

# 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>

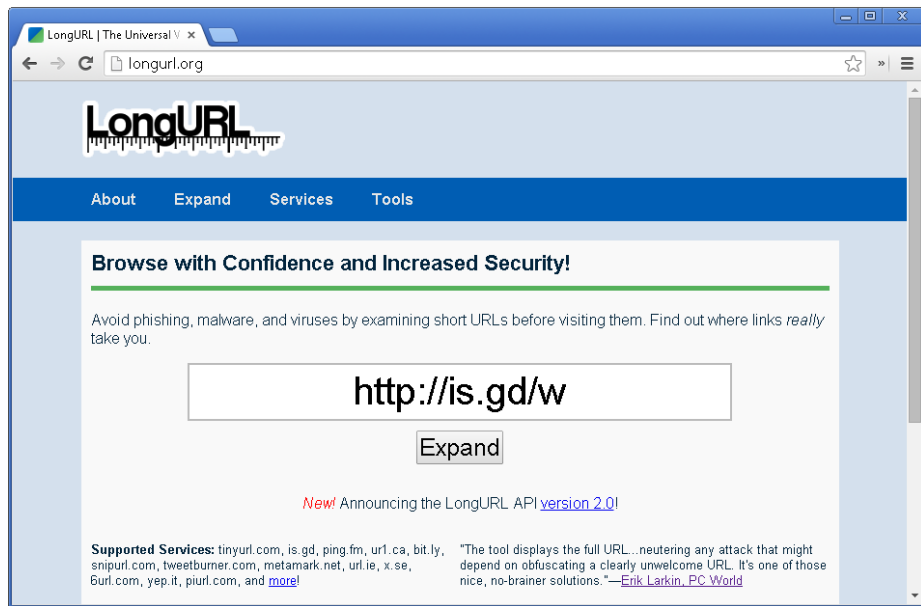
<http://tinyurl.com/jvuhogy>

<http://www.google.com/search?hl=en&q=Digital+Insight+Innovation+Conference&btnI=>

<http://d%49%49%6E%6E%6Fvat%49%6F%6E%63%6F%6E%63e.%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/>

The screenshot shows the Norton Safe Web interface. At the top, it says "Report for piratebay.com" and "safeweb.norton.com/report/show?url=piratebay.com". The main heading is "Safe Web Report for: piratebay.com". Below this, it says "Web Site Location: United Kingdom". There is a "Norton Rating" section with a large green "OK" and "SAFE" label, stating "Norton Safe Web has analyzed piratebay.com for safety and security problems." and "Norton Safe Web found no issues with this site." A "Summary" section lists "Total threats on this site: 0" and "The Norton rating is a result of Symantec's automated analysis system." A "Community Rating" section shows a bar chart with a rating of 1.8 "rated by 13 users". There is also a "Look up a site. Get our rating." search bar and a "Norton Safe Search" bar.

## McAfee Threat Intelligence

<http://www.trustedsource.org/>

The screenshot shows the McAfee Threat Intelligence interface. At the top, it says "piratebay.com - Domain" and "www.mcafee.com/threat-intelligence/domain/default.aspx?domain=piratebay.com". The main heading is "piratebay.com". Below this, it says "This page shows details and results of our analysis on the domain piratebay.com". There is a "Web Reputation" section with a vertical bar chart showing "High Risk", "Medium Risk", "Unverified", and "Minimal Risk". A "Threat Detail" section shows "Web Category: Illegal Software", "Activation: Last Seen: 2014-07-24". There is a "Next Steps" section with links: "Search Again", "View All Threats", "Sign Up McAfee Labs Security Advisory", and "Dispute a URL or Classification". An "Overview" section shows "Associated IP Addresses" and "Online Affiliations". A "DNS Servers for this Domain" section shows "No results found".

# Use a secure password

Have I been affected  
by a breach?

How secure is my  
password?

How can I keep my  
password safe?

