CSE P564: Computer Security and Privacy

Usability, Physical Security, Exceptional Access

Autumn 2024

David Kohlbrenner
dkohlbre@cs

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

Final Project reminders

- Please submit as a group 1x if you are working as a pair

- Much of this lab is about identifying the root cause of a problem, not all potential problems.
  - Because of this, we tend to answer questions less directly.
  - You should always ask: How does the vulnerability relate to XYZ if I’m thinking about changing XYZ.

- There is no length limit to patches. 20-30ish lines changed is a useful estimate for a small-but-effective patch size.
  - If you want to write a 50 line change and refactor 5 functions, that may be changing more than is related to the vulnerability.

Final Project guidance

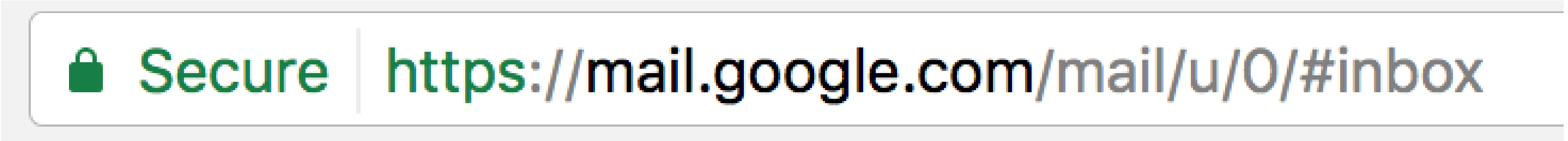
- Always ask:
  - Does the component/feature/etc I'm consider changing relate to the vulnerability in question? Is it part of either the exploit, or a similar exploit?
    - Similar being pretty close in behavior here, needs to abuse the same problem.
  - If I change this thing, does that affect the exploit?
    - If no, then it is likely not relevant.

- Minimize changes
  - Your patch is easier to grade
  - You are less likely to *add* any bugs

- CWEs: aim for more generic CWEs, rather than some of the weird niche ones

Finishing up Usability

The Lock Icon

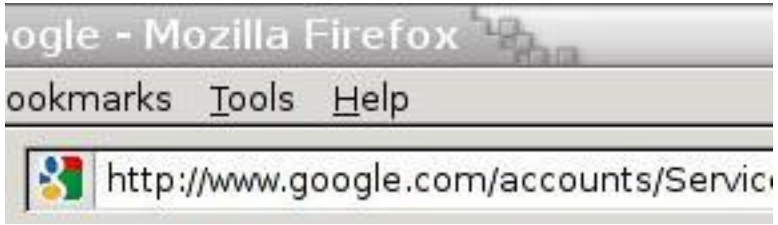


Secure | https://mail.google.com/mail/u/0/#inbox

- 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?

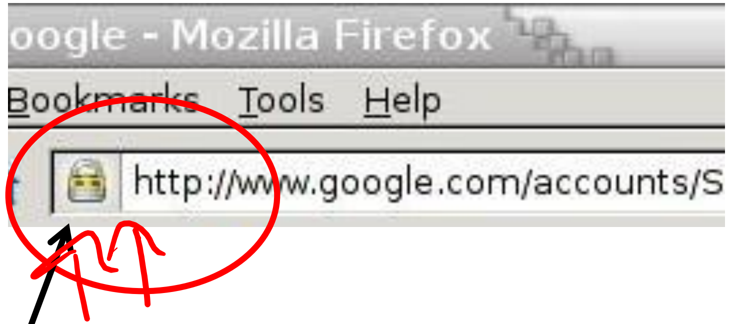


ogle - Mozilla Firefox

ookmarks Tools Help

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

⇒



oogle - Mozilla Firefox

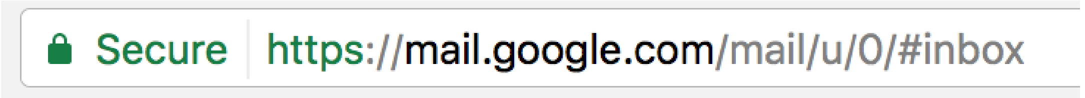
Bookmarks Tools Help

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

Clever favicon inserted by network attacker

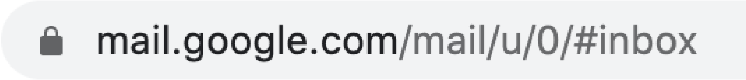
Newer Versions of Chrome

c. 2017

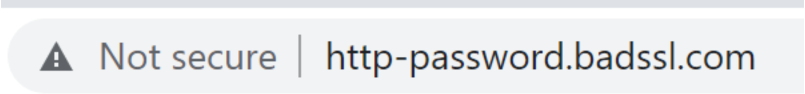


Secure | https://mail.google.com/mail/u/0/#inbox

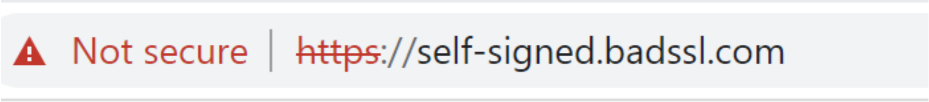
2022



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

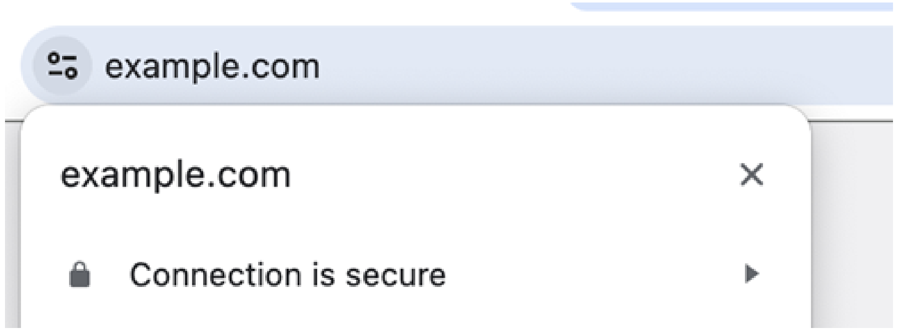


Not secure | http-password.badssl.com



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

2023/2024



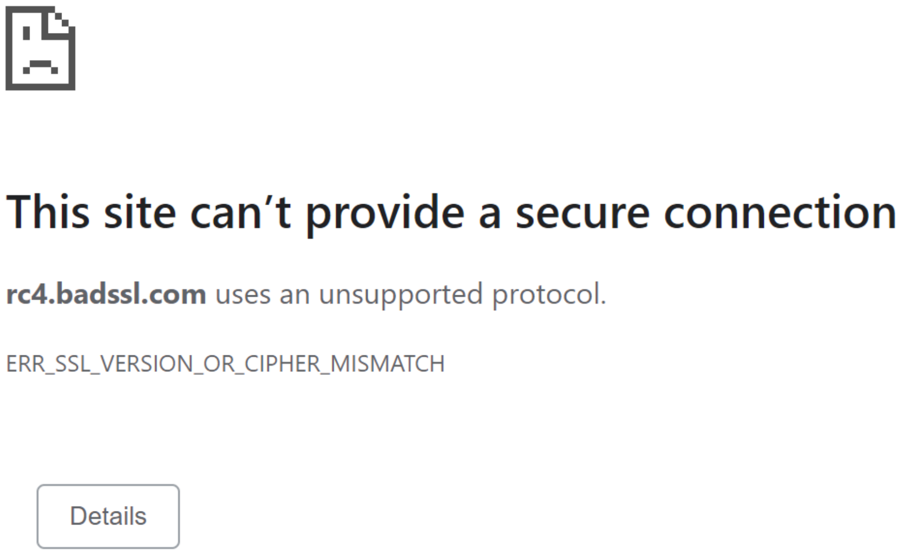
example.com

example.com ✕

Connection is secure ▸

Today’s warnings (2022)

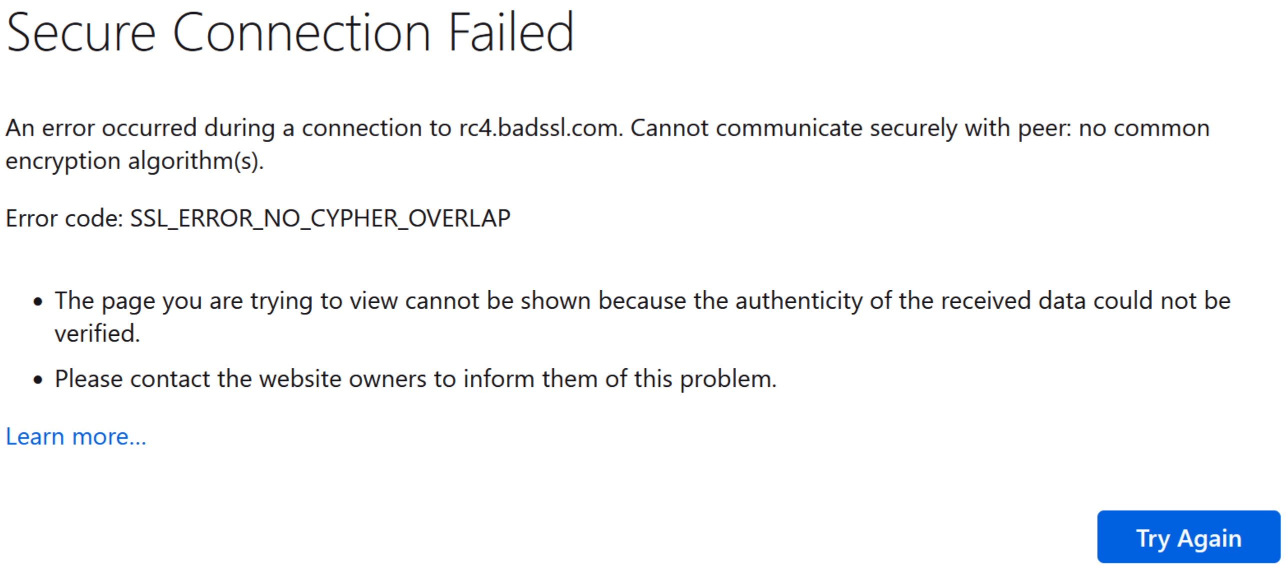
Deprecated encryption schemes



This site can’t provide a secure connection

rc4.badssl.com uses an unsupported protocol.

