CSE 484 / CSE M 584: Computer Security and Privacy

# Usable Security

Spring 2019

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 ...

# 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

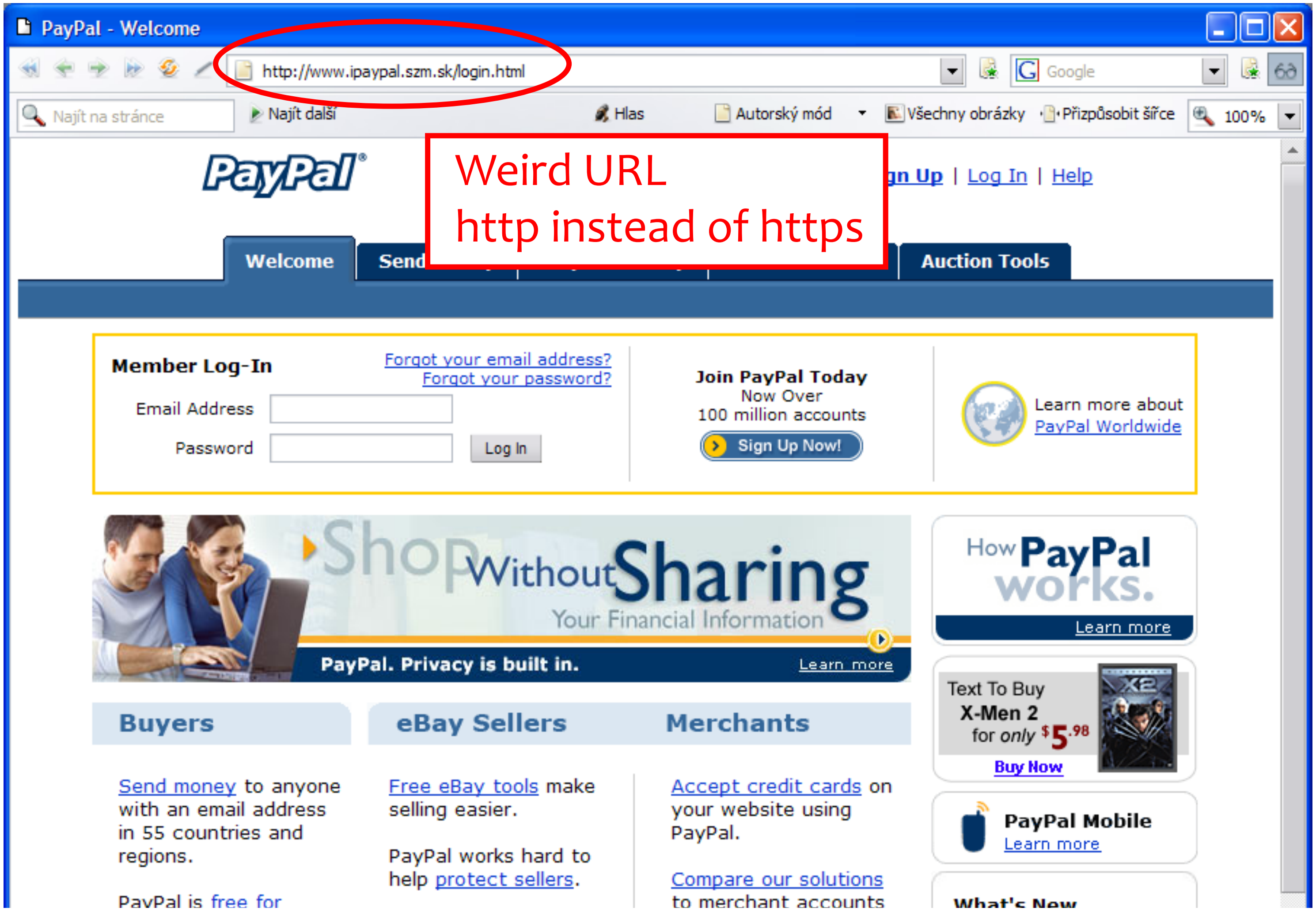
# Usable Security Roadmap

- Lessons from 3 design case studies:
  1. Phishing
  2. SSL indicators
  3. Password managers
- 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

**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

Text To Buy **X-Men 2** for *only* $5.98

**PayPal Mobile** Learn more

**What's New**

**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.

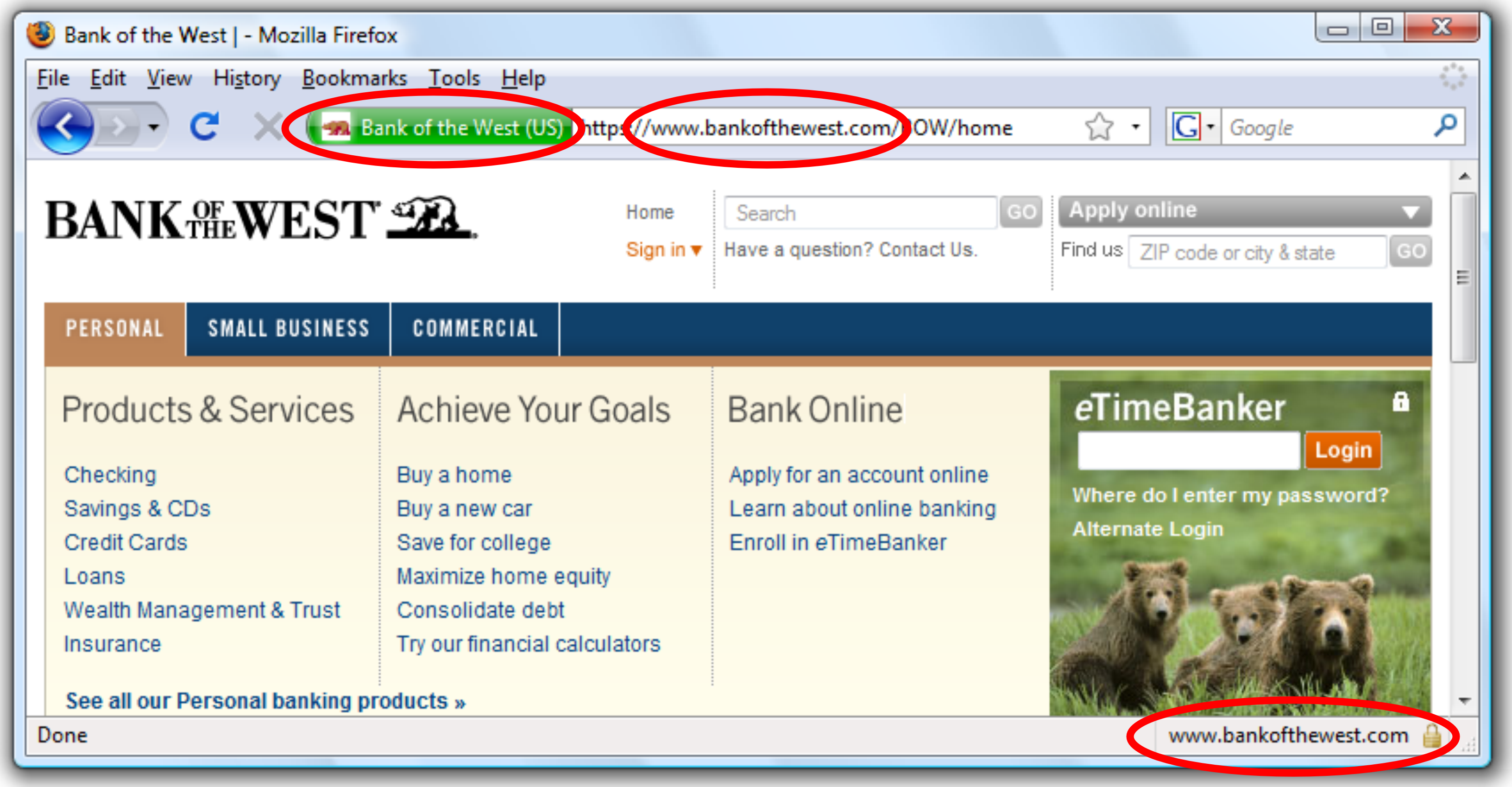
PayPal works hard to help protect sellers.