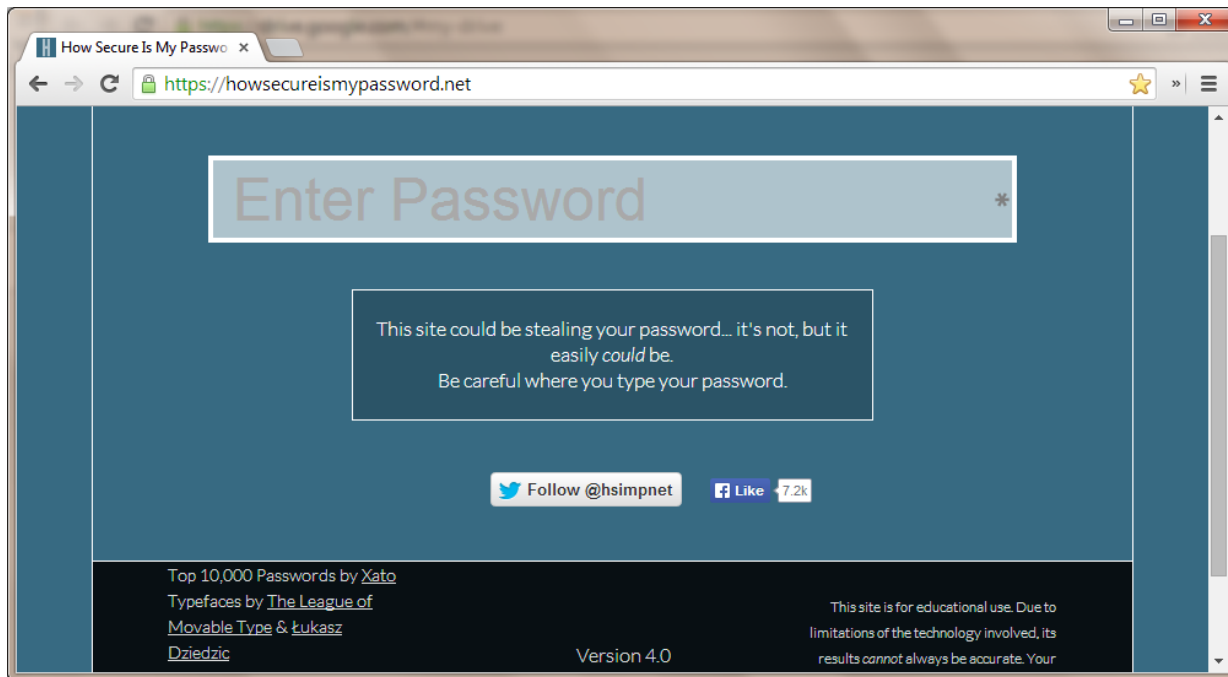


# Adopt MFA!

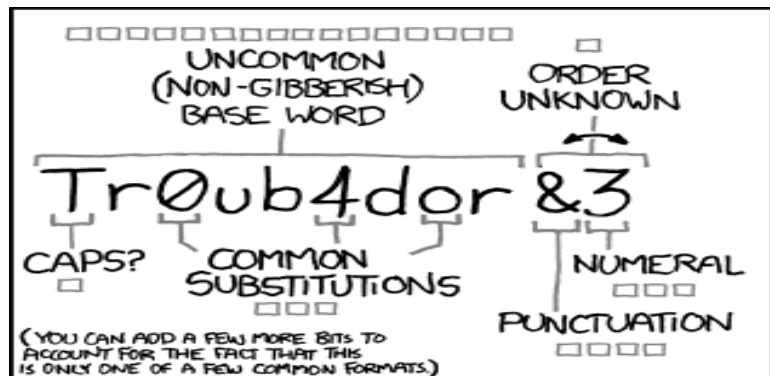
- Google
- Facebook
- LinkedIn
- ...

