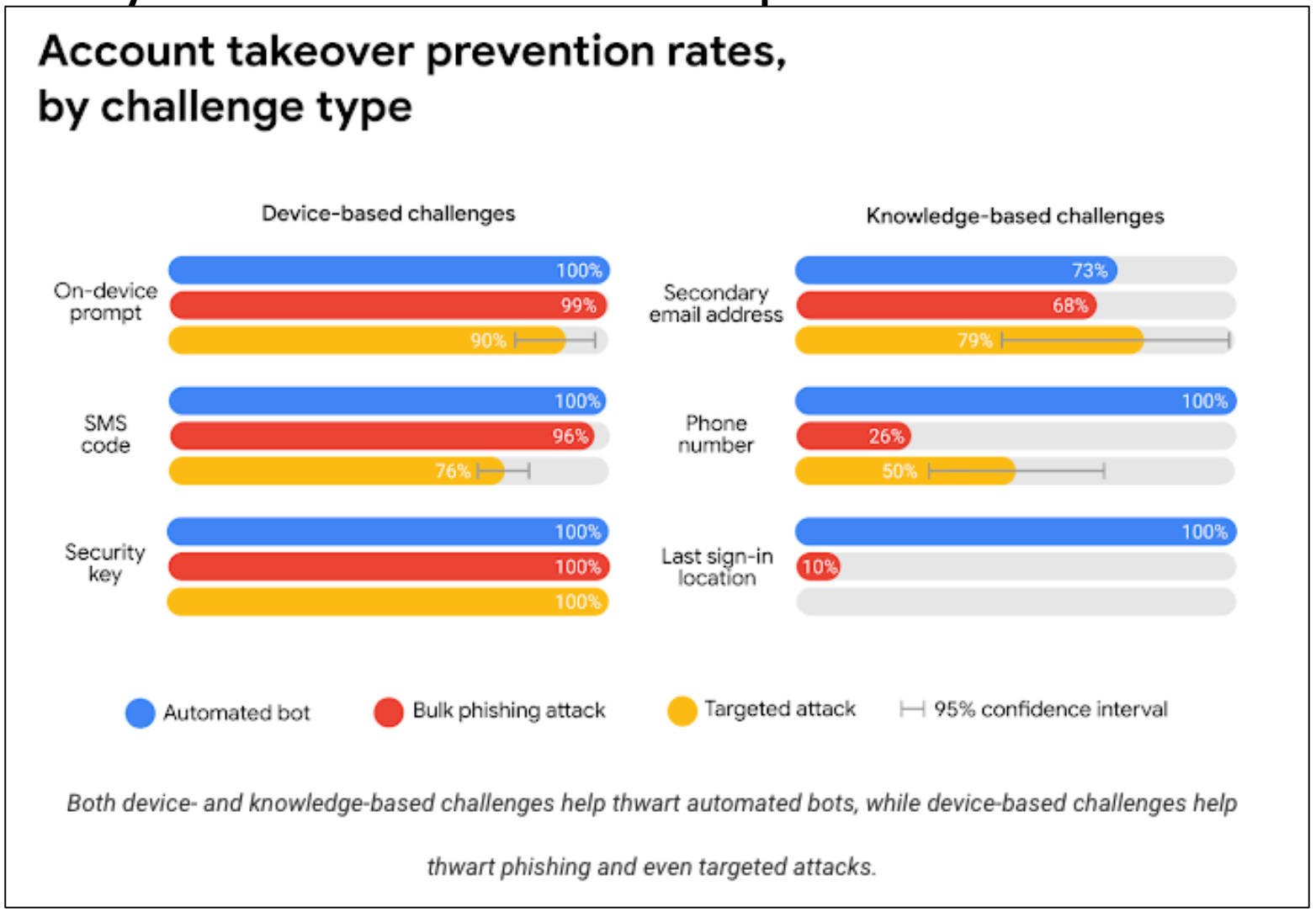
- Generation
  - Secure generation of random passwords
- Management
  - Allows for password-per-account
- Safety?
  - Single point of failure
  - Vulnerability?
  - Phishing?

Multi-Factor Authentication



https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html

Secondary Factors Do Help!



Why does hardware 2FA work?

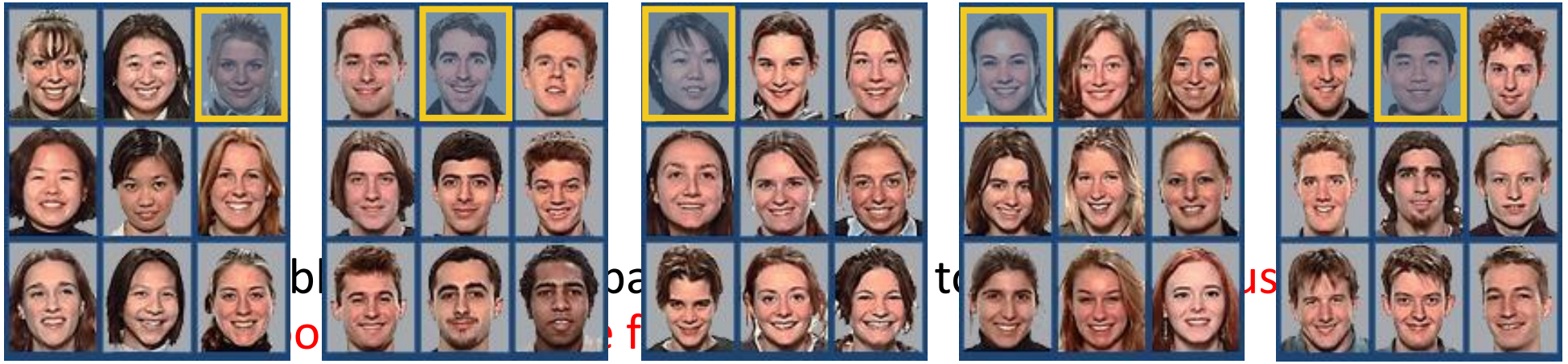
- We need to stop the user *who believe they are logging in* from letting the attacker in.