ERR_SSL_VERSION_OR_CIPHER_MISMATCH



Secure Connection Failed

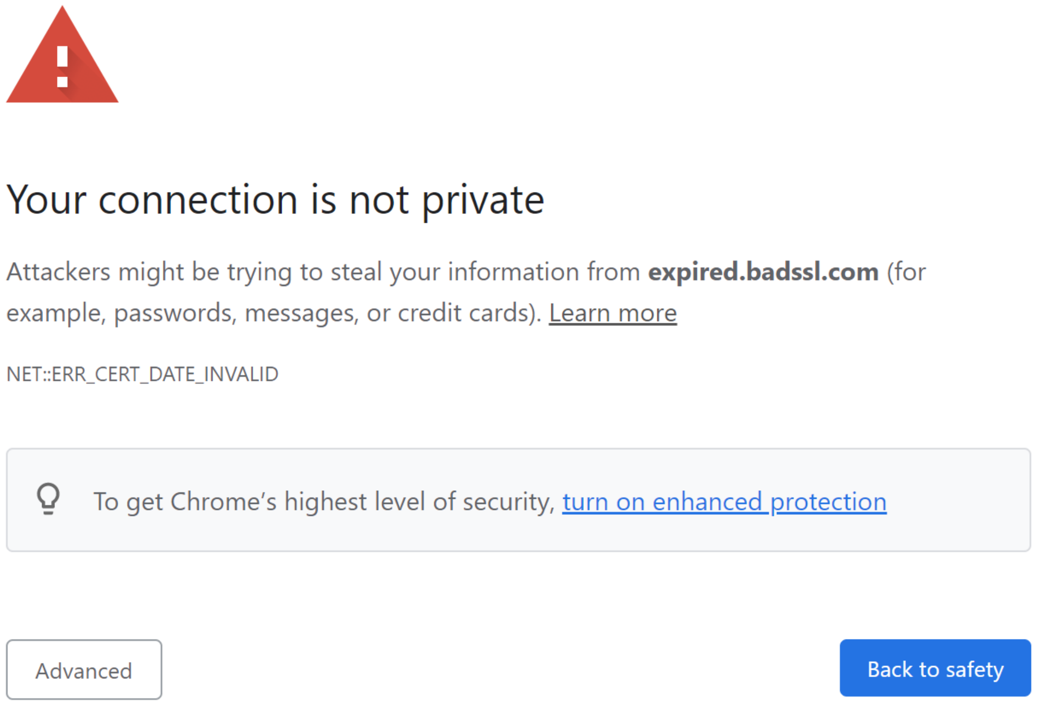
An error occurred during a connection to rc4.badssl.com. Cannot communicate securely with peer: no common encryption algorithm(s).

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

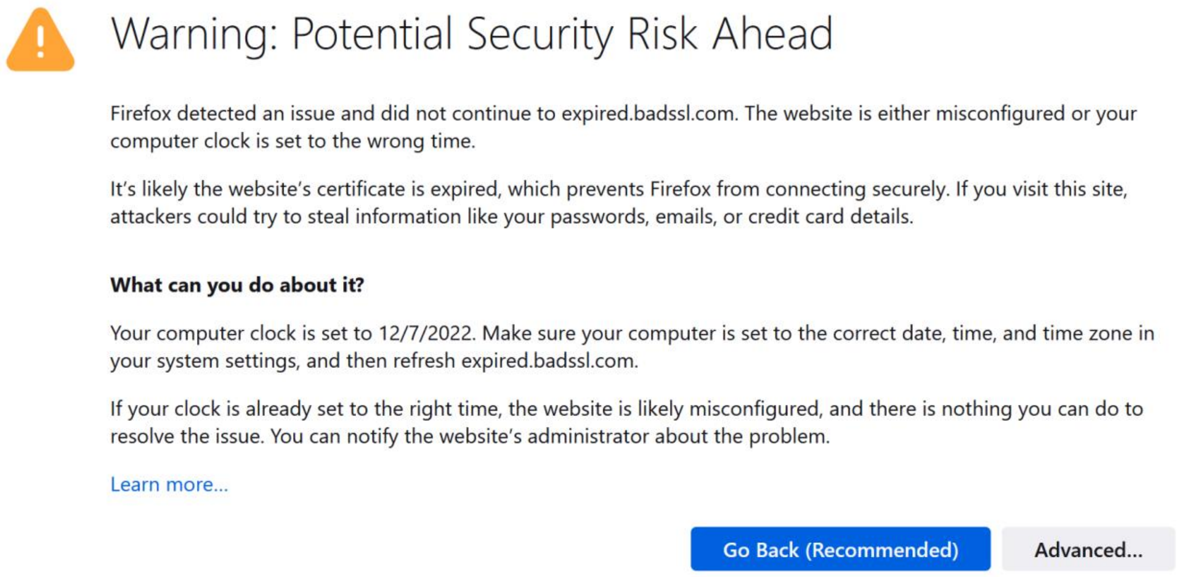


Your connection is not private

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.

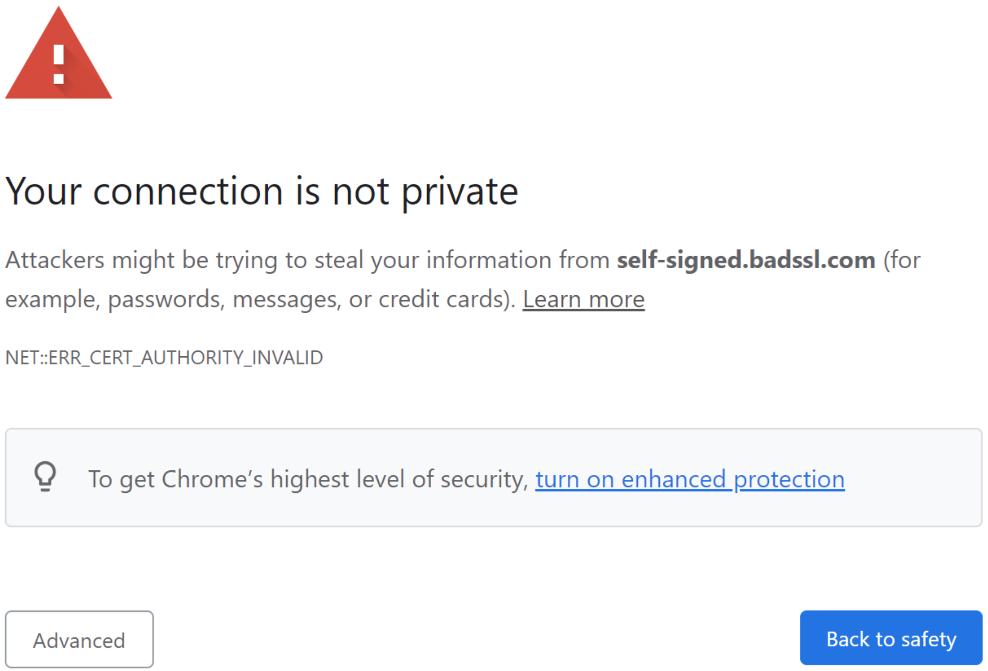
What can you do about it?