# How secure is my password?

<https://howsecureismypassword.net/>



# Complex vs. Long Passwords?



~28 BITS OF ENTROPY

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

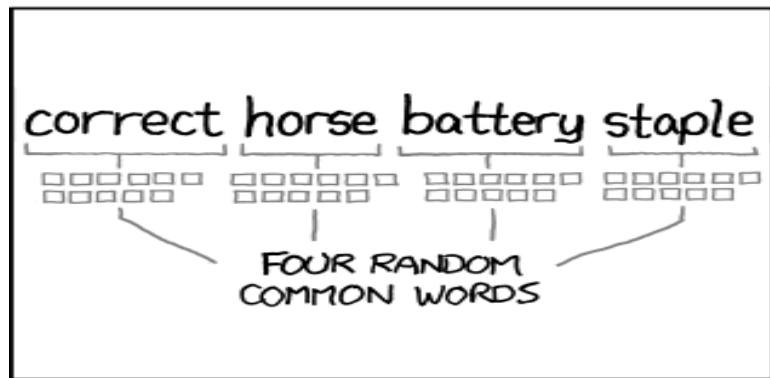
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: **EASY**

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER: **HARD**



~44 BITS OF ENTROPY

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS: **HARD**

THAT'S A BATTERY STAPLE.

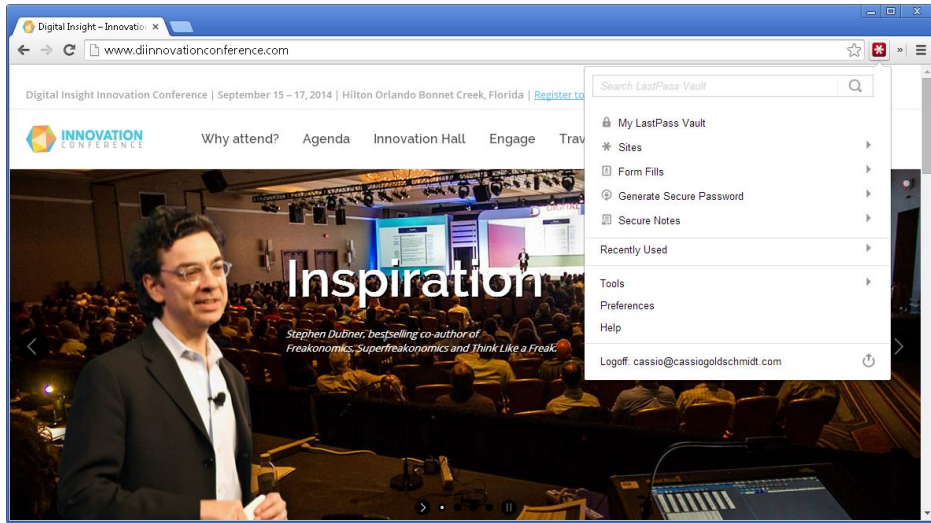
CORRECT!