**Merchants**

Accept credit cards on your website using PayPal.

Compare our solutions to merchant accounts

# Safe to Type Your Password?



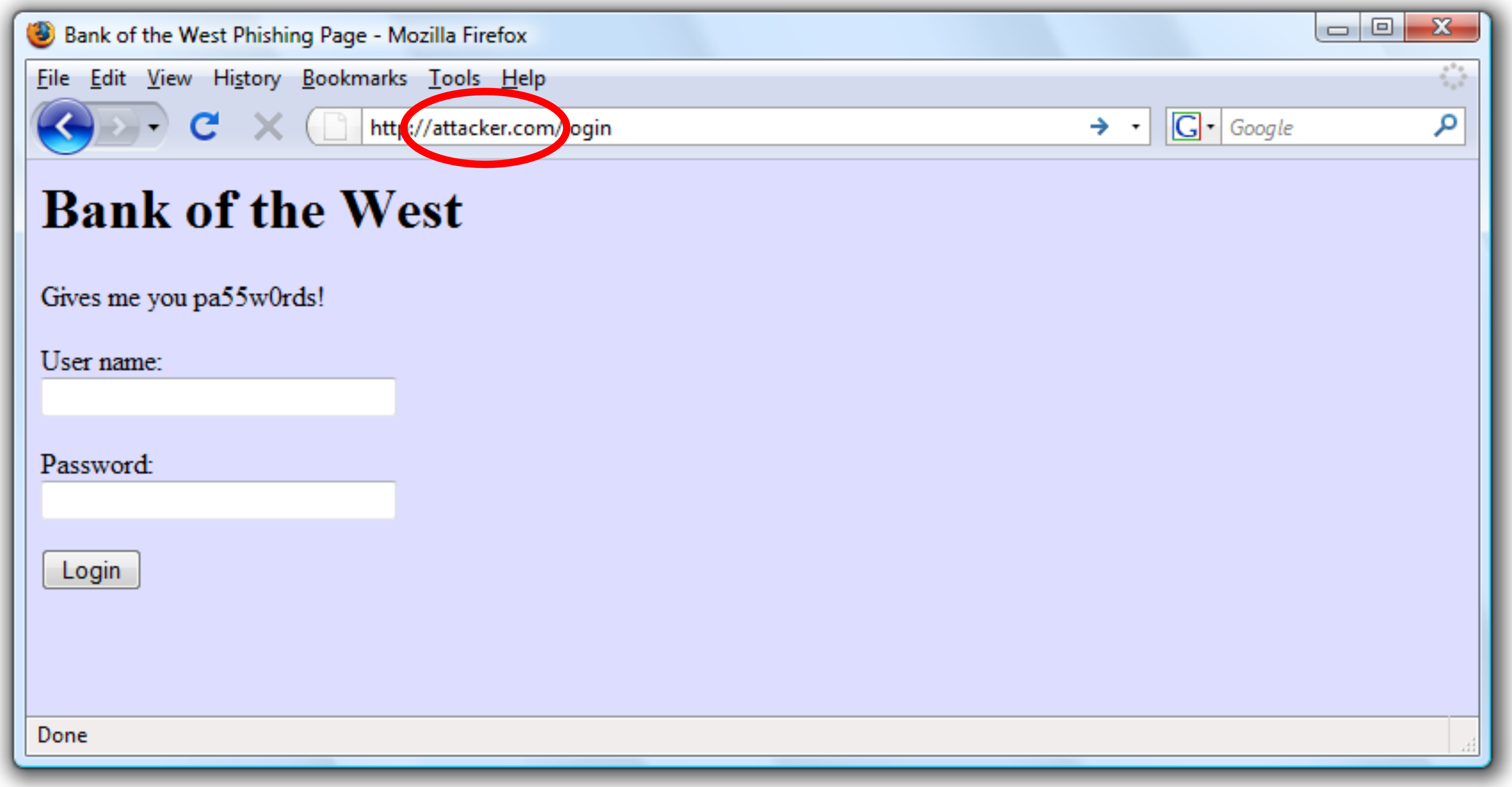
Bank of the West | - Mozilla Firefox

Bank of the West (US) https://www.bankofthewest.com/BOW/home