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

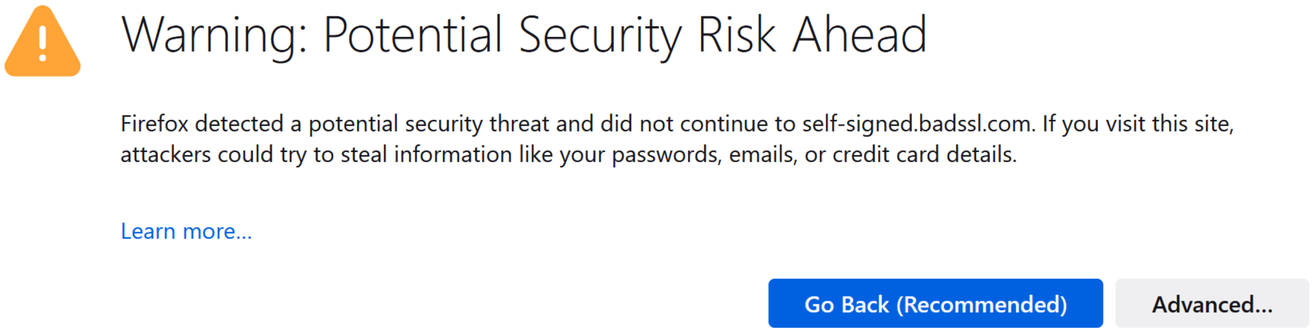


Your connection is not private

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

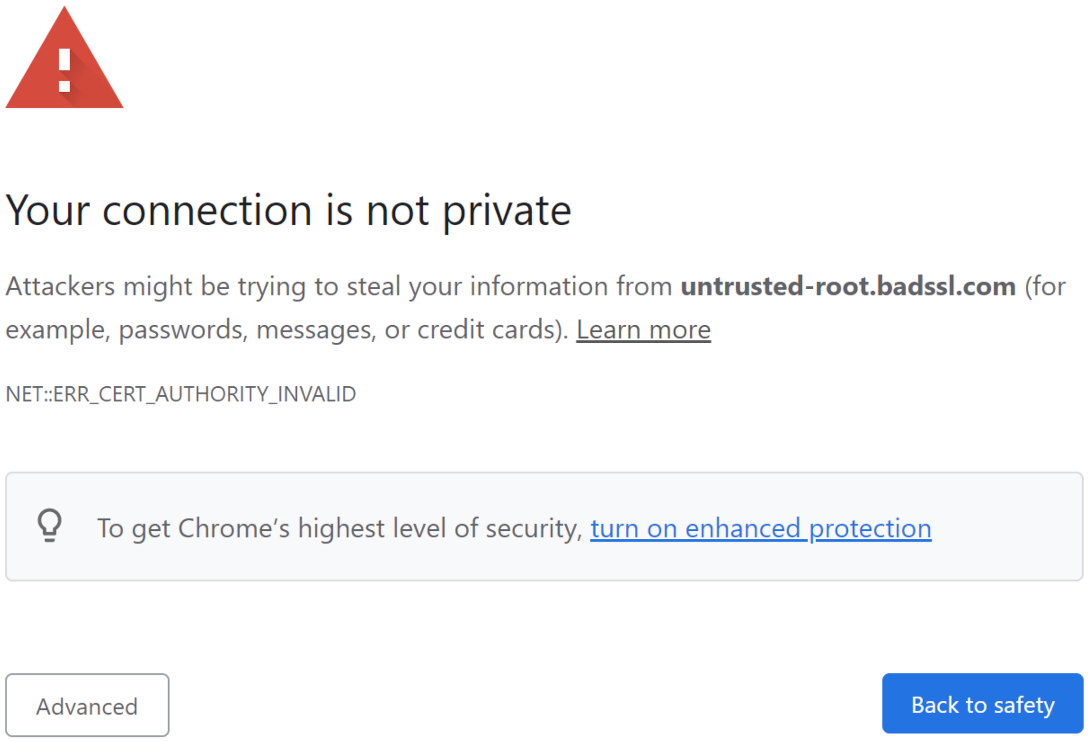


Warning: Potential Security Risk Ahead

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

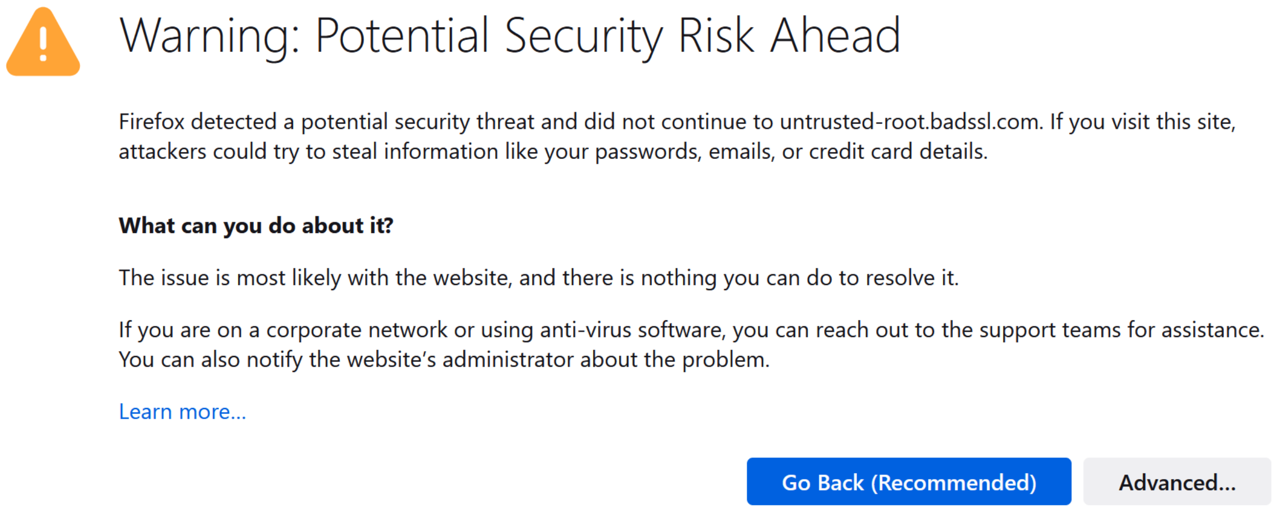


Your connection is not private

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…

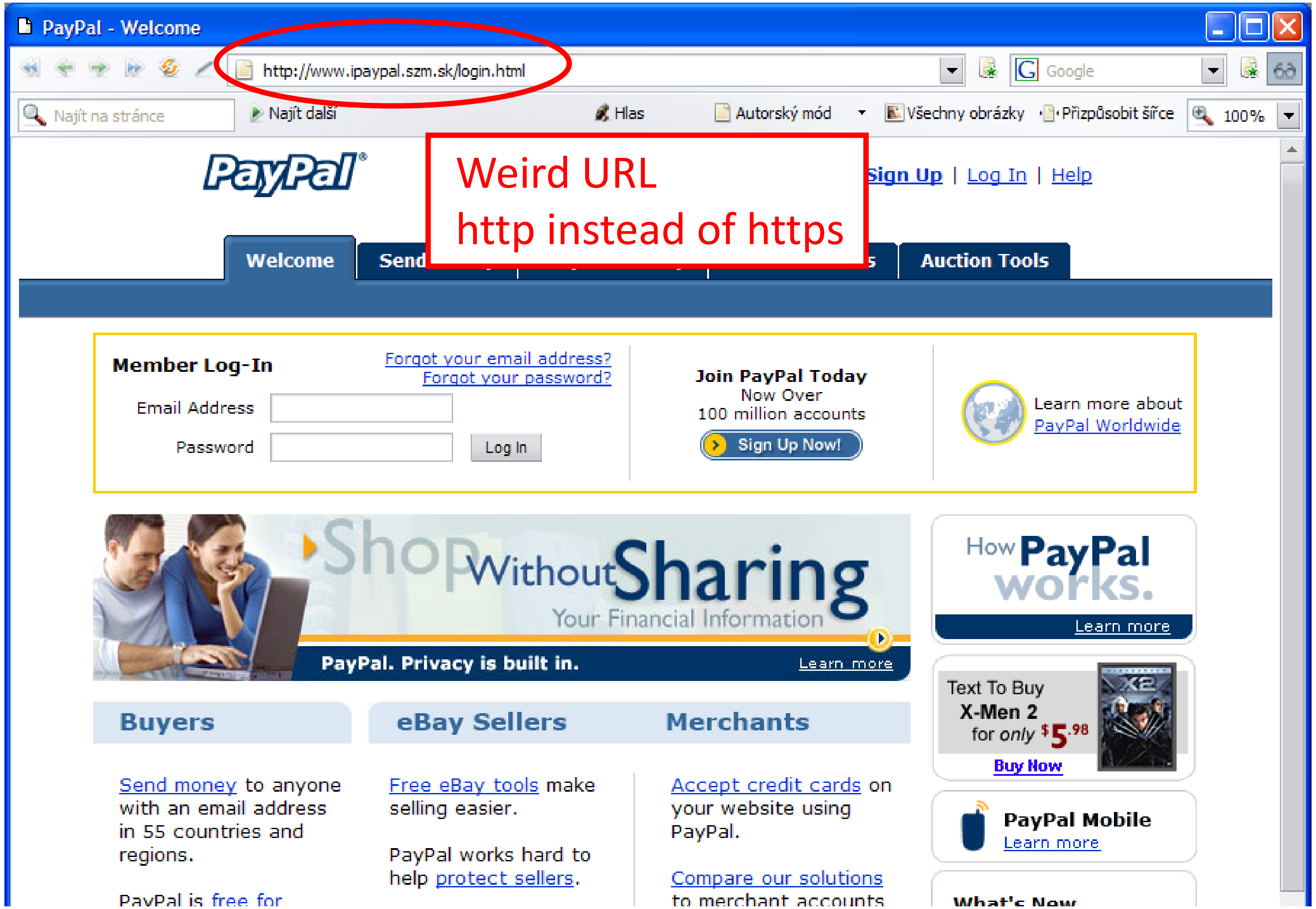
Does anything stand out?

- Gradescope:
- Q1: What are some things that make warnings hard to be effective?
- Q2: Why would Firefox and Chrome choose different warning designs?

Case Study #2: 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

Sign Up | Log In | Help

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

PayPal. Privacy is built in. Learn more

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.