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

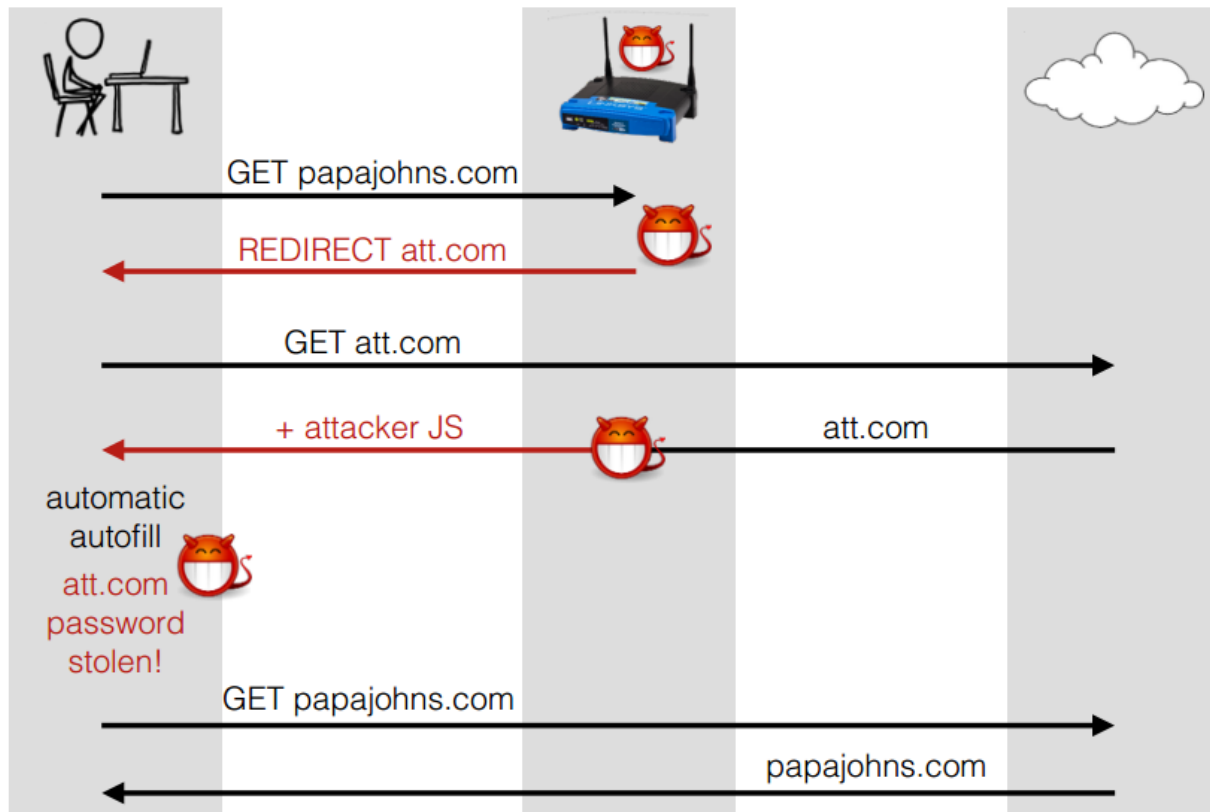


Norton  
IdentitySafe 2014

# 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).

# Redirect Sweep Attack on HTTP Login Page





# Disable Autofill...

## Vulnerable

**Automatic**



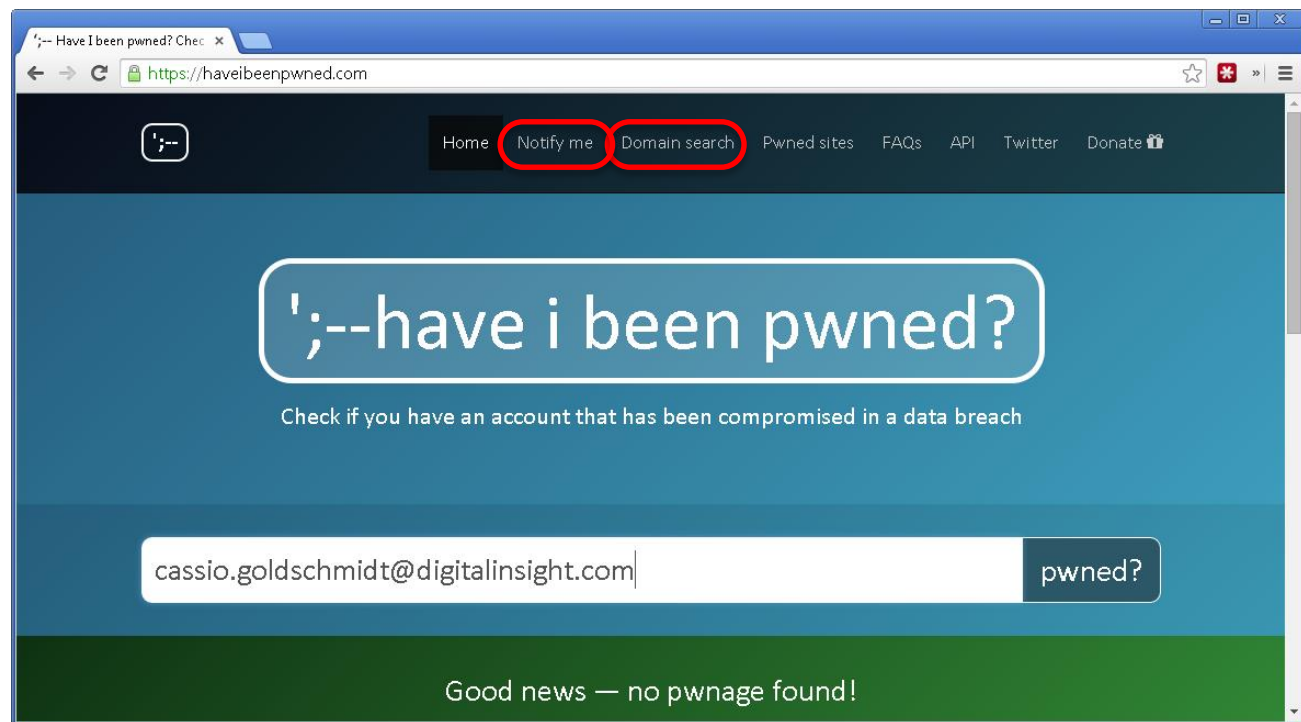