Done

www.bankofthewest.com

# 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

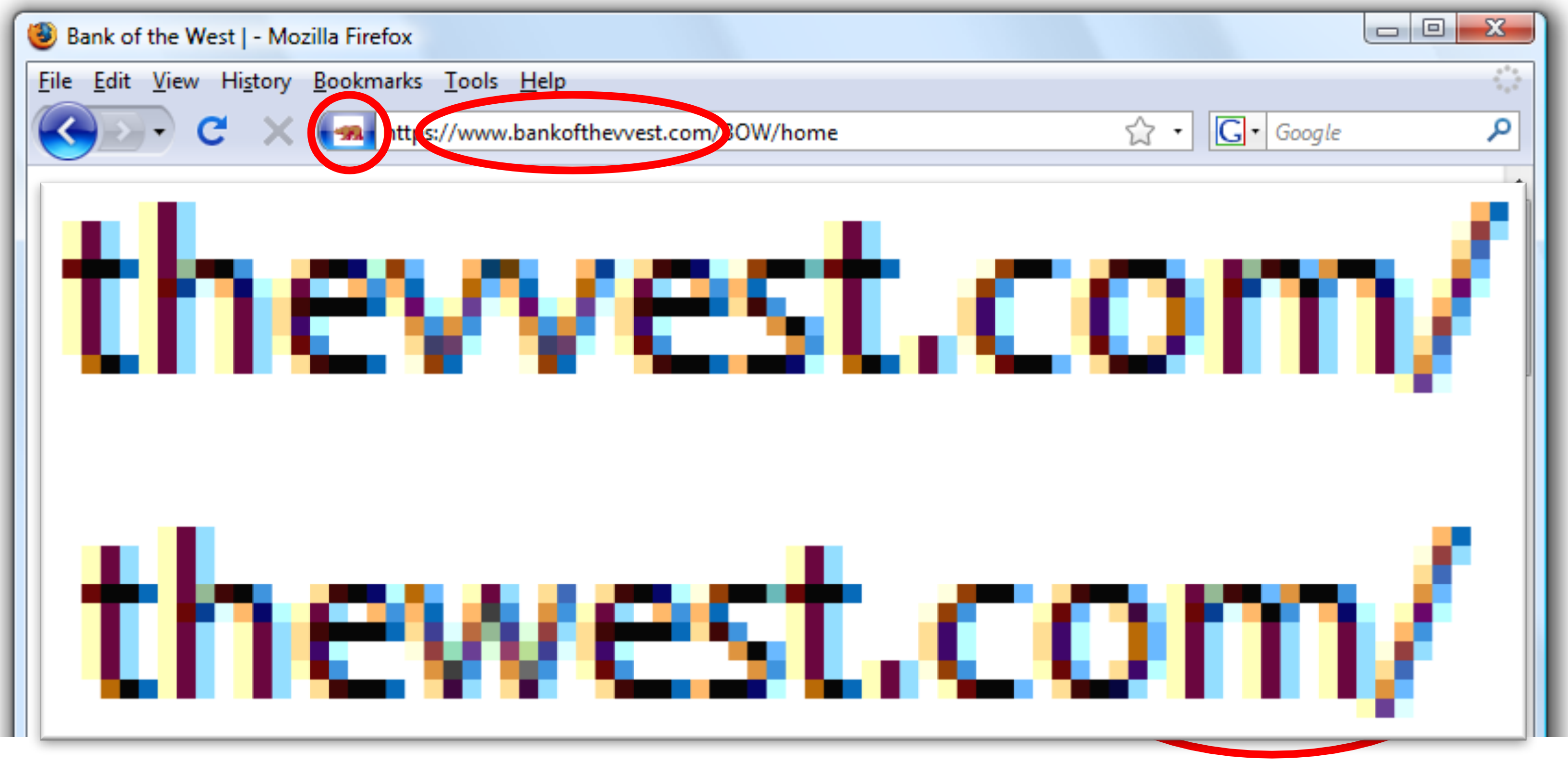
Bank of the West

Gives me you pa55w0rds!

User name:

Password:

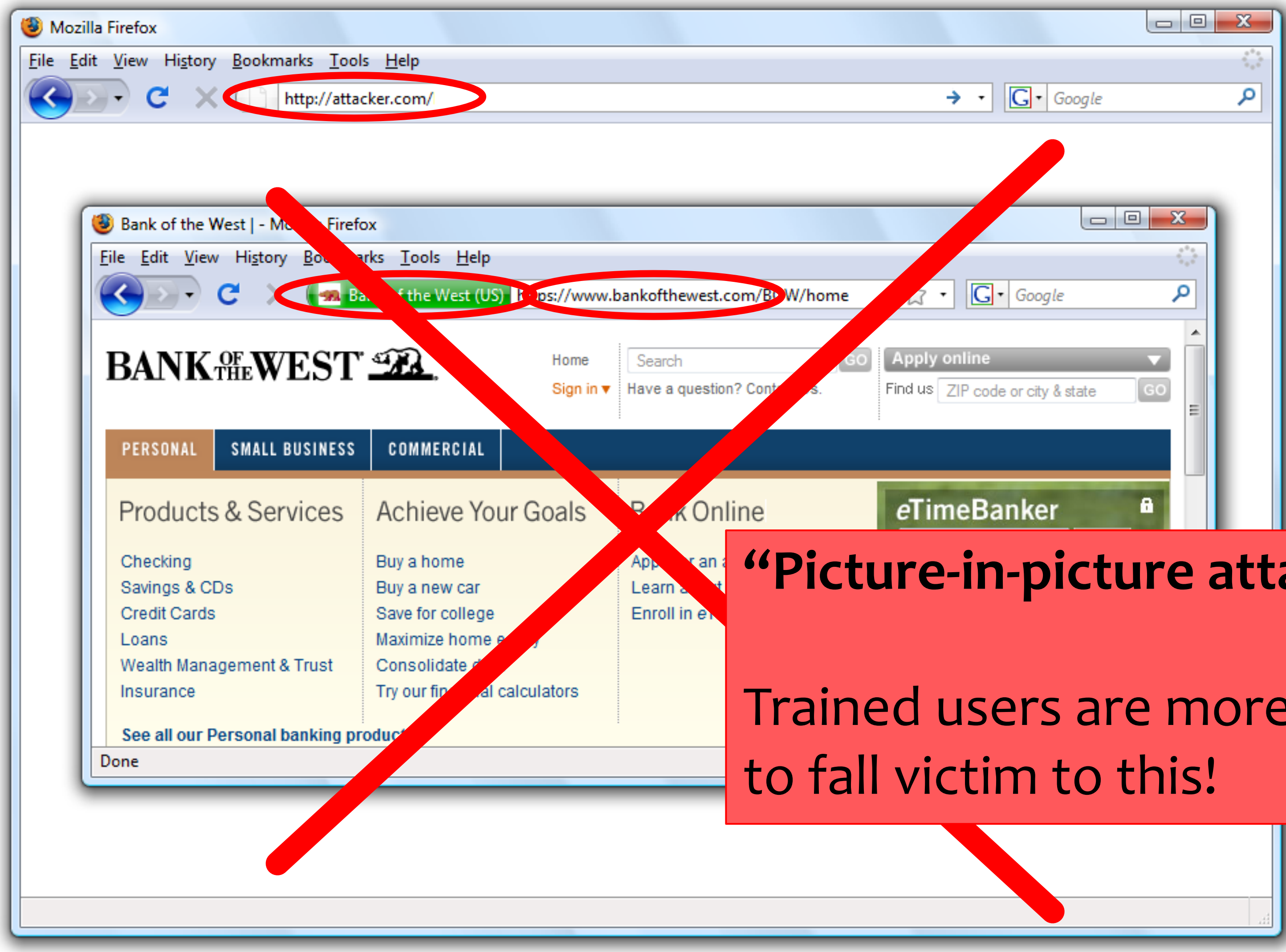
# Safe to Type Your Password?