- Consider:
  - User goes to attacker[.]com/googlelogin.php
  - User *tries to log in*
  - How will SMS codes stop the attacker?
  - How will a token that understands origins stop the attacker?

Hardware 2FA tokens (U2F/FIDO)

Graphical Passwords

- Many variants… one example: Passfaces
  - Assumption: easy to recall faces

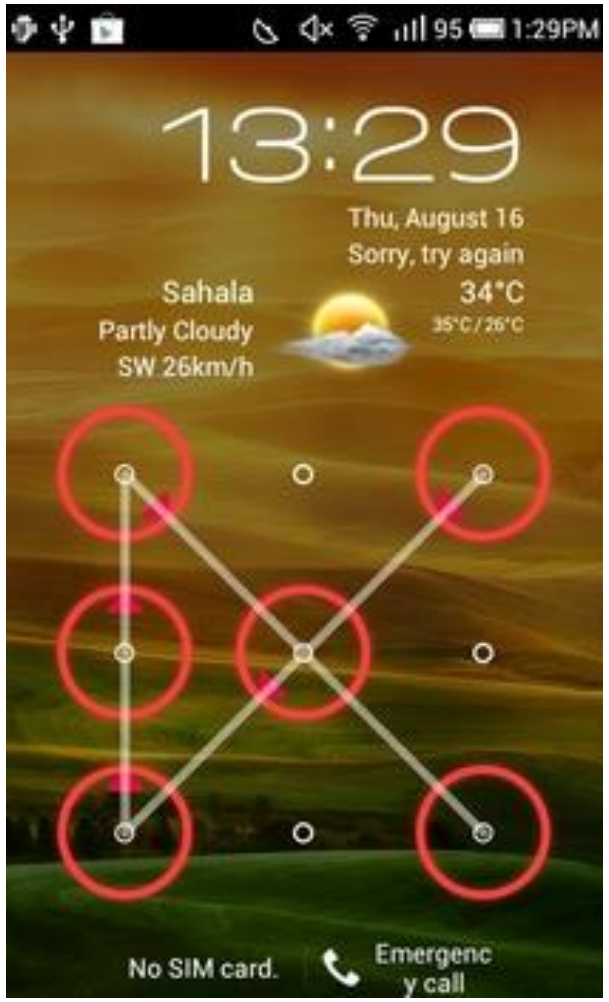


Graphical Passwords

- Another variant: draw on the image (Windows 8)

- Problem: users choose predictable points/lines

Unlock Patterns



- Problems:
  - Predictable patterns (familiar pattern by now)
  - Smear patterns
  - Side channels: apps can use accelerometer and gyroscope to extract pattern!

What About Biometrics?

- Authentication: **What you are**
- Unique identifying characteristics to authenticate user or create credentials
  - Biological and physiological: Fingerprints, iris scan
  - Behaviors characteristics - how perform actions: Handwriting, typing, gait
- Advantages:
  - Nothing to remember
  - Passive
  - Can’t share (generally)
  - With perfect accuracy, could be fairly unique

What are reasons to use/*not* use biometrics?

Issues with Biometrics

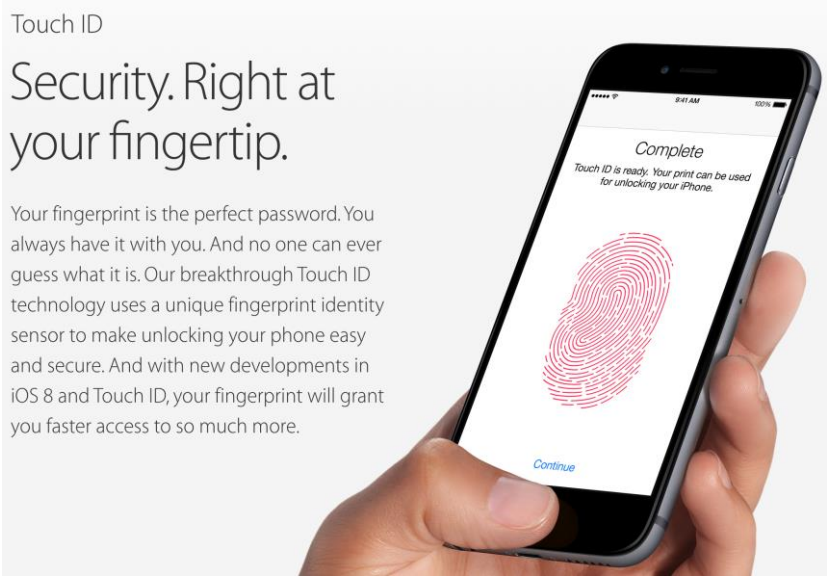
- Private, but not secret
  - Maybe encoded on the back of an ID card?
  - Maybe encoded on your glass, door handle, ...
  - Sharing between multiple systems?
- Revocation is difficult (impossible?)
  - Sorry, your iris has been compromised, please create a new one...
- Physically identifying
  - Soda machine to cross-reference fingerprint with DMV?
- Birthday paradox
  - With false accept rate of 1 in a million, probability of false match is above 50% with only 1609 samples

US Law and Biometrics

- Circuit splits on what 5th amendment covers.
- Broadly: some biometrics (e.g. face unlock) may *not* be protected
  - Some biometrics (e.g. fingerprint) *might* be protected
- Passcodes *are* protected

Attacking Biometrics

- An adversary might try to steal biometric info
  - Malicious fingerprint reader
    - Consider when biometric is used to derive a cryptographic key
  - Residual fingerprint on a glass



Passkeys (2024ish)

- An actual, deployed, genuine *password replacement*
  - *Also a 2fa replacement!*
  - *And a username replacement!*

- Basic goals:
  - Store some sort of key on user end-devices
  - Use that key to login to Stuff
  - Don’t allow losing the key
  - Somehow make the key moving between devices Easy