## Not Vulnerable

**Manual**



# How to find out if my password or my user's accounts have been breached?

<https://haveibeenpwned.com>



# Use an Antivirus

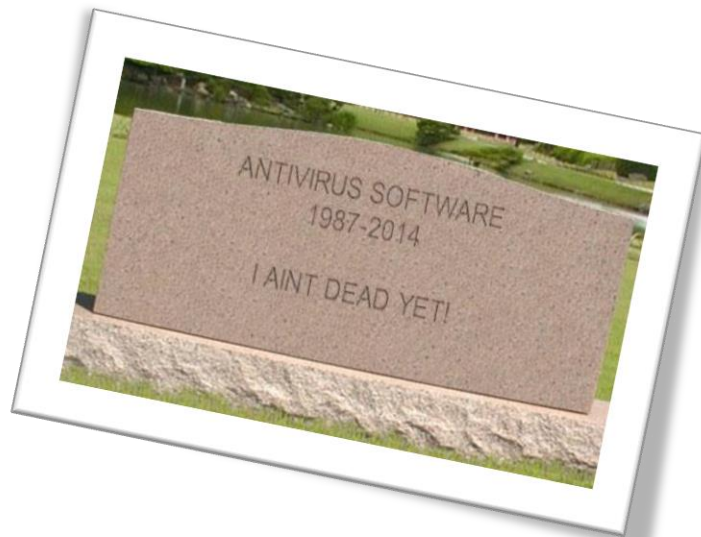
How do I know my AV is working?

Do I still need AV?

The AV says the file is okay... Can I get a "second opinion"?