Bank of the West | - Mozilla Firefox

https://www.bankofthevvest.com/BOW/home

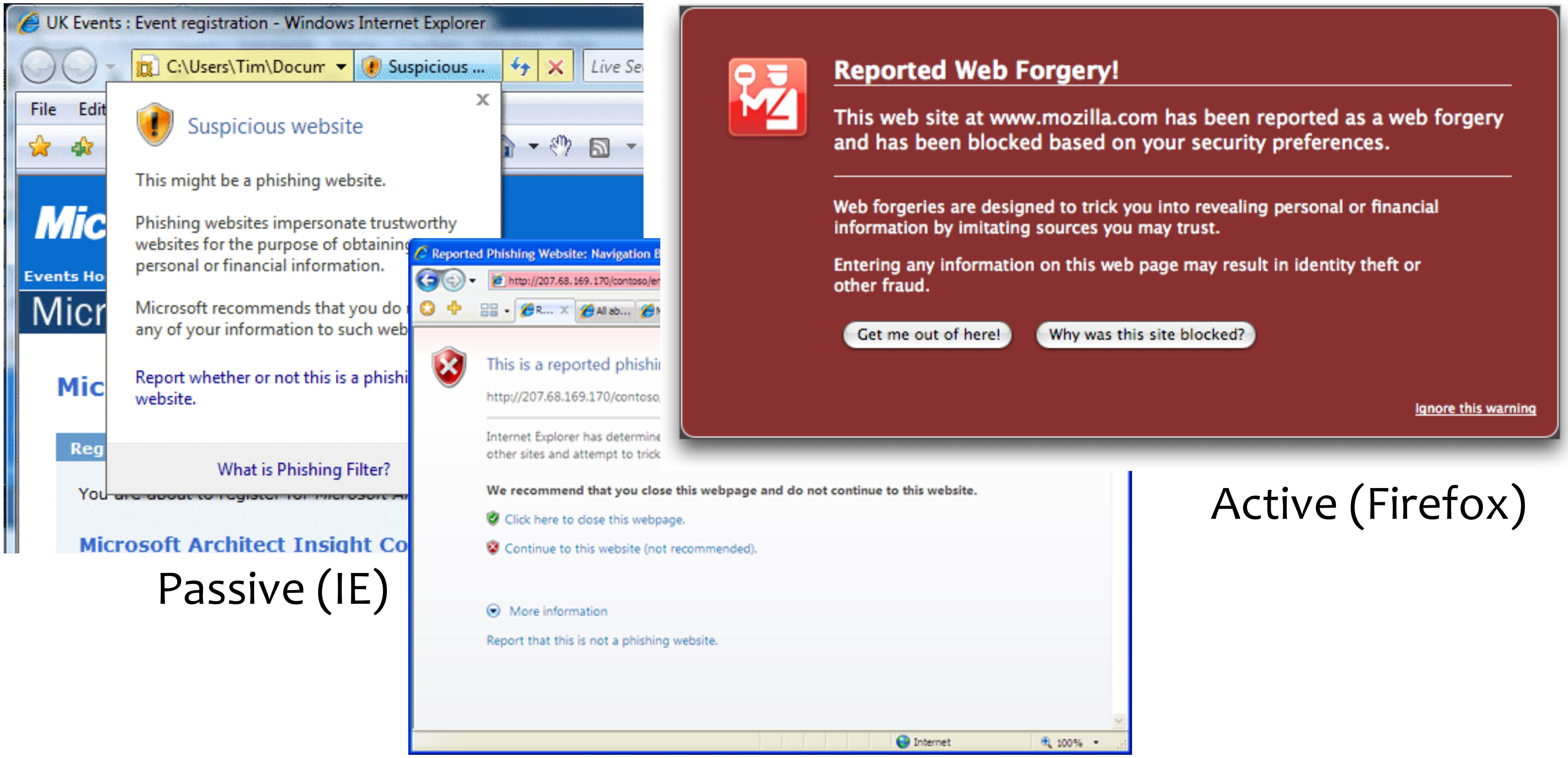
# Safe to Type Your Password?



**"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?

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.

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)

[Egelman et al.]

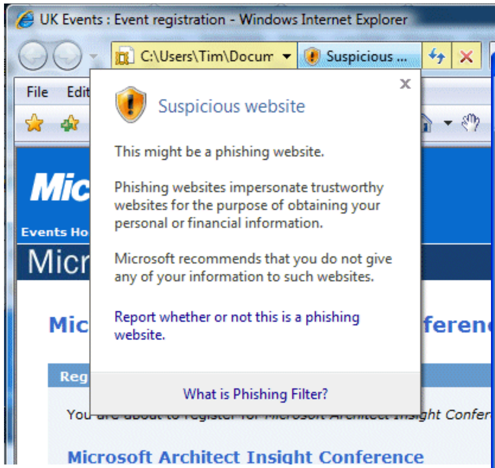
# Are Phishing Warnings Effective?

- 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
feren
Reg
Microsoft Architect Insight Conference

Suspicious website

This might be a phishing website.

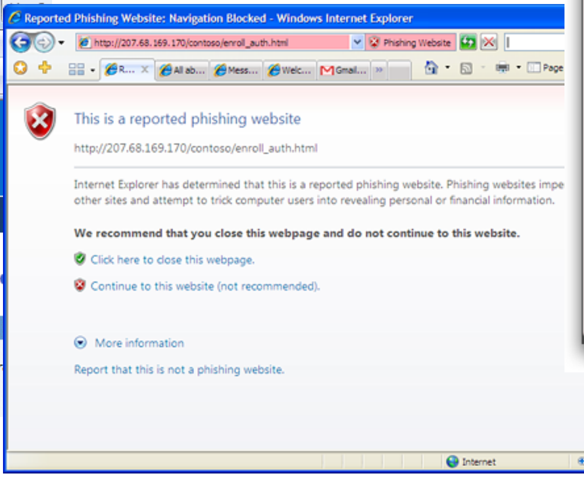
Phishing websites impersonate trustworthy websites for the purpose of obtaining your personal or financial information.

