Advanced Security Tips for End Users
Today’s Agenda

A Deeper Dive

- Do not click on suspicious links
- Use a secure password
- Use an antivirus
- Never bank from an untrusted network
Do not click on suspicious links

How do I know where the URL is taking me?

How can I tell if a website is not malicious?
Where is this taking me?

http://www.diinnovationconference.com/
http://63.172.234.25
http://0x3FACEA19
http://1068296729
http://077.0254.0352.031
http://goo.gl/jeSA3x
http://bit.ly/1tDt0LB
http://tinyurl.com/jvuhogy
http://d%49%49%6E%6E%6Fvat%49%6F%6E%63%6F%6Efer%6E%63%6Fm/
How do I know where the URL is taking me?

http://longurl.org/
How can I tell if a website is not malicious?

Norton Safeweb
https://safeweb.norton.com/

McAfee Threat Intelligence
http://www.trustedsource.org/
Use a secure password

- How secure is my password?
- Have I been affected by a breach?
- How can I keep my password safe?
Adopt MFA!

- Google
- Facebook
- LinkedIn
- ...
How secure is my password?

https://howsecureismypassword.net/
**Complex vs. Long Passwords?**

- **Complex Password: Tr0ub4dor & 3**
  - Uncommon (non-gibberish) base word
  - Order unknown
  - Caps?
  - Common substitutions
  - Numerical
  - Punctuation
  - ~28 bits of entropy
  - \(2^{28} \approx 3 \text{ days at 1000 guesses/sec}\)
  - Difficulty to guess: EASY
  - Difficulty to remember: HARD

- **Long Password: Correct horse battery staple**
  - Four random common words
  - ~44 bits of entropy
  - \(2^{44} \approx 550 \text{ years at 1000 guesses/sec}\)
  - Difficulty to guess: HARD
  - Difficulty to remember: YOU’VE ALREADY MEMORIZED IT

*Through 20 years of effort, we’ve successfully trained everyone to use passwords that are hard for humans to remember, but easy for computers to guess.*
How to keep up with a different password for every site?

- lastpass.com, password safe
Should we Autofill?

**Browser-based:**
- Chrome 34
- Firefox 29
- Safari 7.0
- IE 11
- Android Browser 4.3

**Third-party:**
- 1Password 4.5
- LastPass 2.0
- KeePass 2.24
- Keeper 7.5
- Norton IdentitySafe 2014

Credits: David Silver, Suman Jana, and Dan Boneh, Stanford University; Eric Chen and Collin Jackson, Carnegie Mellon University
Attacks against autofill?

• Dynamically change "form action" tag using JavaScript
• DNS trickery (change IP, maintain DNS name)
• Redirect sweep attack on HTTP Login Page (Aug 22 2014).

Credits: David Silver, Suman Jana, and Dan Boneh, Stanford University; Eric Chen and Collin Jackson, Carnegie Mellon University
Redirect Sweep Attack on HTTP Login Page

Credits: David Silver, Suman Jana, and Dan Boneh, Stanford University; Eric Chen and Collin Jackson, Carnegie Mellon University
Disable Autofill…

Vulnerable

Automatic

Not Vulnerable

Manual

Credits: David Silver, Suman Jana, and Dan Boneh, Stanford University; Eric Chen and Collin Jackson, Carnegie Mellon University
How to find out if my password or my user’s accounts have been breached?

https://haveibeenpwned.com
Use an Antivirus

Do I still need AV?

How to I know my AV is working?

The AV says the file is okay... Can I get a “second opinion”?
Is Antivirus still relevant?

- Traditional AV is not enough
- Firewall
- Digital identity safeguard
- Prevents unauthorized access to webcam
- Alerts dangerous public WiFi networks
- Parental control
- Vulnerability scanner
- System hardening
- Download intelligence
- Behavior blocking
- Email, IM scan
- System optimization
How do I know my AV is working?

http://www.eicar.org/85-0-Download.html
What’s the most comprehensive way to scan a file?

https://www.virustotal.com
Never bank from an untrusted network

Yeah, right...
How do I defend against zero day attacks?

• A lot of the vulnerabilities are based on the same types weaknesses.

• Microsoft EMET can mitigate some vulnerabilities before patches are out!
Certificate Validation
Certificate Validation

App Talks to Evil Server

Cert Store

Cert Auth

Cert Auth

Evil Cert Auth

Cert Auth
Pinning – How does it work?
Pinning for end users - EMET
Advanced Security Tips for End Users

Thank You!