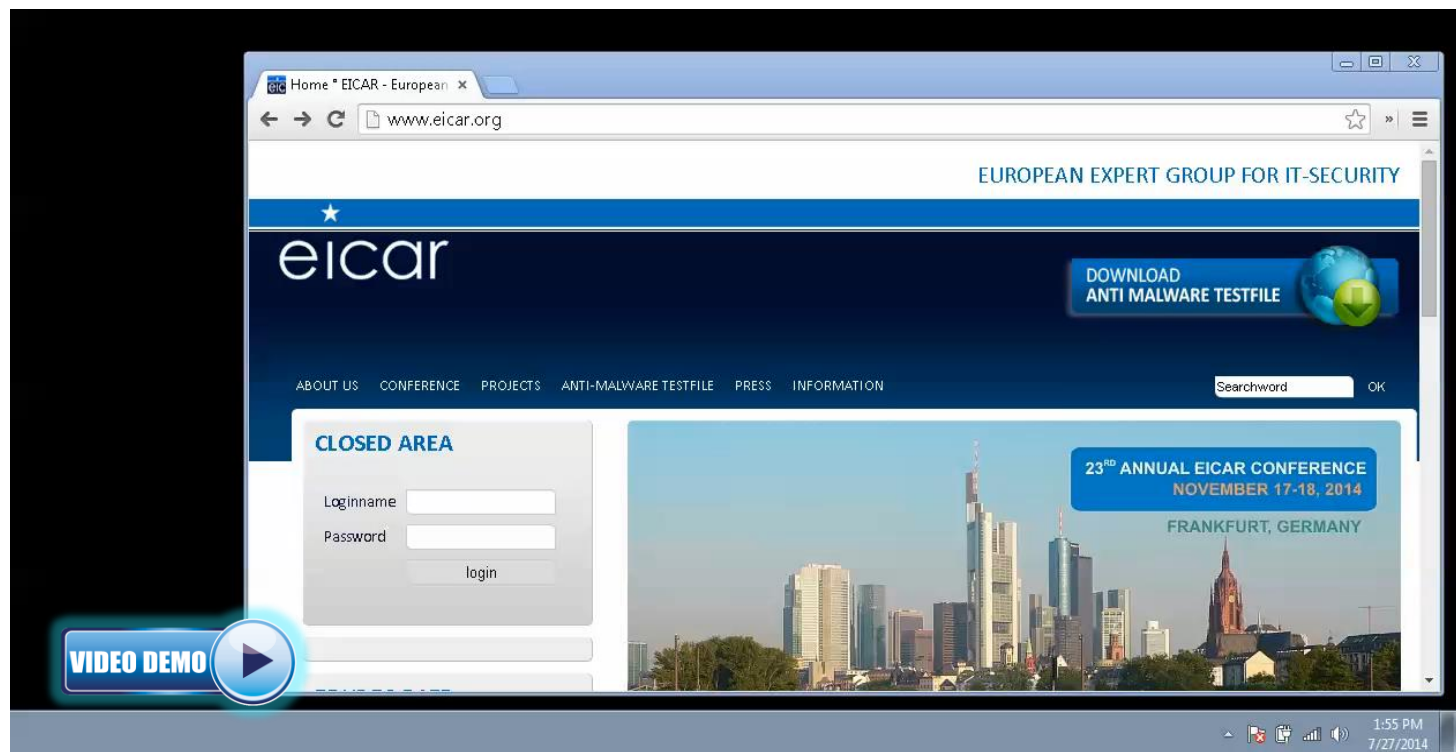
# Is Antivirus still relevant?

- **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



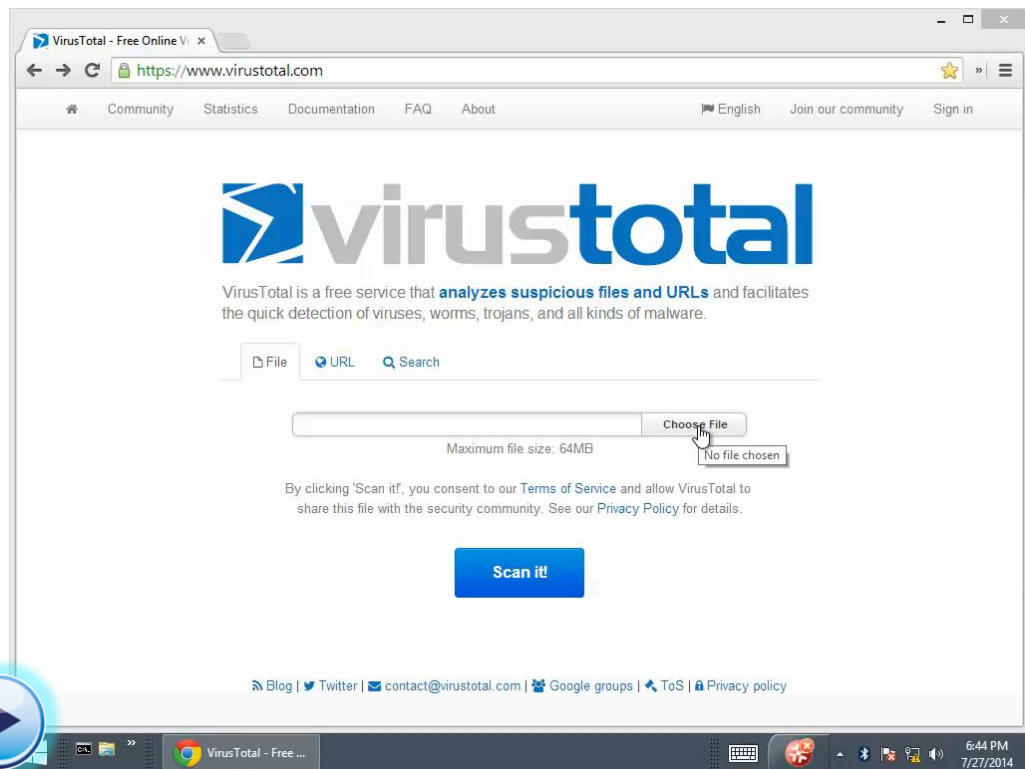
# How do I know my AV is working?