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.**

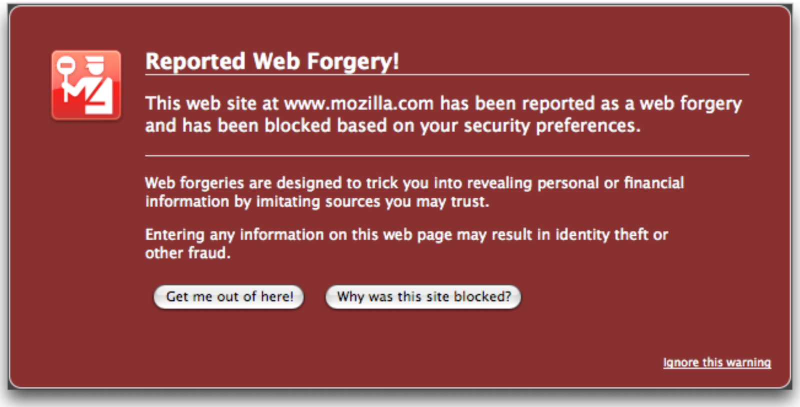
Click here to close this webpage.

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.]

# Active vs. Passive Warnings

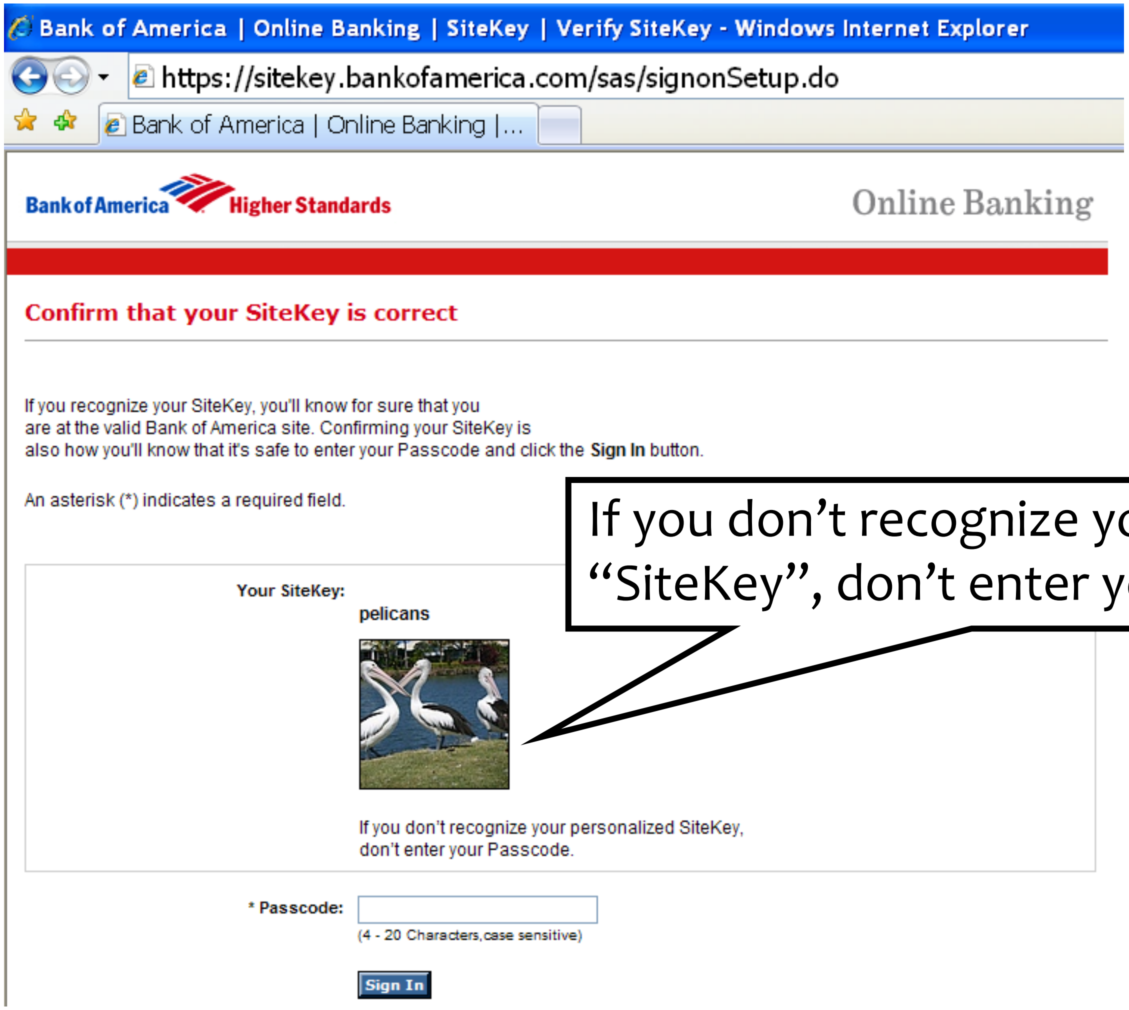
- Some fail to notice warnings entirely
  - Passive warning takes a couple of seconds to appear; if user starts typing, his keystrokes dismiss the warning
- Some saw the warning, closed the window, went back to email, clicked links again, were presented with the same warnings… repeated 4-5 times
  -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

- 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”
- Common issue: Warning/prompt fatigue
  - We’ll see this issue again re: mobile security…

# 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
Sign In

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:**

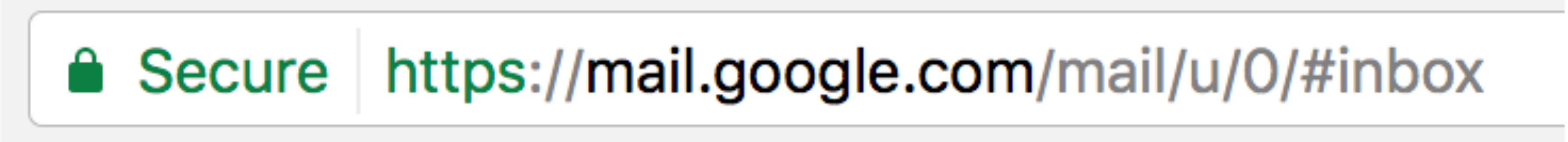
(4 - 20 Characters, case sensitive)

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

# Case Study #2: Browser 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?
  *[covered in section last week]*

# The Lock Icon

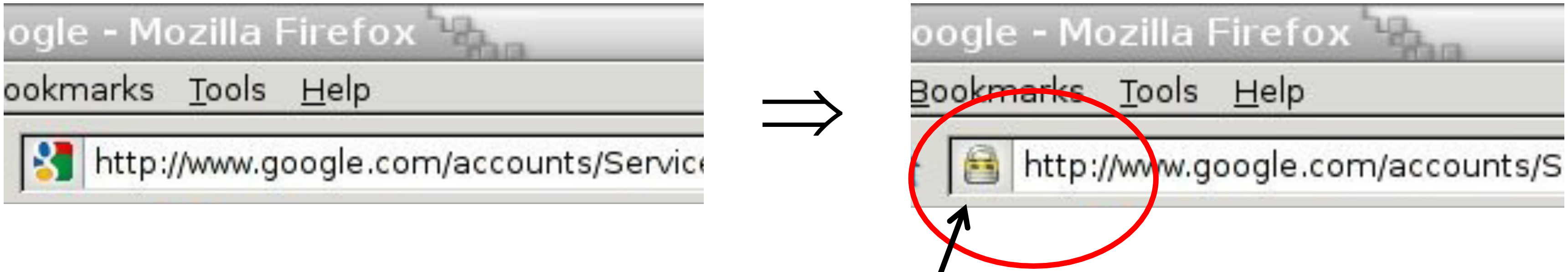


🔒 Secure | https://mail.google.com/mail/u/0/#inbox

- 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]