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

- How often have you been frustrated by a security measure and wanted it to turn off?
  - Or *never turned on*

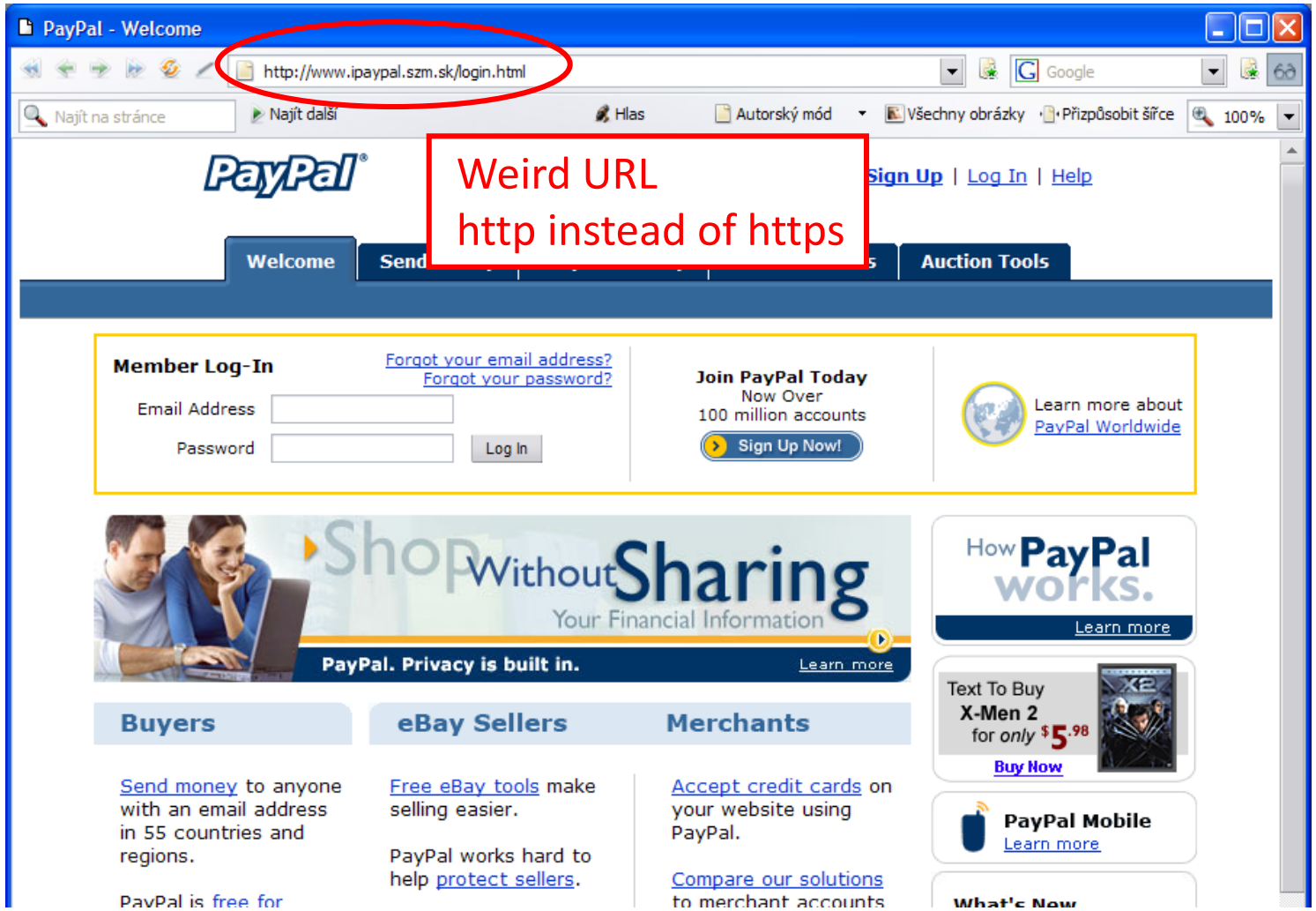
Usable Security Roadmap

- 2 case studies
  - HTTPS indicators + SSL warnings – Done in section, will summarize
  - Phishing/etc