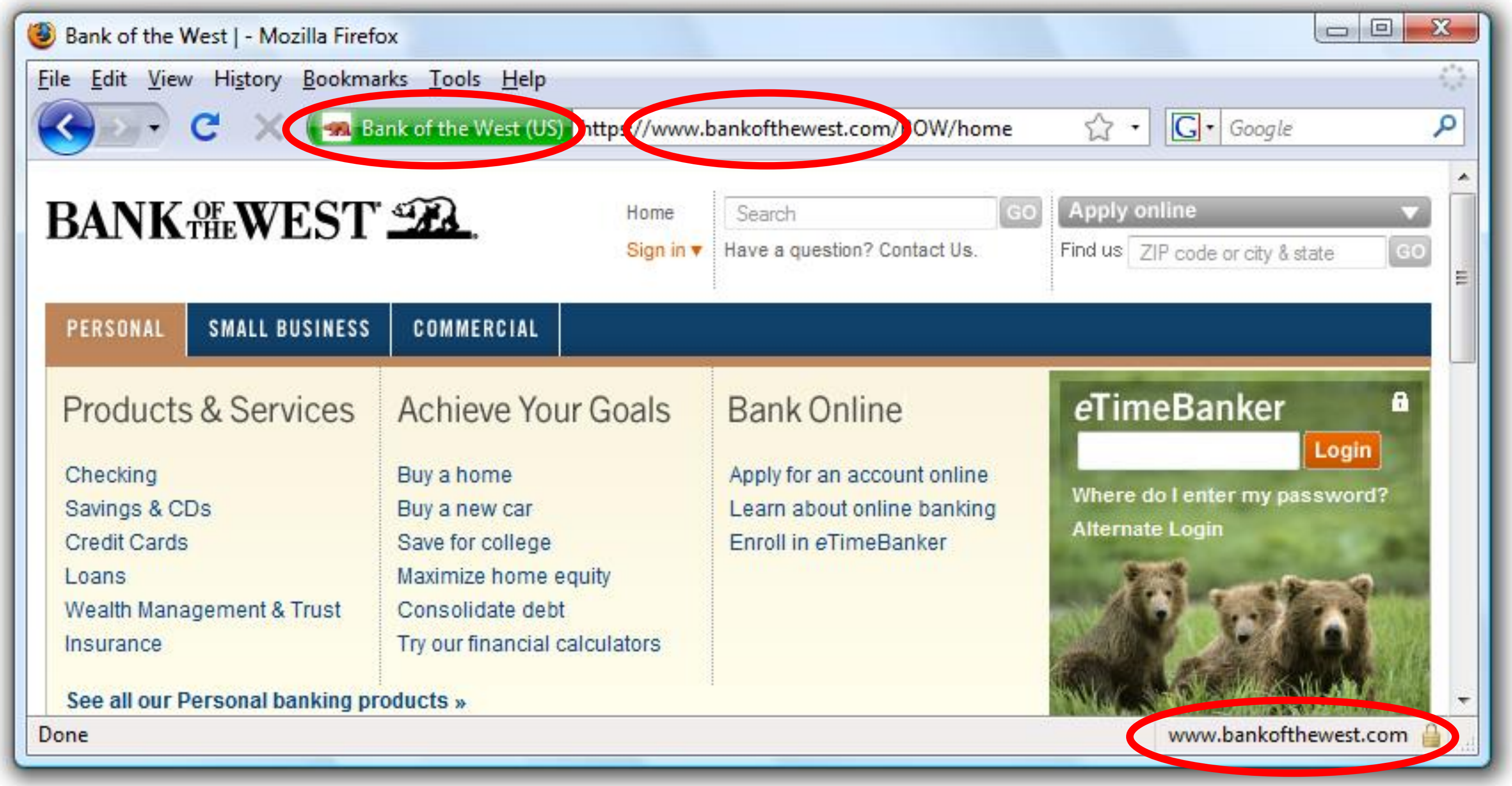
Merchants

Accept credit cards on your website using PayPal.

Compare our solutions to merchant accounts

What's New

Safe to Type Your Password?


Bank of the West | - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Bank of the West (US)
https://www.bankofthewest.com/BOW/home
Google
Done
www.bankofthewest.com

BANK OF THE WEST

Home

Sign in ▾

Search GO

Have a question? Contact Us.

Apply online ▾

Find us ZIP code or city & state GO

PERSONAL | SMALL BUSINESS | COMMERCIAL

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

eTimeBanker

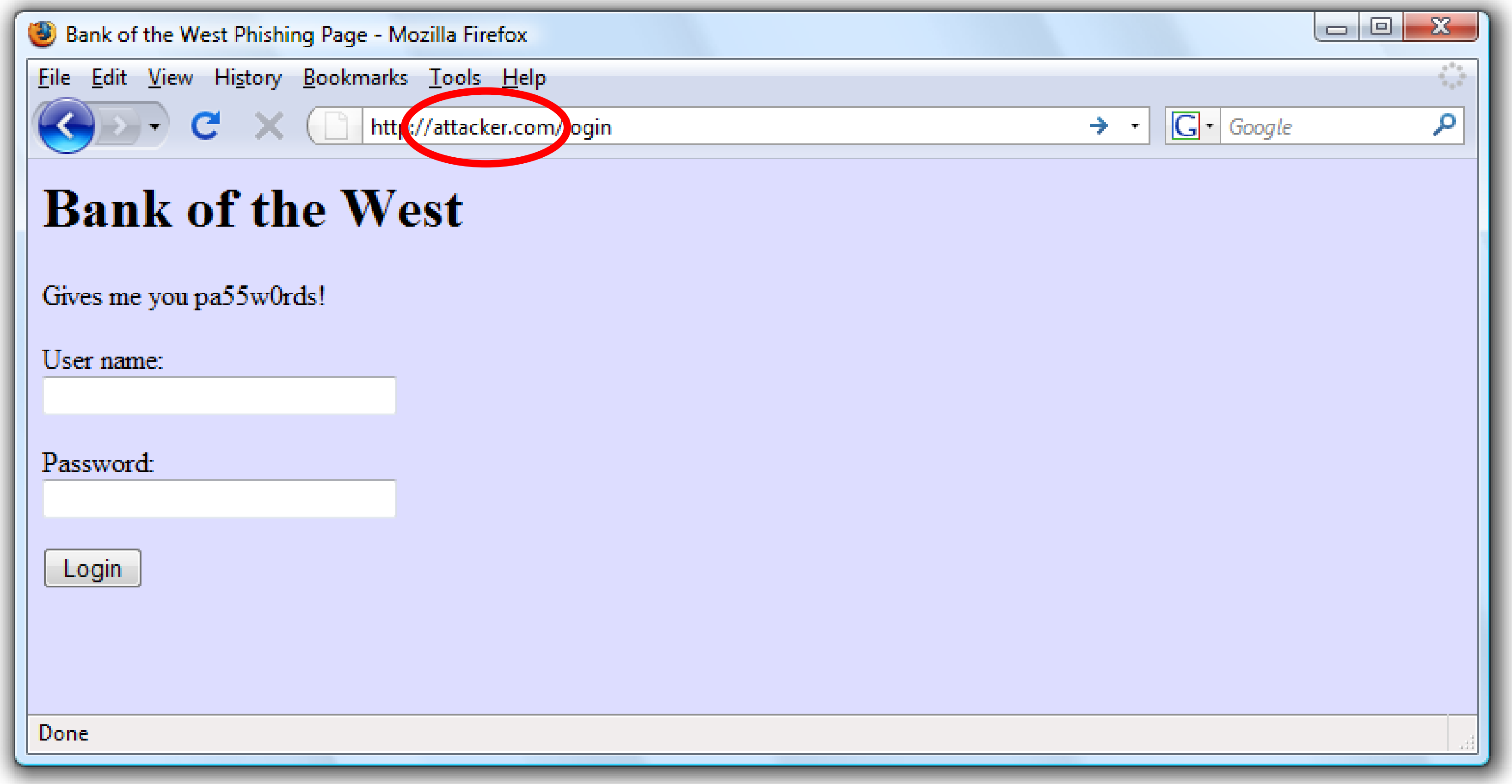
Login

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!

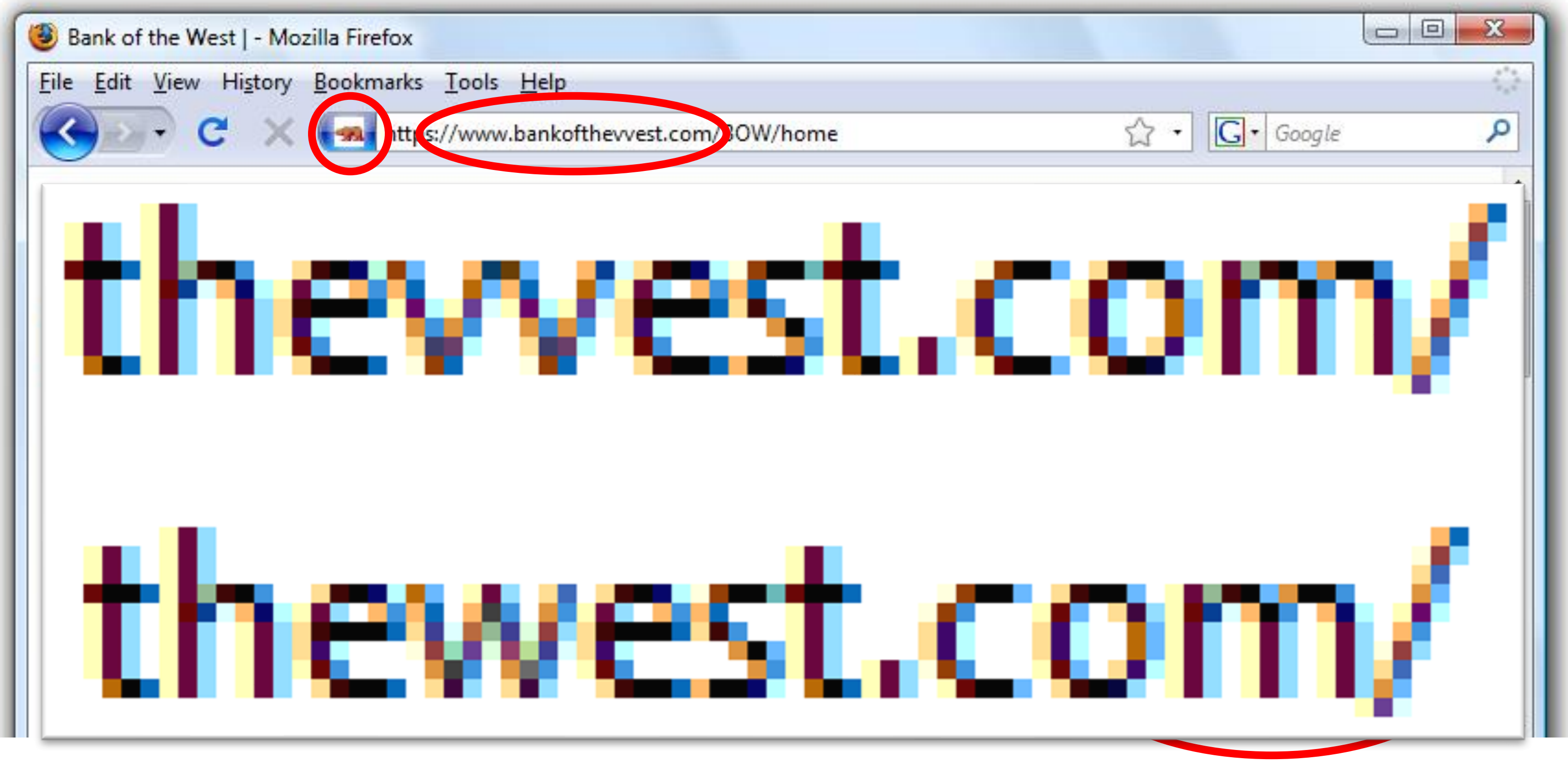
User name:

Password:

Login

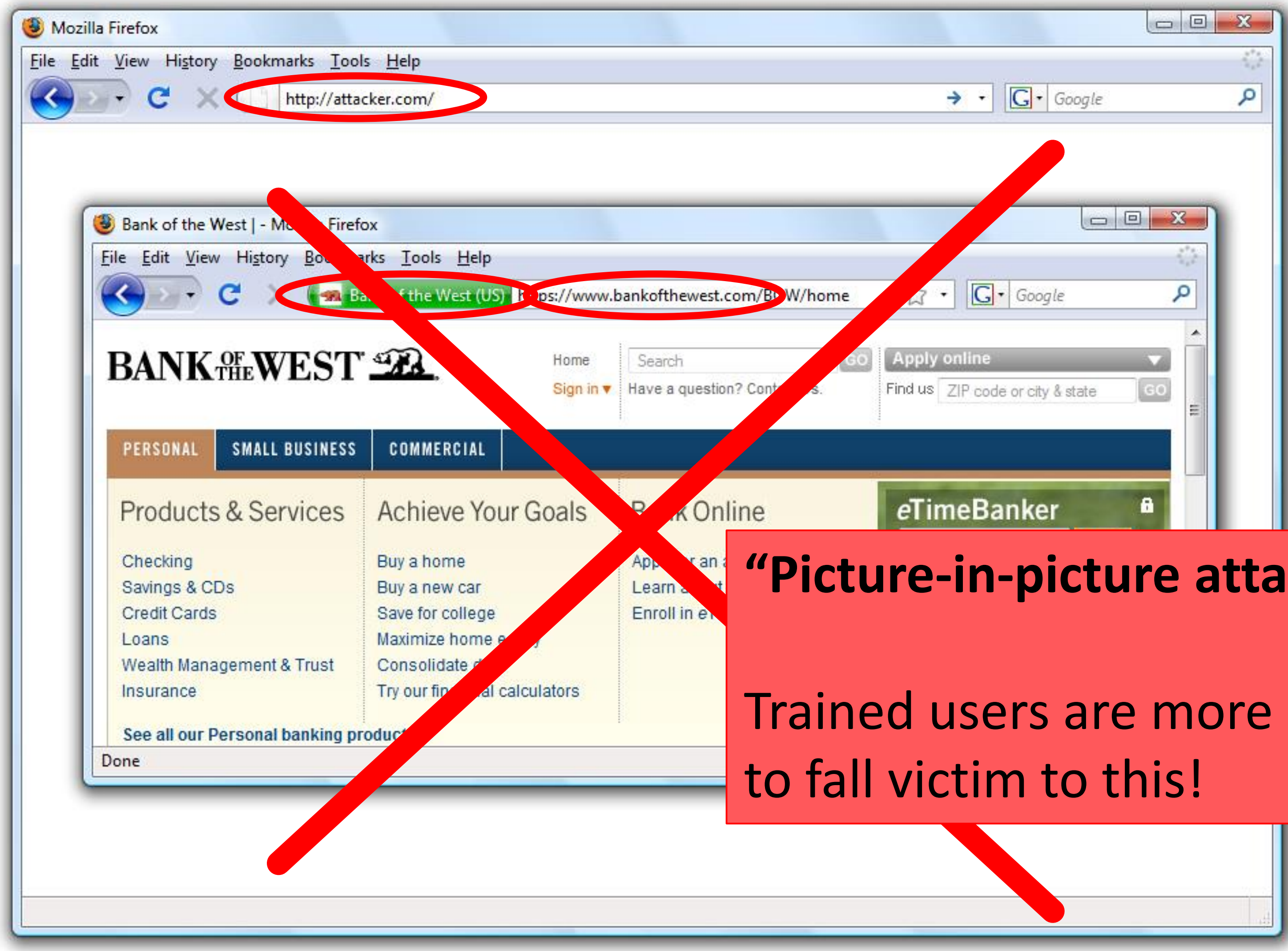
Done

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/

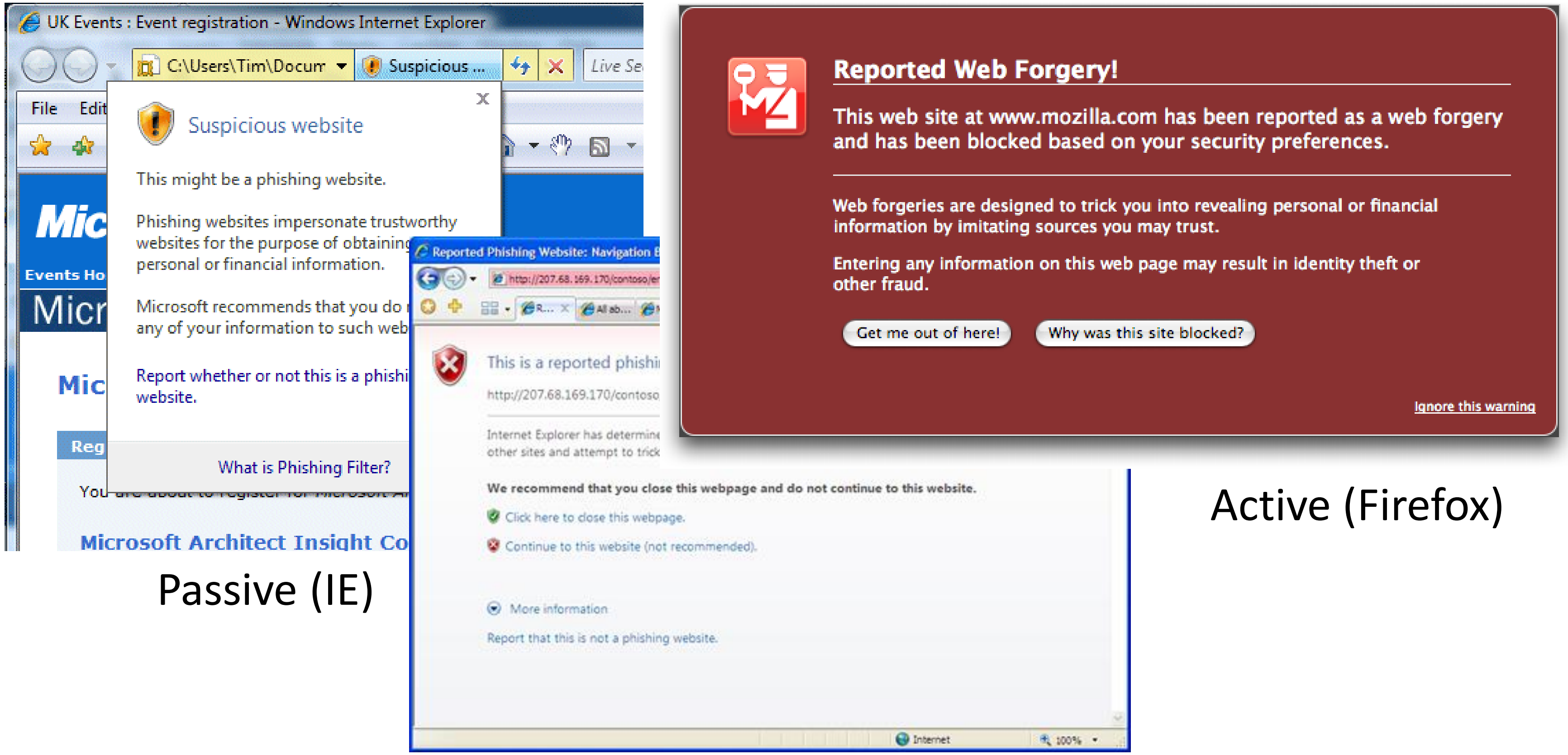
Safe to Type Your Password?



“Picture-in-picture attacks”

Trained users are more likely to fall victim to this!

Phishing Warnings (2008)



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?

You are about to register for Microsoft Ar

Microsoft Architect Insight Co

Passive (IE)

Reported Phishing Website: Navigation B
http://207.68.169.170/contoso/er

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.

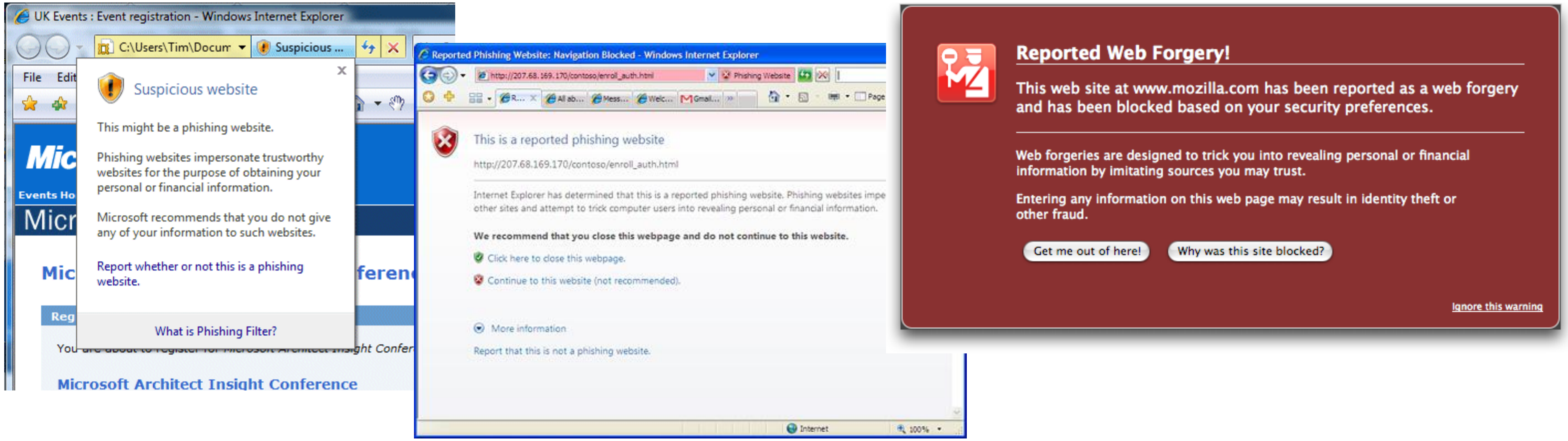
Entering any information on this web page may result in identity theft or other fraud.