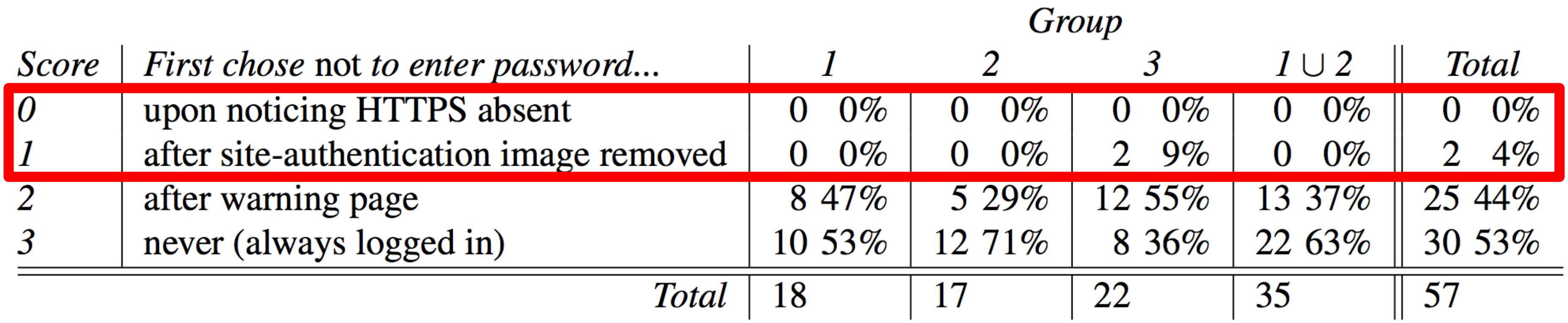
# Will You Notice?



Clever favicon inserted by network attacker

# Do These Indicators Help? (2007)

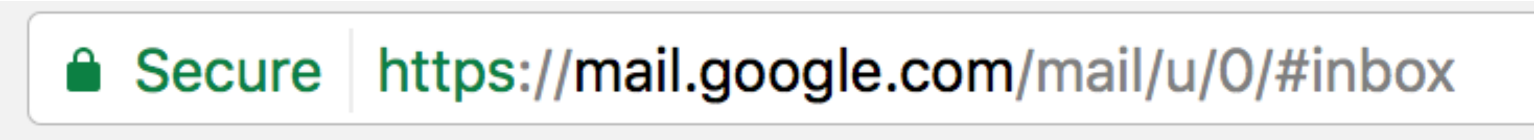
- “The Emperor’s New Security Indicators”
  - http://www.usablesecurity.org/emperor/emperor.pdf



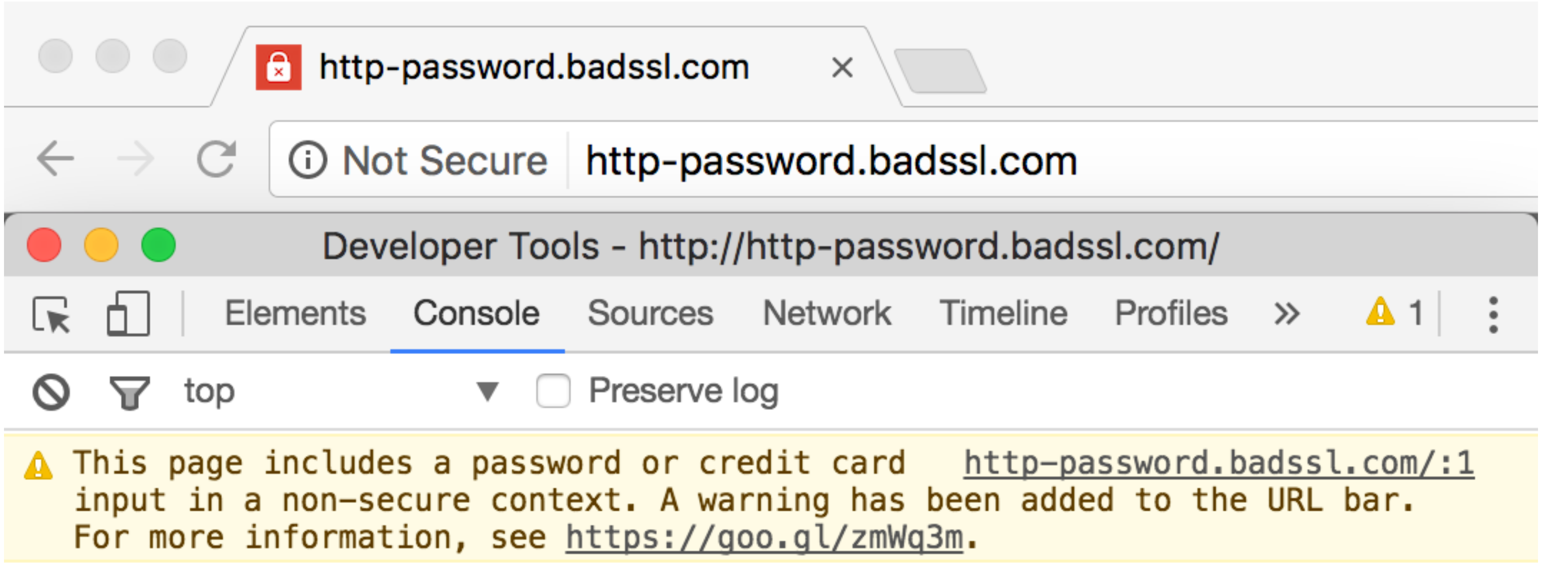
|  |  | *Group* |  |  |  |  |
|---|---|---|---|---|---|---|
| *Score* | *First chose* not *to enter password...* | *1* | *2* | *3* | *1* ∪ *2* | *Total* |
| *0* | upon noticing HTTPS absent | 0 0% | 0 0% | 0 0% | 0 0% | 0 0% |
| *1* | after site-authentication image removed | 0 0% | 0 0% | 2 9% | 0 0% | 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 |