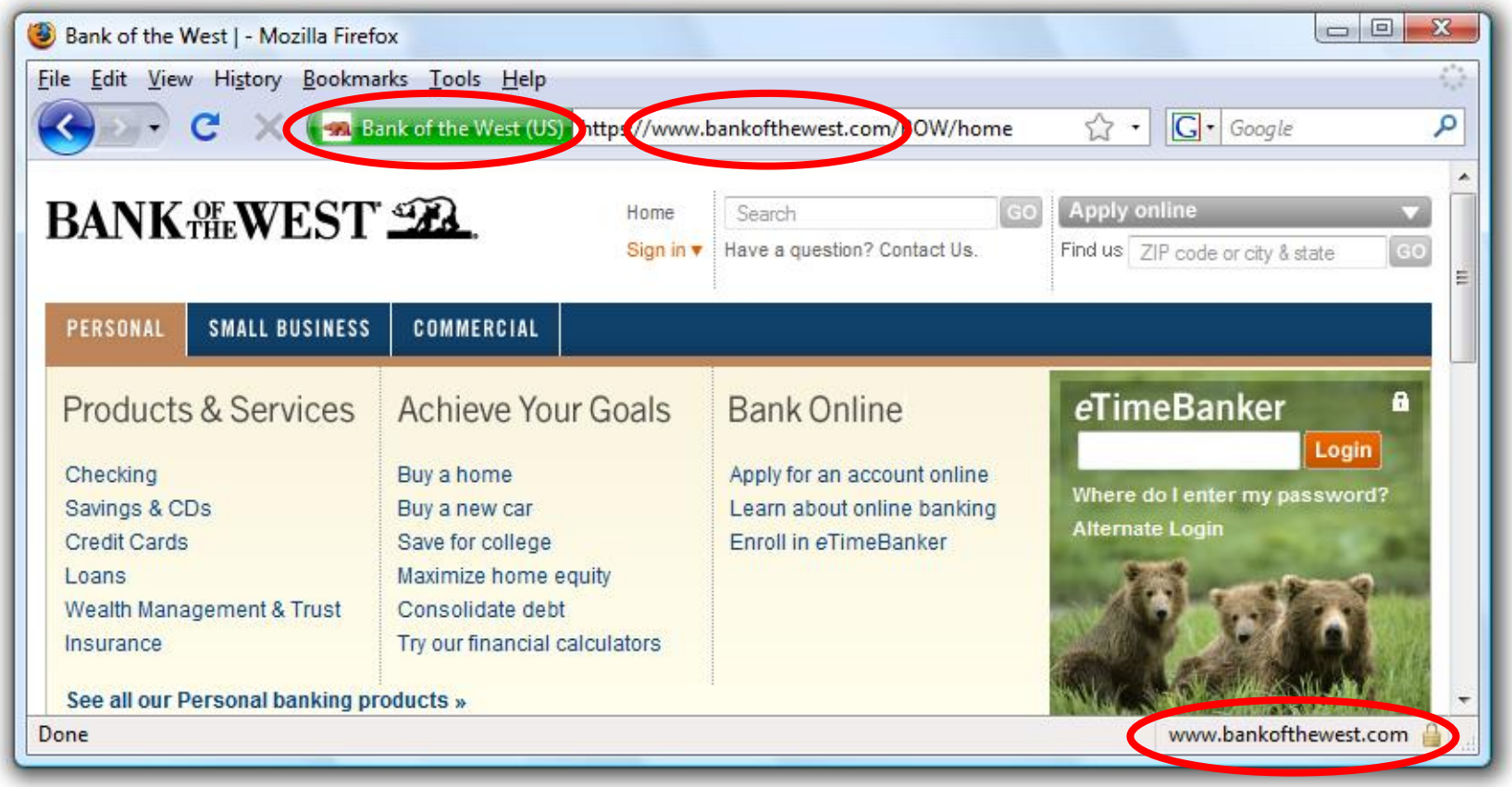
Case Study #1: Phishing

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

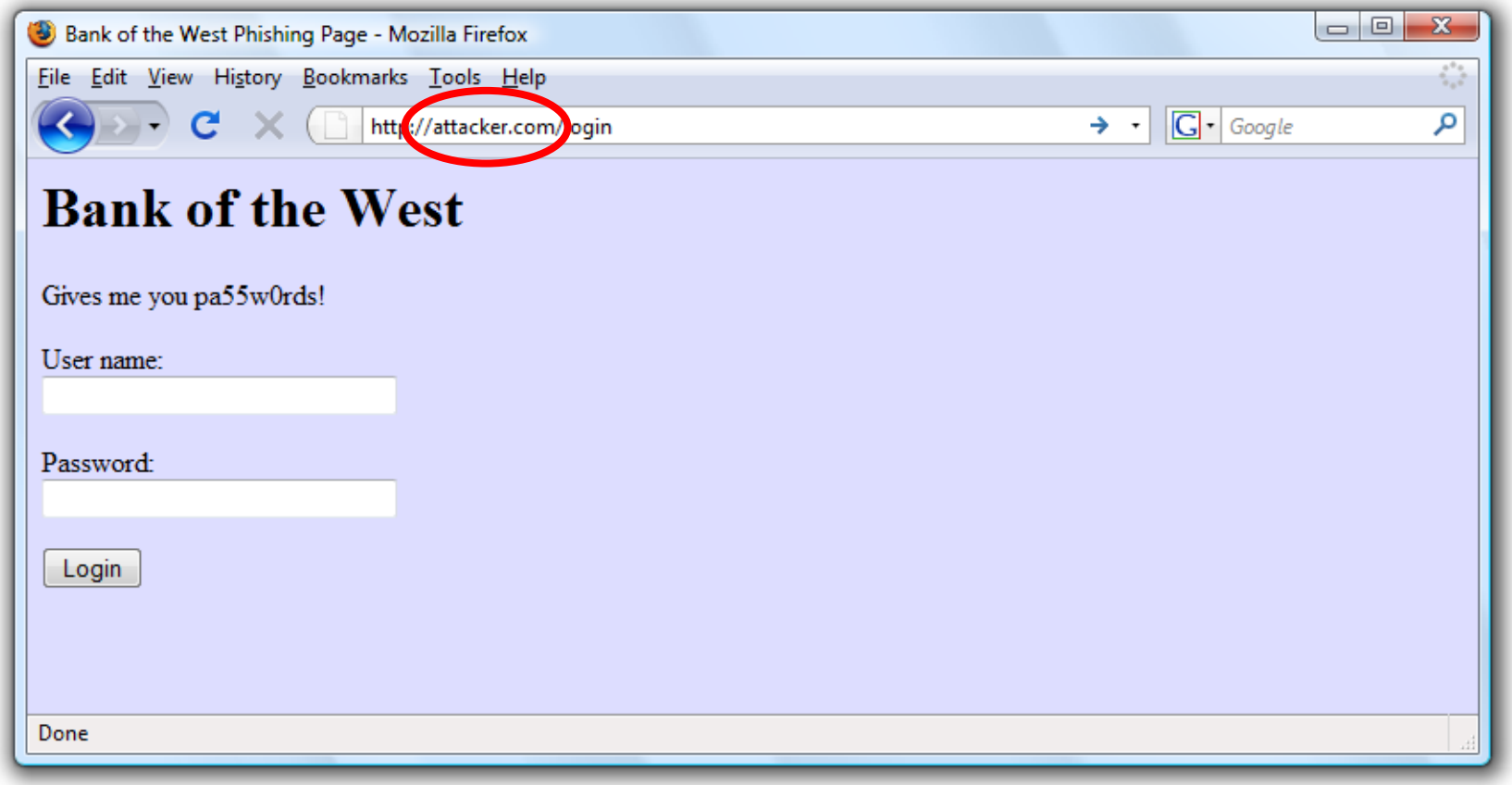
A Typical Phishing Page



Safe to Type Your Password?