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
Reg
ferenc
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.

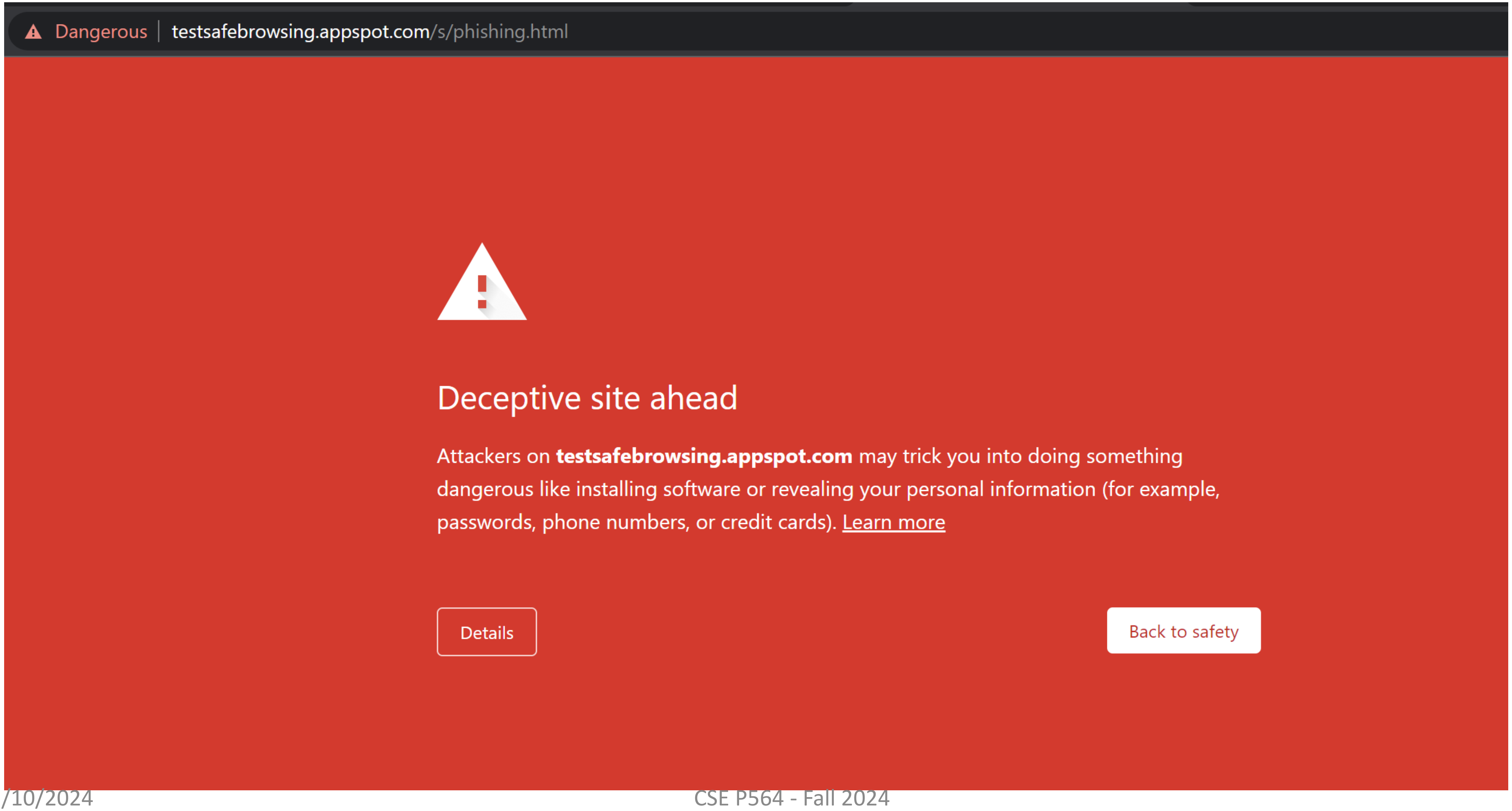
Passive (IE) Active (IE) Active (Firefox)

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)

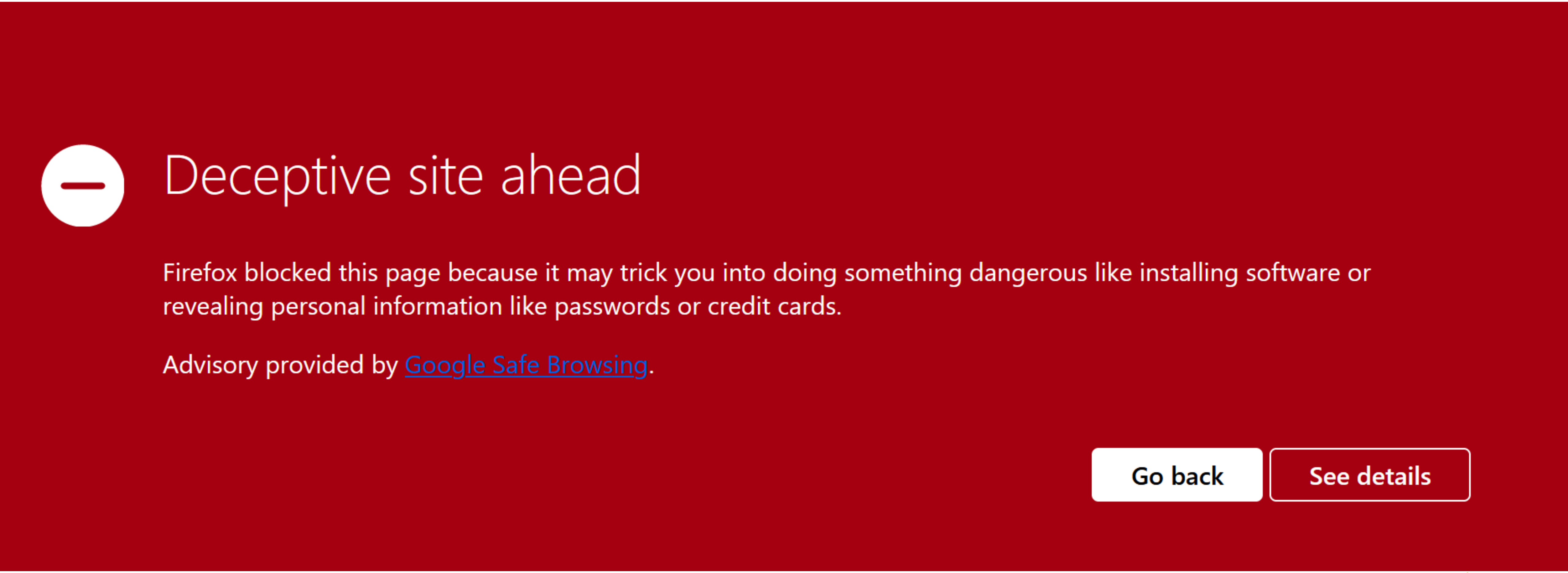
Modern warnings



Dangerous | testsafebrowsing.appspot.com/s/phishing.html

Deceptive site ahead

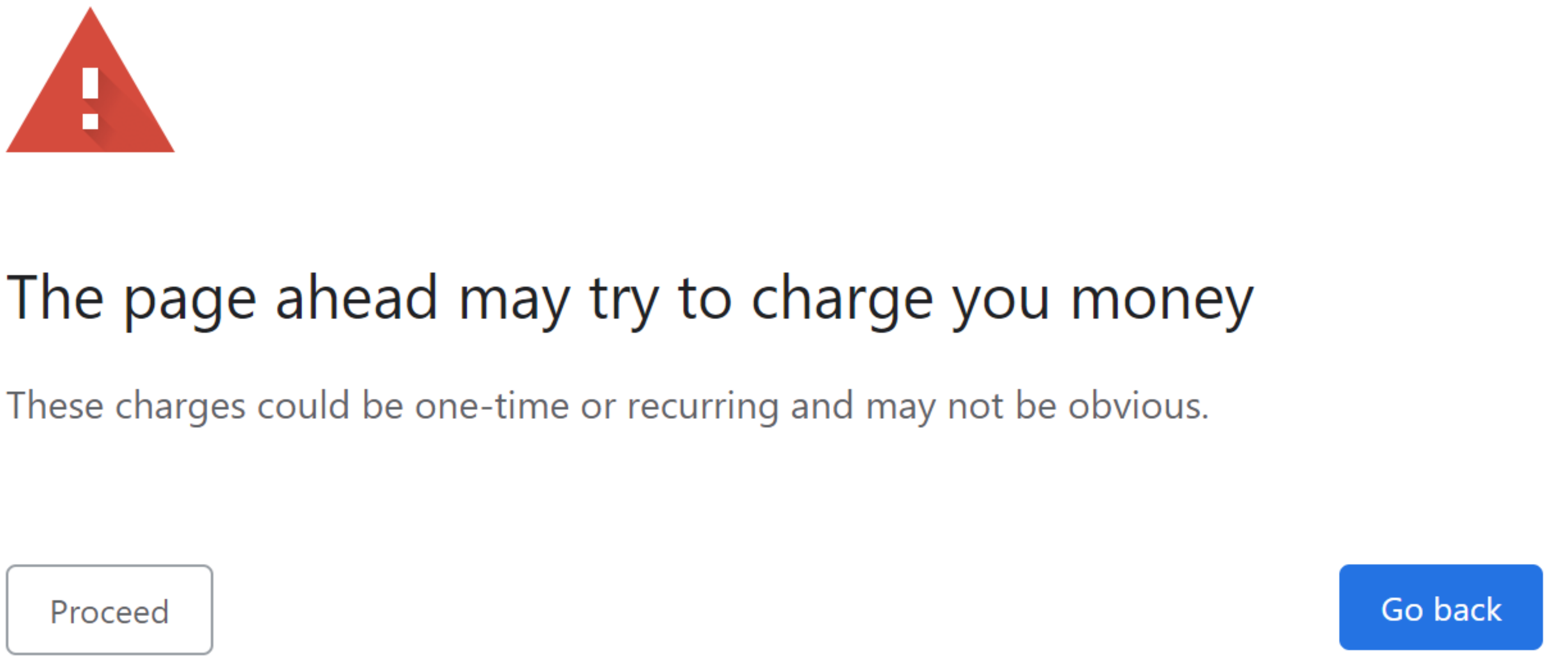
Attackers on **testsafebrowsing.appspot.com** may trick you into doing something dangerous like installing software or revealing your personal information (for example, passwords, phone numbers, or credit cards). Learn more