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

# Latest Design in Chrome



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



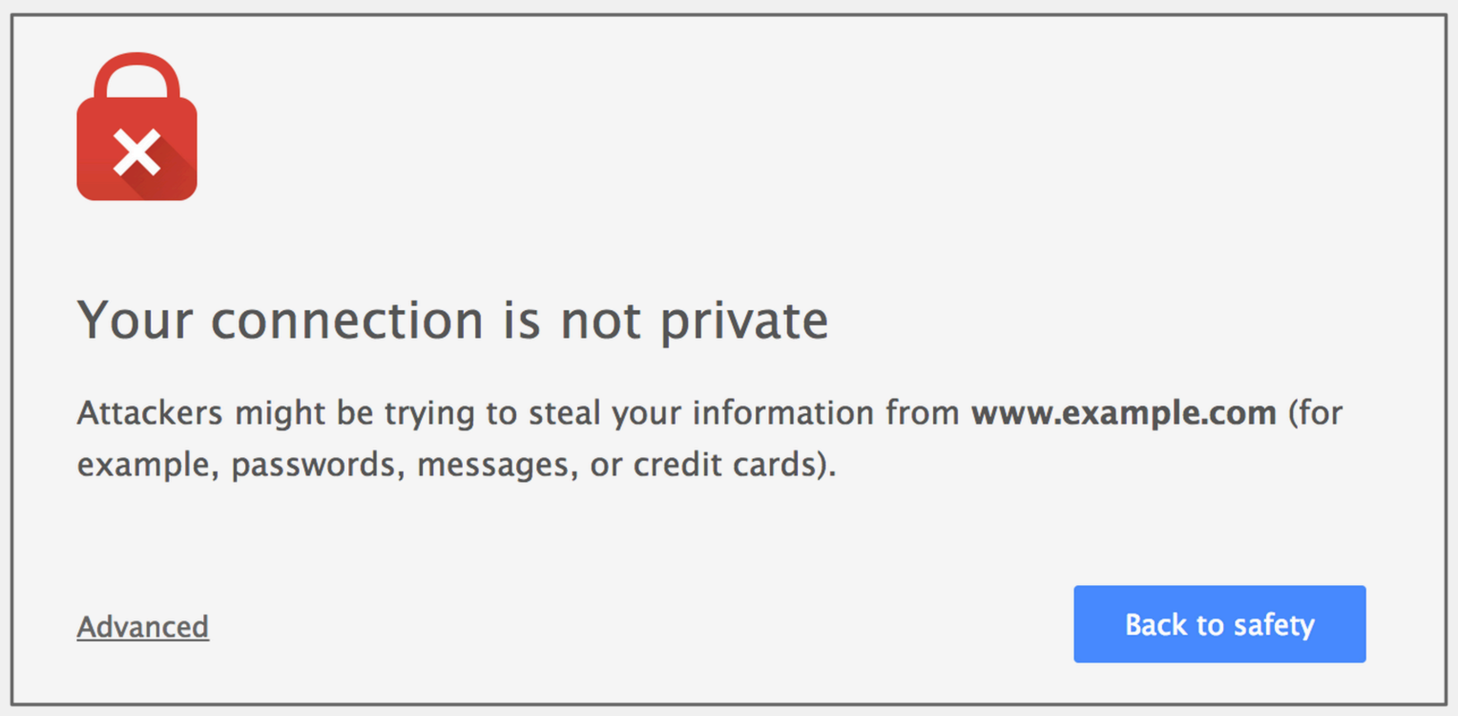
ⓘ Not Secure http-password.badssl.com

Developer Tools - http://http-password.badssl.com/

```
⚠ 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.
```

# HTTPS Warnings

- When HTTPS connection is “bad” (e.g., untrusted cert)
- Discussed last week in section
- Opinionated design helps!



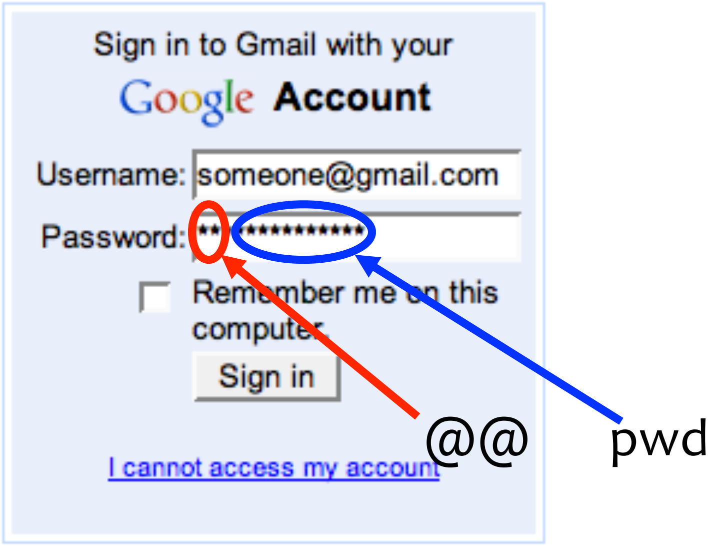
Your connection is not private

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

# Case Study #3: Password Managers

- Password managers handle creating and "remembering" strong passwords
- Potentially:
  - **Easier** for users
  - More **secure**
- Early examples:
  - PwdHash (Usenix Security 2005)
  - Password Multiplier (WWW 2005)

# PwdHash



Sign in to Gmail with your
Google Account

Username: someone@gmail.com

Password: *************

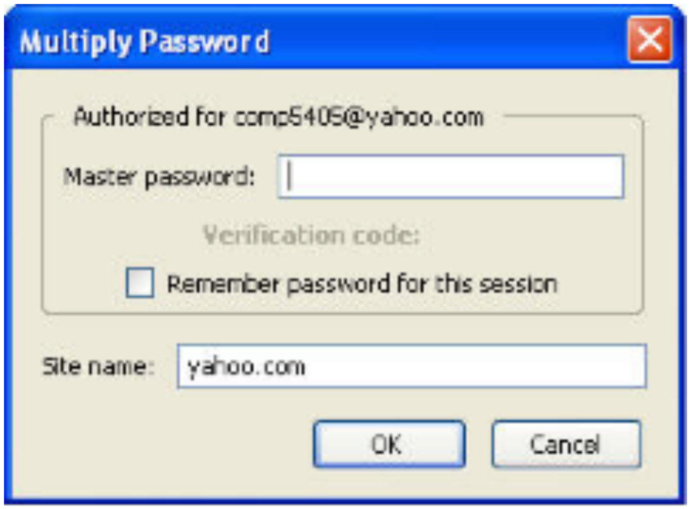
□ Remember me on this computer.

@@ in front of passwords
to protect; or F2

sitePwd = Hash(pwd,domain)

Prevent phishing attacks

# Password Multiplier



Multiply Password

Authorized for comp5405@yahoo.com

Master password:

Verification code:

□ Remember password for this session

Site name: yahoo.com

Activate with Alt-P or
double-click

sitePwd = Hash(username,
pwd, domain)

Both solutions target simplicity and transparency.