<http://www.eicar.org/85-0-Download.html>



# What's the most comprehensive way to scan a file?

<https://www.virustotal.com>



VIDEO DEMO

# Never bank from an untrusted network

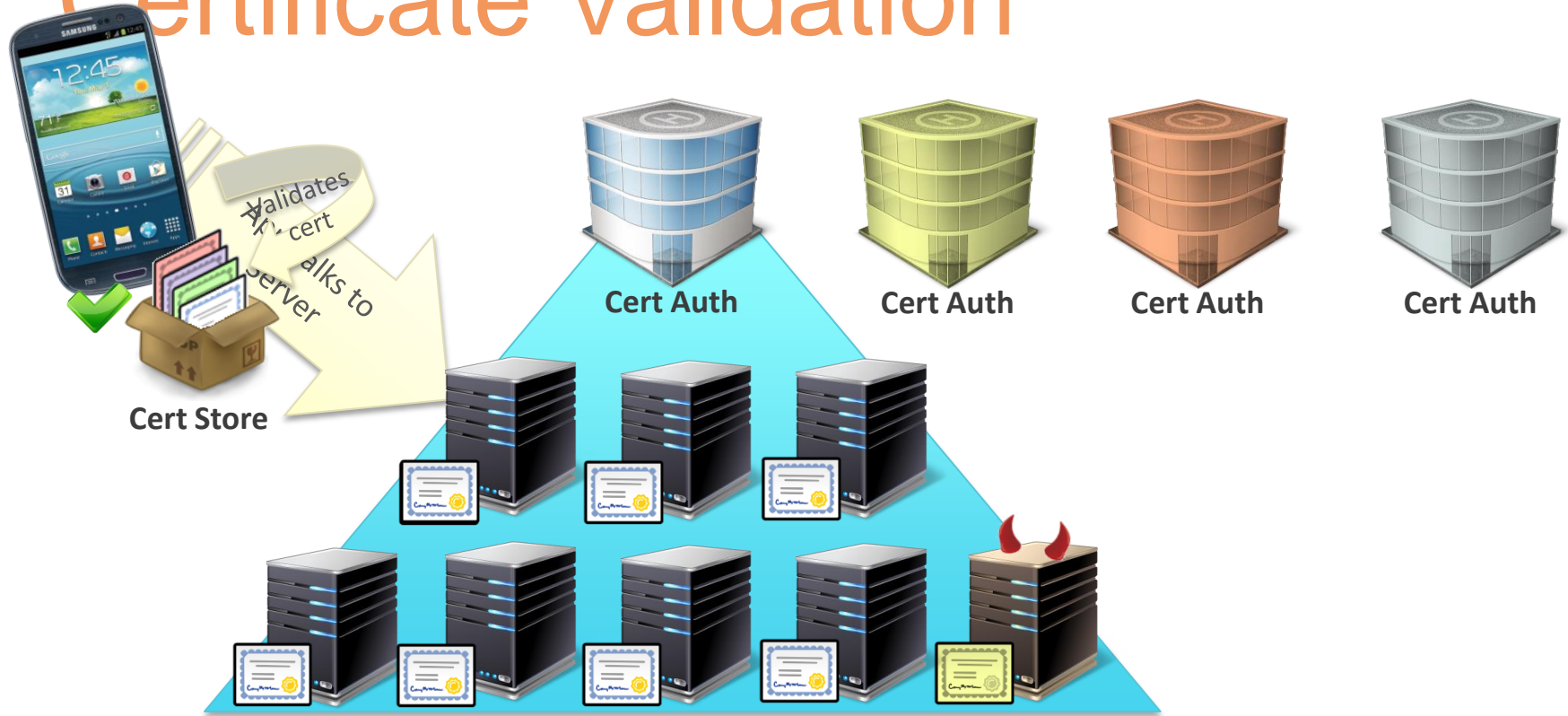
Yeah, right...