Deceptive site ahead

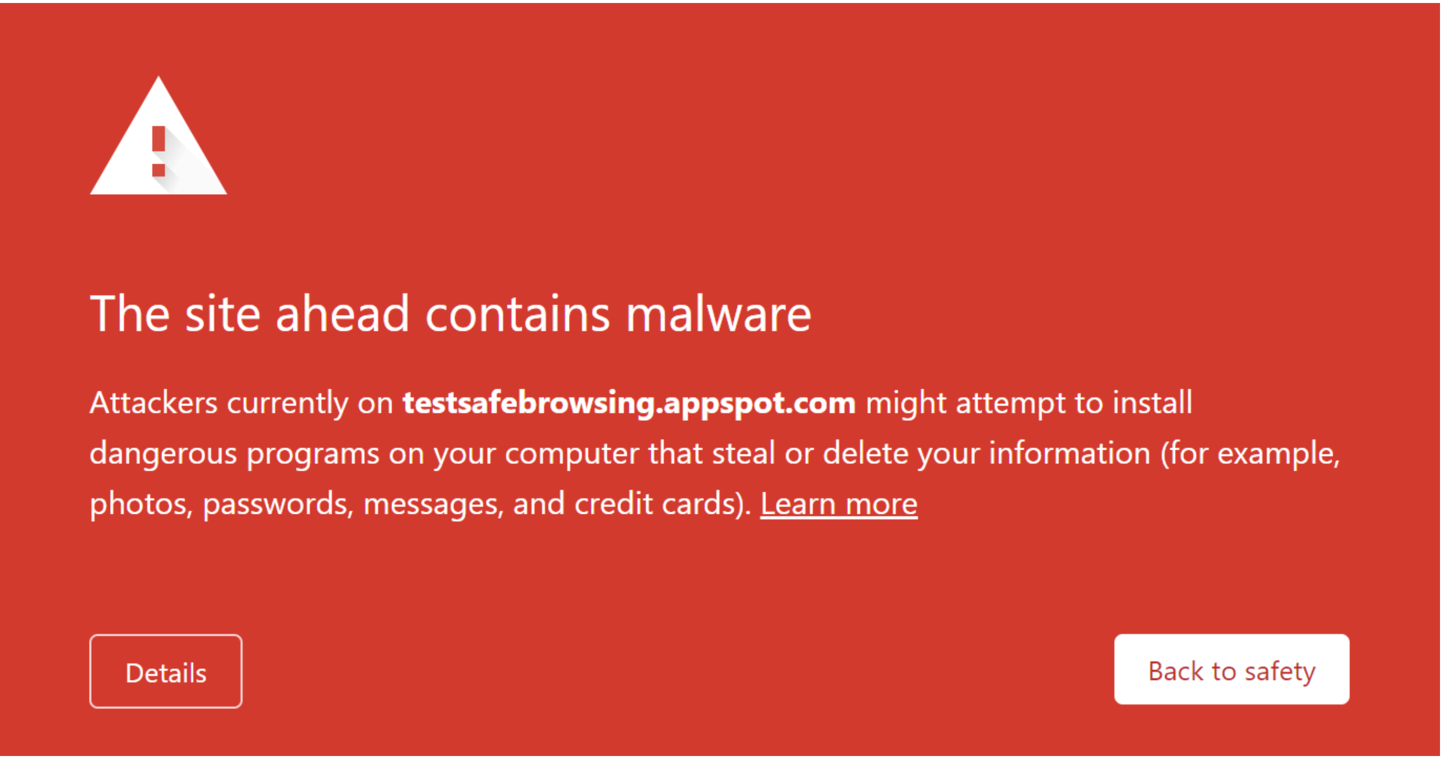
Firefox blocked this page because it may trick you into doing something dangerous like installing software or revealing personal information like passwords or credit cards.

Advisory provided by Google Safe Browsing.



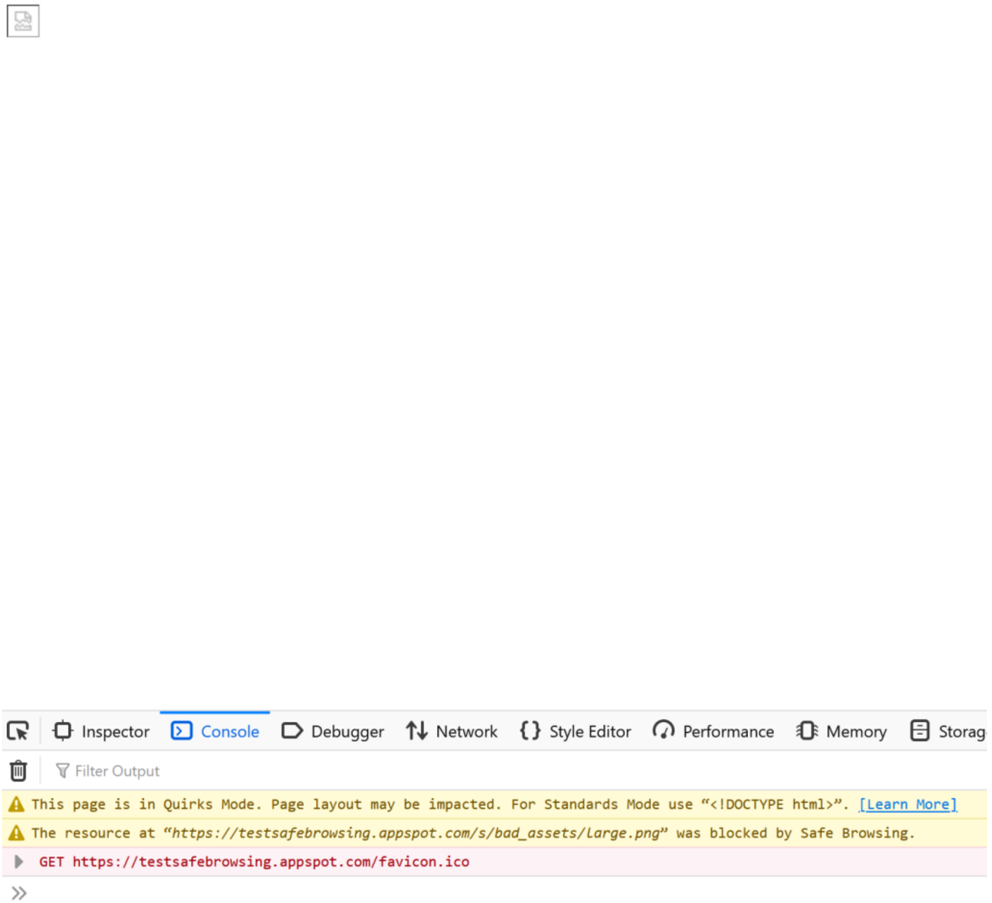
The page ahead may try to charge you money

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?