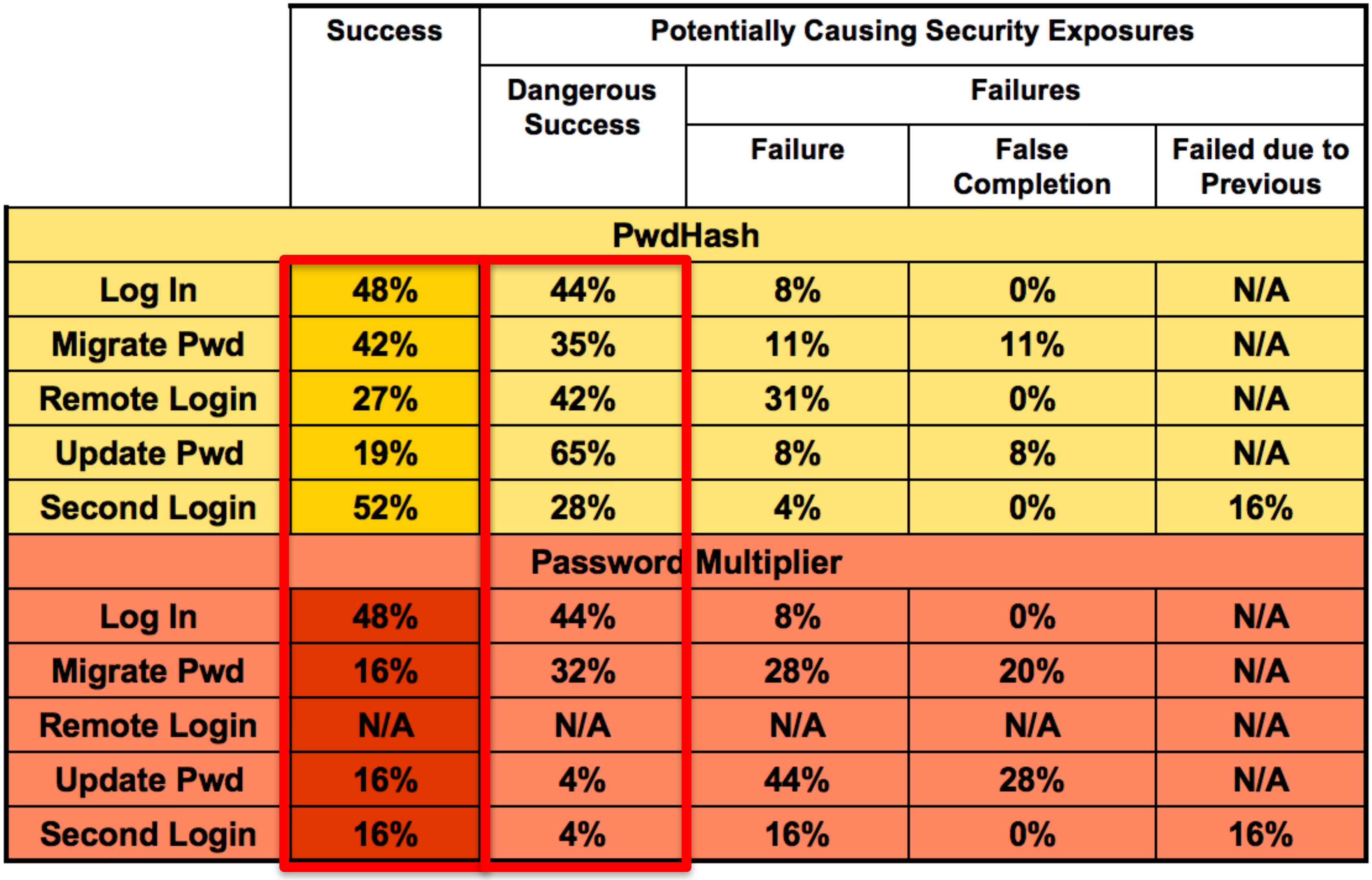
[Chiasson, van Oorschot, Biddle]

# Usability Testing

- Are these programs usable? If not, what are the problems?
- Approaches for evaluating usability:
  - Usability inspection (no users)
    - Cognitive walkthroughs
    - Heuristic evaluation
  - User study
    - Controlled experiments
    - Real usage

[Chiasson, van Oorschot, Biddle]

# Task Completion Results



| | Success | Potentially Causing Security Exposures | | | |
|---|---|---|---|---|---|
| | | Dangerous Success | Failures | | |
| | | | Failure | False Completion | Failed due to Previous |
| PwdHash | | | | | |
| Log In | 48% | 44% | 8% | 0% | N/A |
| Migrate Pwd | 42% | 35% | 11% | 11% | N/A |
| Remote Login | 27% | 42% | 31% | 0% | N/A |
| Update Pwd | 19% | 65% | 8% | 8% | N/A |
| Second Login | 52% | 28% | 4% | 0% | 16% |
| Password Multiplier | | | | | |
| Log In | 48% | 44% | 8% | 0% | N/A |
| Migrate Pwd | 16% | 32% | 28% | 20% | N/A |
| Remote Login | N/A | N/A | N/A | N/A | N/A |
| Update Pwd | 16% | 4% | 44% | 28% | N/A |
| Second Login | 16% | 4% | 16% | 0% | 16% |

[Chiasson, van Oorschot, Biddle]

# Problem: Mental Model

- Users seemed to have misaligned mental models
  - Not understand that one needs to put "@@" before *each* password to be protected.
  - Think different passwords generated for each session.
  - Think successful when were not.
  - Not know to click in field before Alt-P.
  - Don't understand what's happening: "Really, I don't see how my password is safer because of two @'s in front"

[Chiasson, van Oorschot, Biddle]

# Problem: Transparency

- Unclear to users whether actions successful or not.
  - Should be obvious when plugin activated.
  - Should be obvious when password protected.
- Users feel that they should be able to know their own password.

[Chiasson, van Oorschot, Biddle]

# Problem: Dangerous Errors

- Tendency to try all passwords
  - A poor security choice – phishing site could collect many passwords!
  - May make the use of PwdHash or Password Multiplier *worse* than not using any password manager.
- Usability problem leads to security vulnerabilities.
  - Theme in course: sometimes things designed to increase security can also increase other risks

# Beyond Specific Tools: Different User Groups

- Not all users are the same!
- Designing for one group of users, or "generic" users, may leads to dangerous failures or reasons that people will not use security tools
- Examples from (qualitative) research at UW:
  - Journalists (most sources are not like Snowden!)
  - Refugees in US (security measures may embed US cultural assumptions!)

# 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
- …?