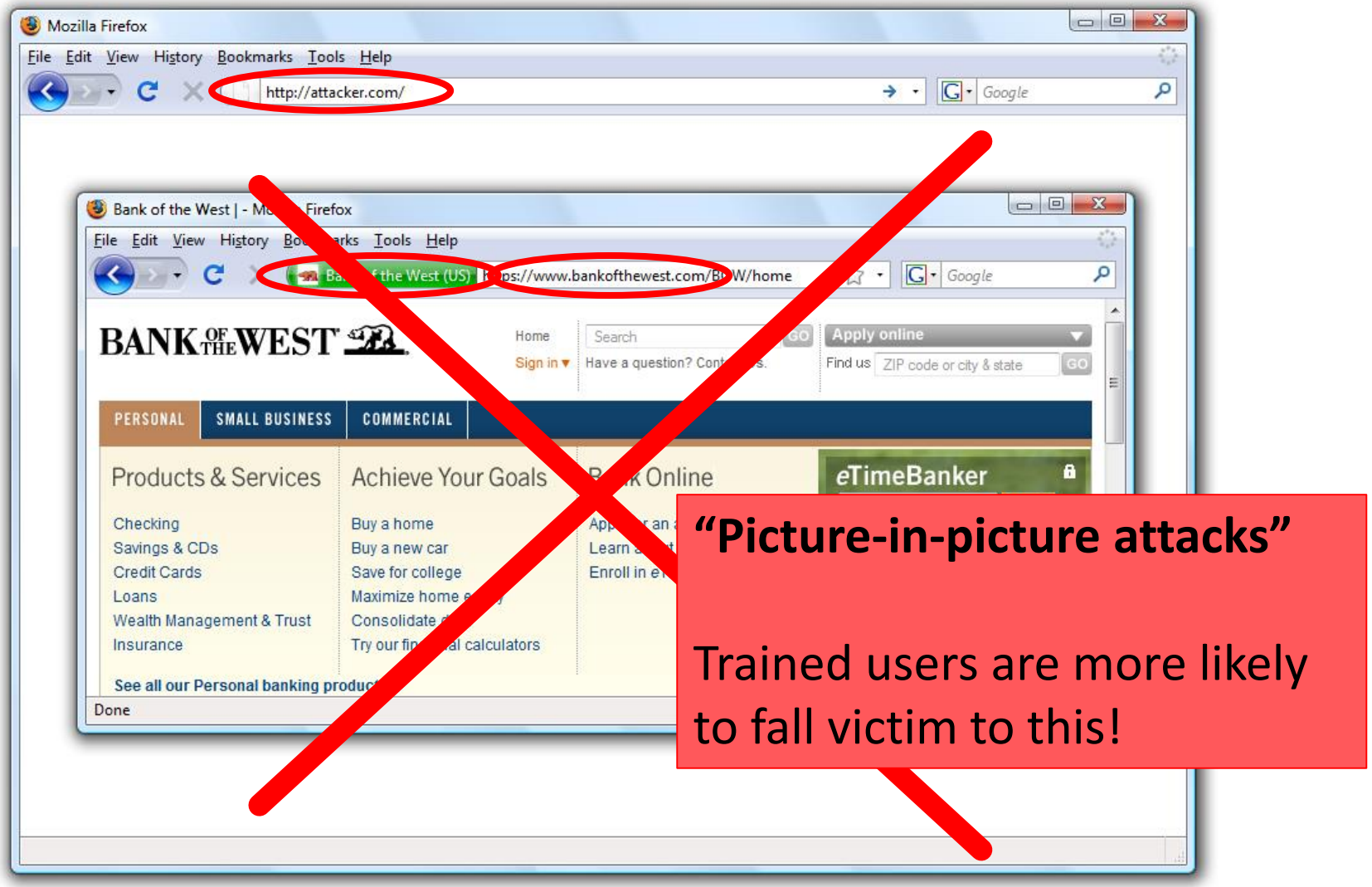


Safe to Type Your Password?



Safe to Type Your Password?

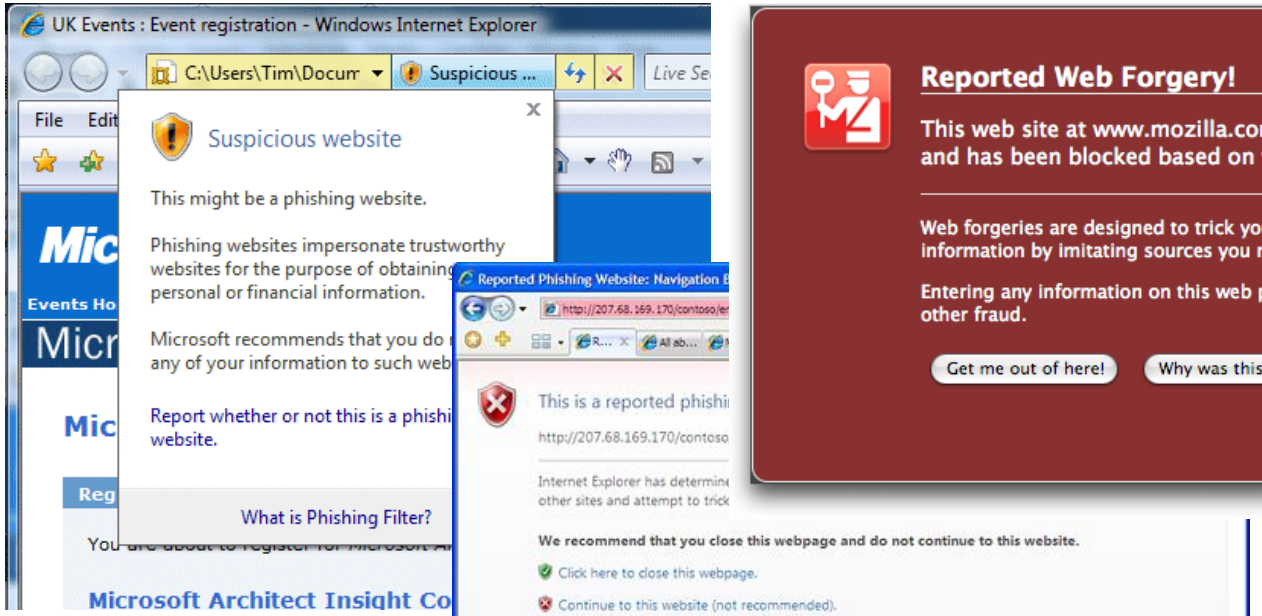
Safe to Type Your Password?