Exceptional Access

Or, letting the government into locked devices

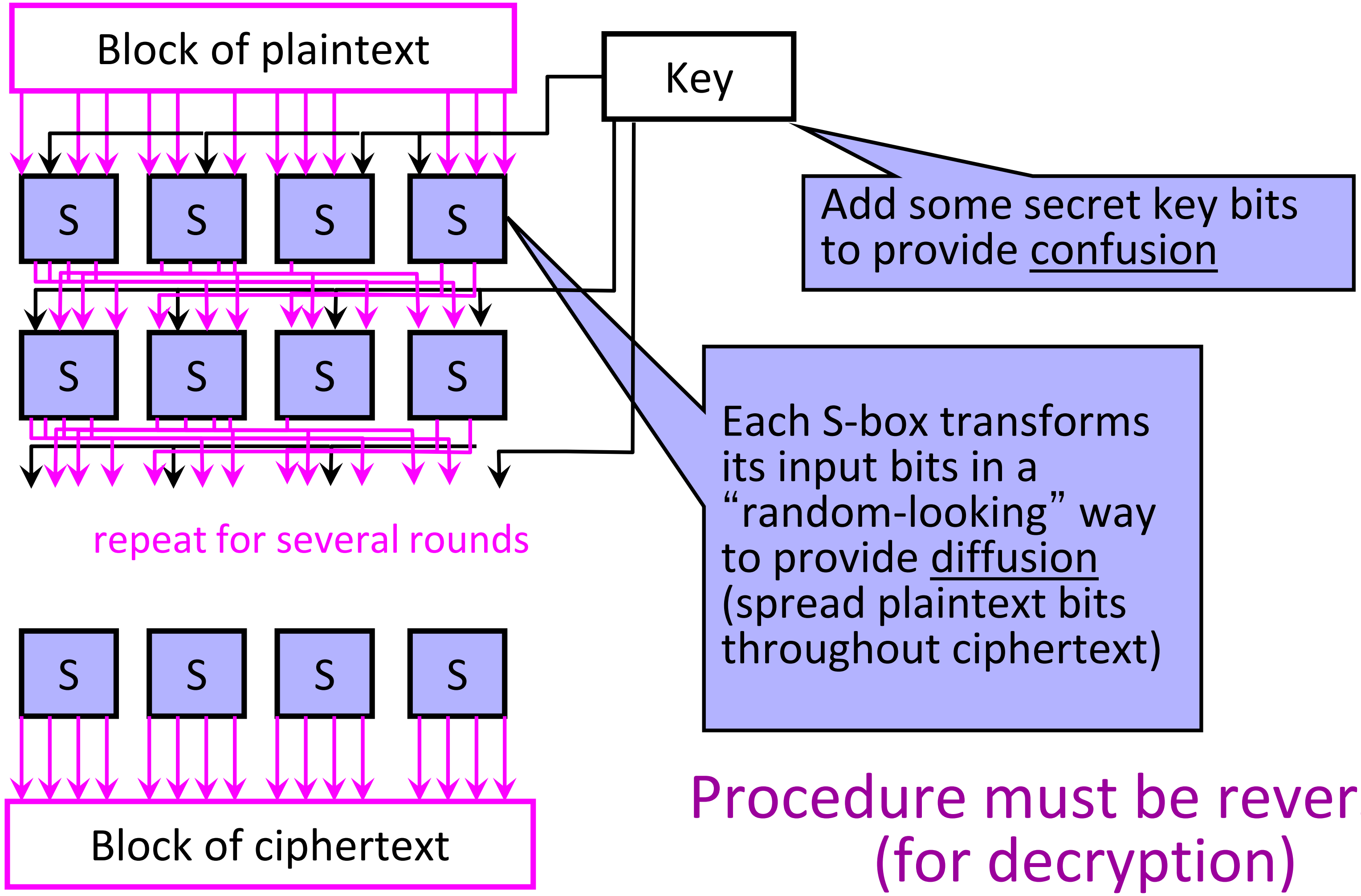
A brief aside, useful for consideration

- DES S-boxes

- Dual_EC_DRBG

DES S-boxes standardization

- Recall:

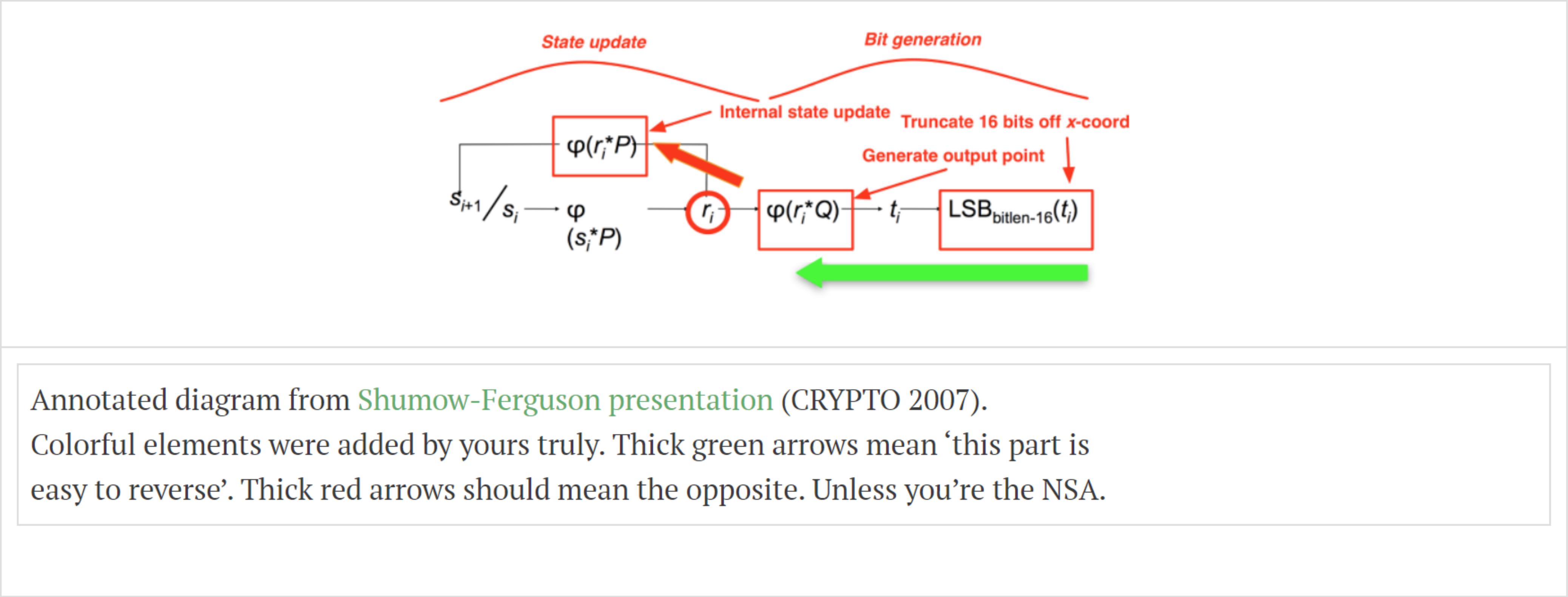


Add some secret key bits to provide confusion

Each S-box transforms its input bits in a “random-looking” way to provide diffusion (spread plaintext bits throughout ciphertext)

Procedure must be reversible (for decryption)

DUAL_EC_DRBG



Annotated diagram from Shumow-Ferguson presentation (CRYPTO 2007). Colorful elements were added by yours truly. Thick green arrows mean 'this part is easy to reverse'. Thick red arrows should mean the opposite. Unless you're the NSA.

https://blog.cryptographyengineering.com/2013/09/18/the-many-flaws-of-dualecdrbg/

https://hovav.net/ucsd/dist/juniper.pdf

History: Dual-use

- Technologies under restriction regimes may be *dual-use*

- A missile is *not* dual-use
  - Hunting firearms *are* dual-use

- That is, military and civilian applications

Discuss

History: Cryptography

- Post WWII all cryptography was a ‘munition’
  - Subject to export restrictions
  - Fundamentally a military technology

- This was (mostly) reasonable

- It stopped being (as) reasonable once electronic communications became a thing
  - Really clearly dual-use at this point

History: The crypto wars (1st)

- Cold war ends in 1991
- Some export restrictions are lifted in 1992
  - <40bits of key systems allowed
  - 40 bits is crackable in days at the time

- PGP (Pretty Good Privacy) written in 1992
  - >>>40 bits

- “Crypto wars” kick off as a reaction to restrictions

History: SSL in the 90s

- Netscape had SSL (HTTPS) for e-commerce
- Problem: SSL was 128bits of key
- Solution: Two versions of the browser
  - US Version: 128bits
  - International Version: 40bits (reveals 88bits)

History: The Clipper Chip

- 1994 a new system is proposed: Skipjack
- 80-bits of security
- “Trap-door” built in to allow government recovery of messages
  - This was public
- Proposal was to put the “clipper chip” into everything

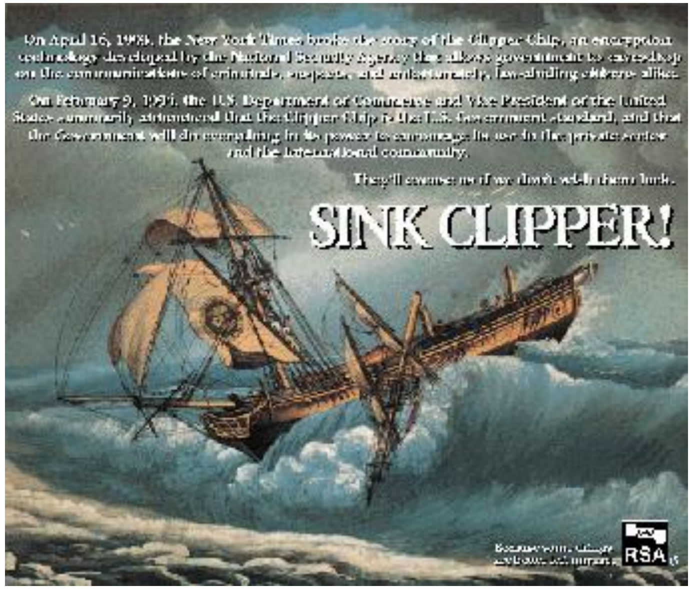
History: The Clipper Chip

- Argument was that ‘terrorists’ would be caught

- This was… not well received

- It also had a number of serious technical flaws

- It died reasonably fast


On April 16, 1993, the New York Times broke the story of the Clipper Chip, an encryption technology developed by the National Security Agency that allows government to eavesdrop on the communications of criminals, suspects, and unfortunately, law-abiding citizens alike.
On February 9, 1994, the U.S. Department of Commerce and Vice President of the United States summarily announced that the Clipper Chip is the U.S. Government standard, and that the Government will do everything in its power to encourage its use in the private sector and the international community.
SINK CLIPPER!
RSA

By Source (WP:NFCC#4), Fair use, https://en.wikipedia.org/w/index.php?curid=48926067

https://www.mattblaze.org/papers/escrow-acsac11.pdf

History: Crypto wars end

- In 2000 restrictions are eased
    - (Per 1996 order that made this possible)

- AES is standardized

- Cryptography ‘golden age’ starts

Today: Continuation

- Cryptography is back in the headlines
- It is trivial to have encrypted data
  - Mobile phones
  - Backup systems
  - Messaging platforms
- Governments want access to encrypted data

Good starting points

- Lawful Device Access without Mass Surveillance Risk: A Technical Design Discussion - Stefan Savage
  - http://cseweb.ucsd.edu/~savage/papers/lawful.pdf

- The Export of Cryptography in the 20th Century and the 21^{st} - Whitfield Diffie and Susan Landau
  - https://privacyink.org/pdf/export_control.pdf

- Key Escrow from a Safe Distance Looking Back at the Clipper Chip
  - https://www.mattblaze.org/papers/escrow-acsac11.pdf

Course Evaluation

- Please fill out the course evaluation!
  - https://uw.iasystem.org/survey/297878
  - Or check email

- A good activity for when you are done lockpicking or while you are waiting for locks ☺