"Picture-in-picture attacks"

Trained users are more likely to fall victim to this!

Phishing Warnings (2008)



Passive (IE)

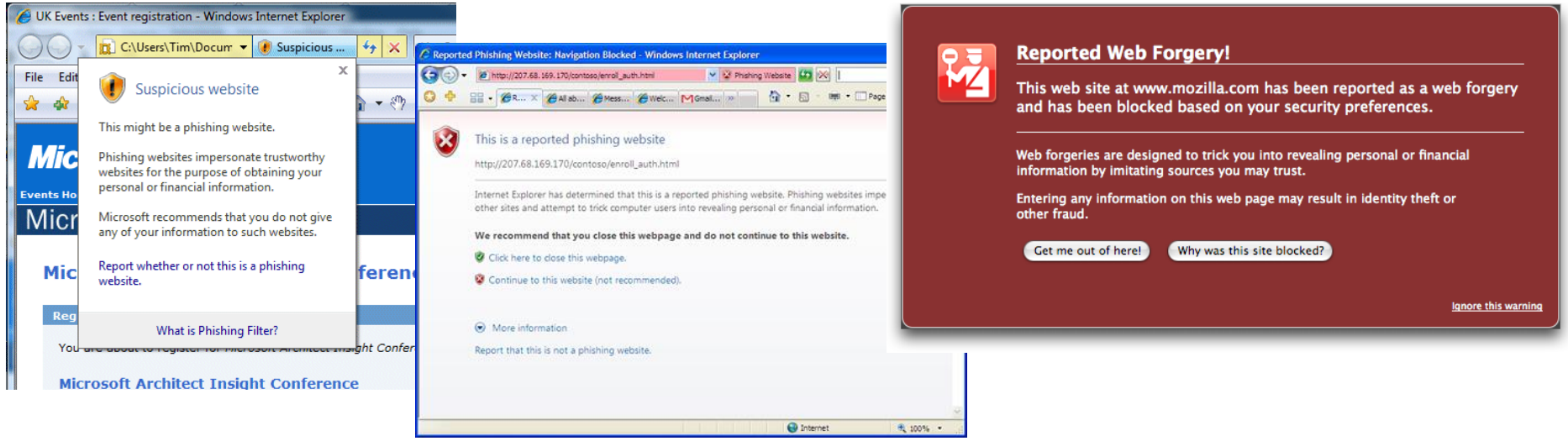
Active (Firefox)

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

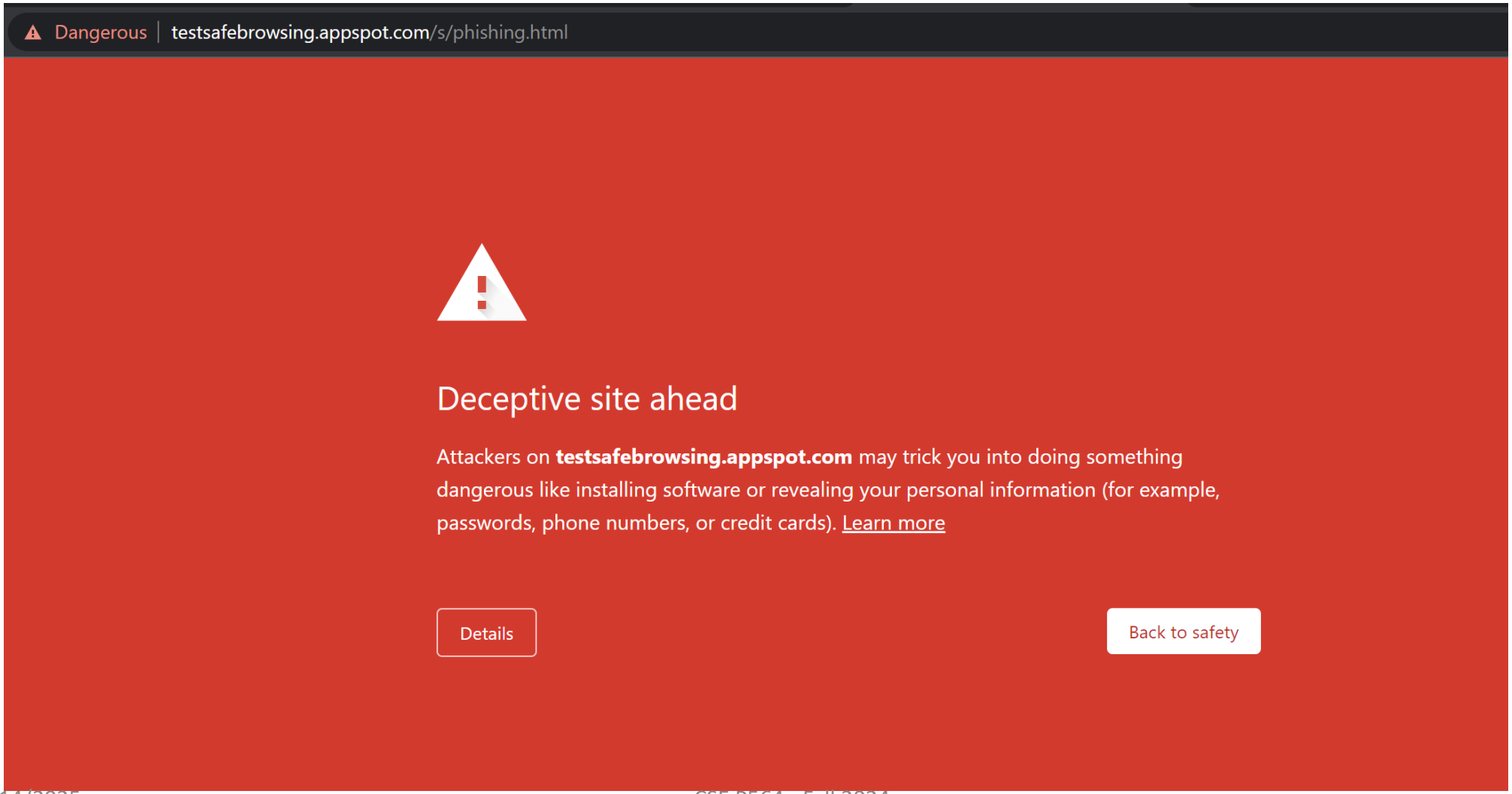


Passive (IE) Active (IE) Active (Firefox)

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
  - E.g. for Edge

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.

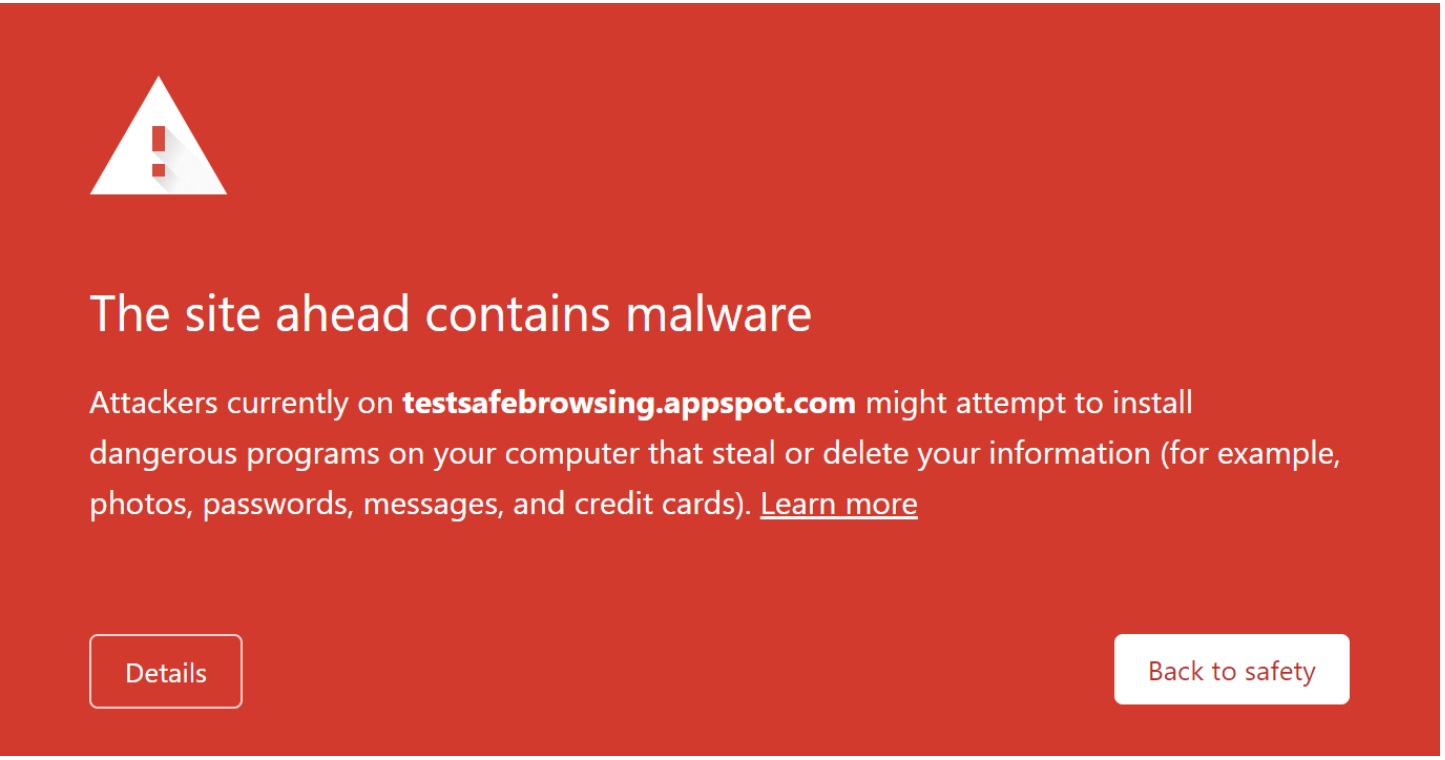
Go back | See details

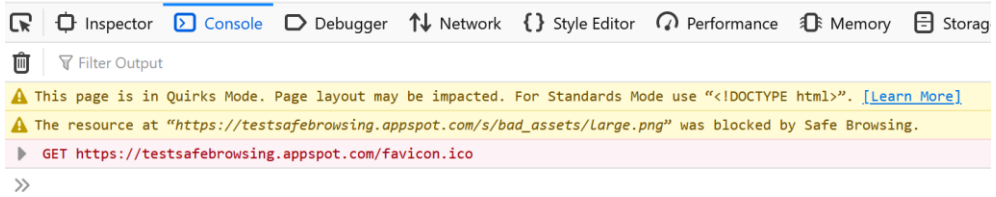
The page ahead may try to charge you money

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

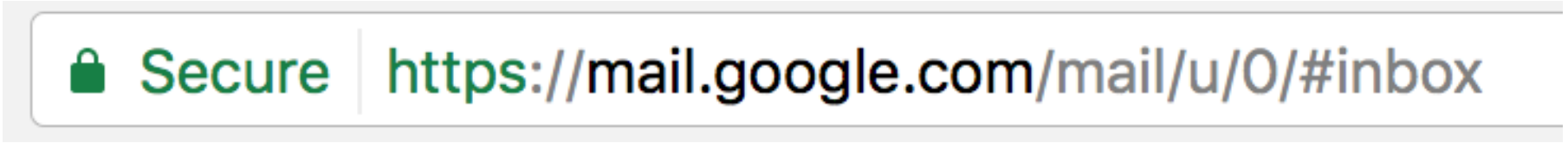

Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storag
Filter Output
This page is in Quirks Mode. Page layout may be impacted. For Standards Mode use "<!DOCTYPE html>". [Learn More]
The resource at "https://testsafebrowsing.appspot.com/s/bad_assets/Large.png" was blocked by Safe Browsing.
GET https://testsafebrowsing.appspot.com/favicon.ico

Does anything stand out?

- Gradescope:
- Why would Firefox, Edge, and Chrome choose different warning designs?

What makes security features usable?

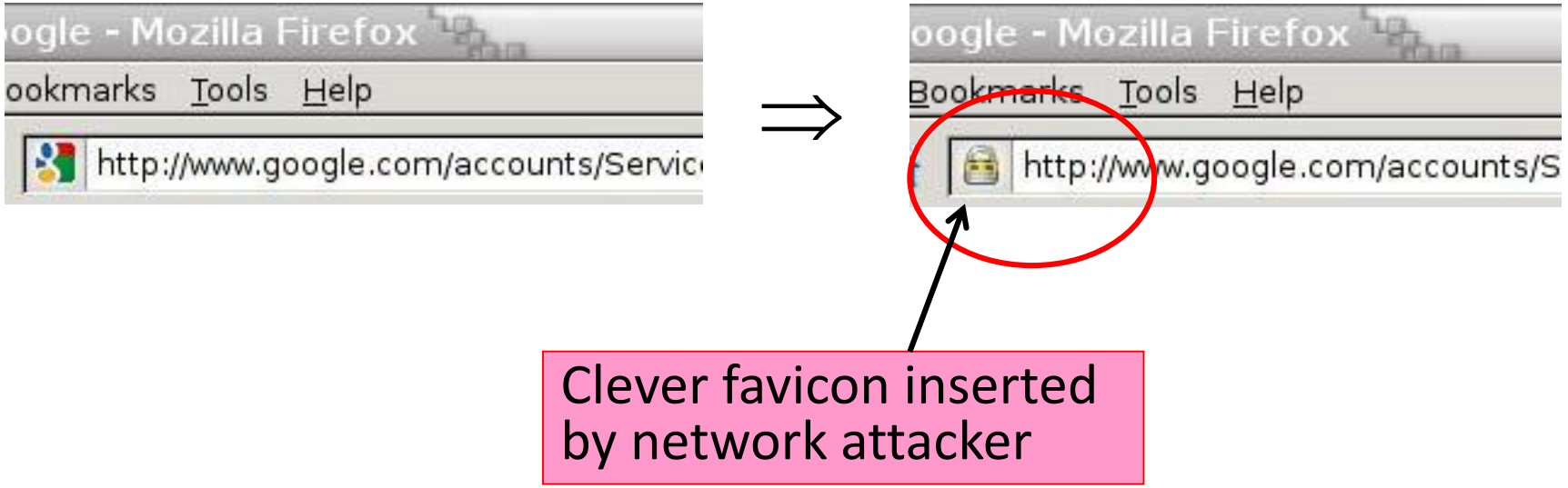
Case Study #2: The Lock Icon



- 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

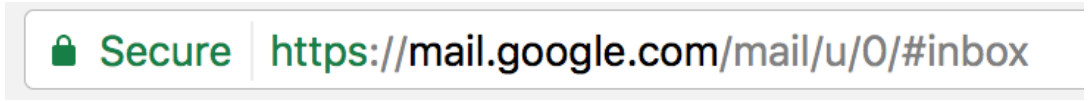
[Moxie Marlinspike]

Will You Notice?

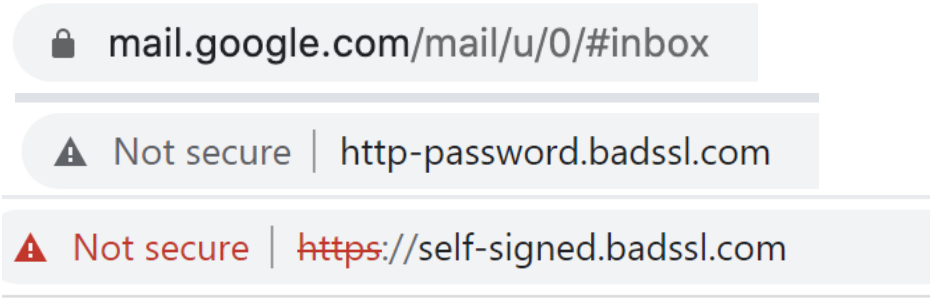


Newer Versions of Chrome

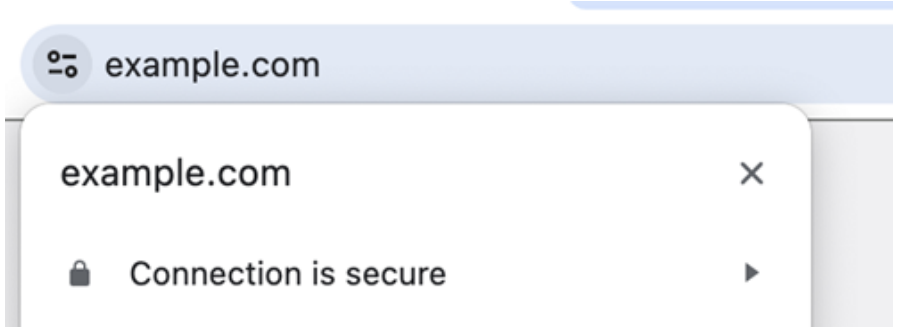
c. 2017



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...