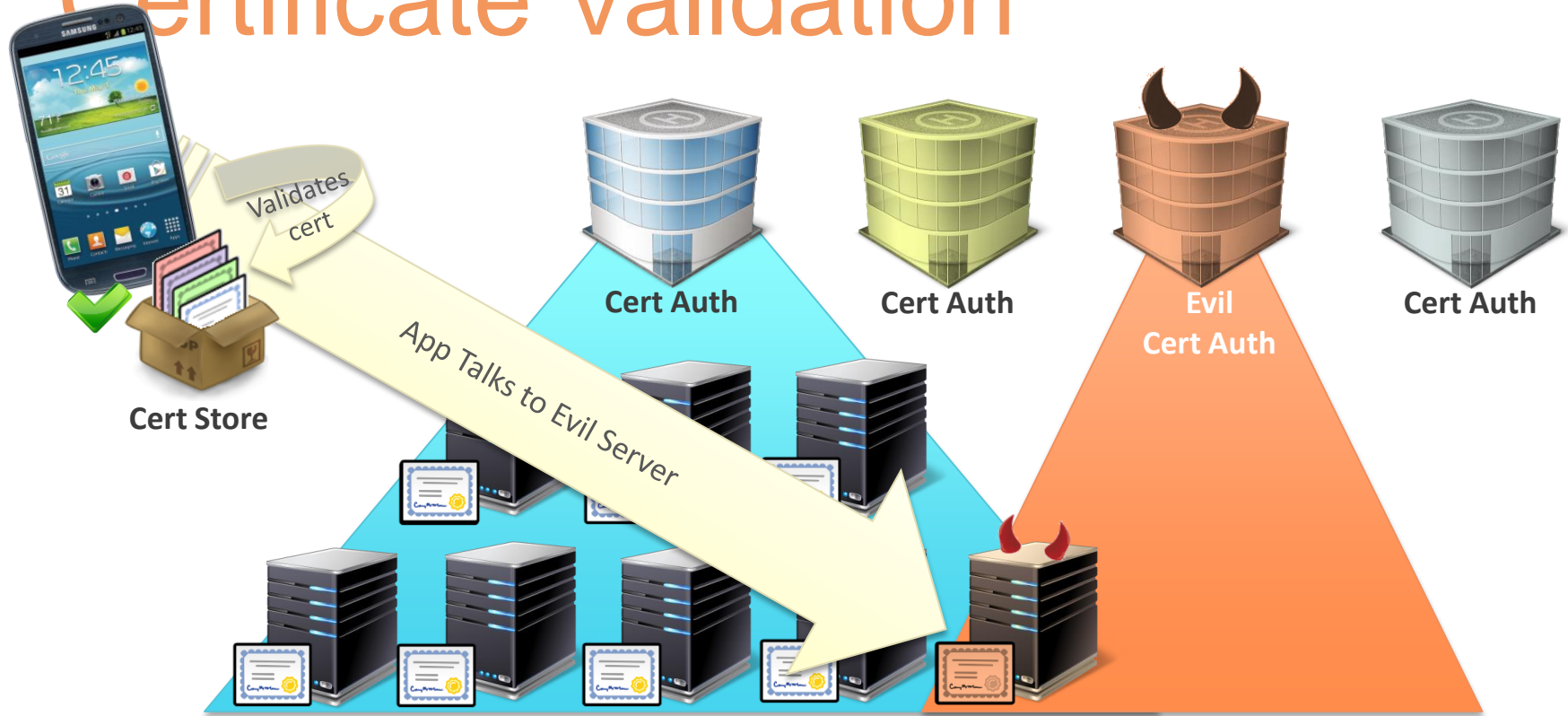
# How do I defend against zero day attacks?

- A lot of the vulnerabilities are based on the same types weaknesses.
- Microsoft EMET can mitigate some vulnerabilities before patches are out!

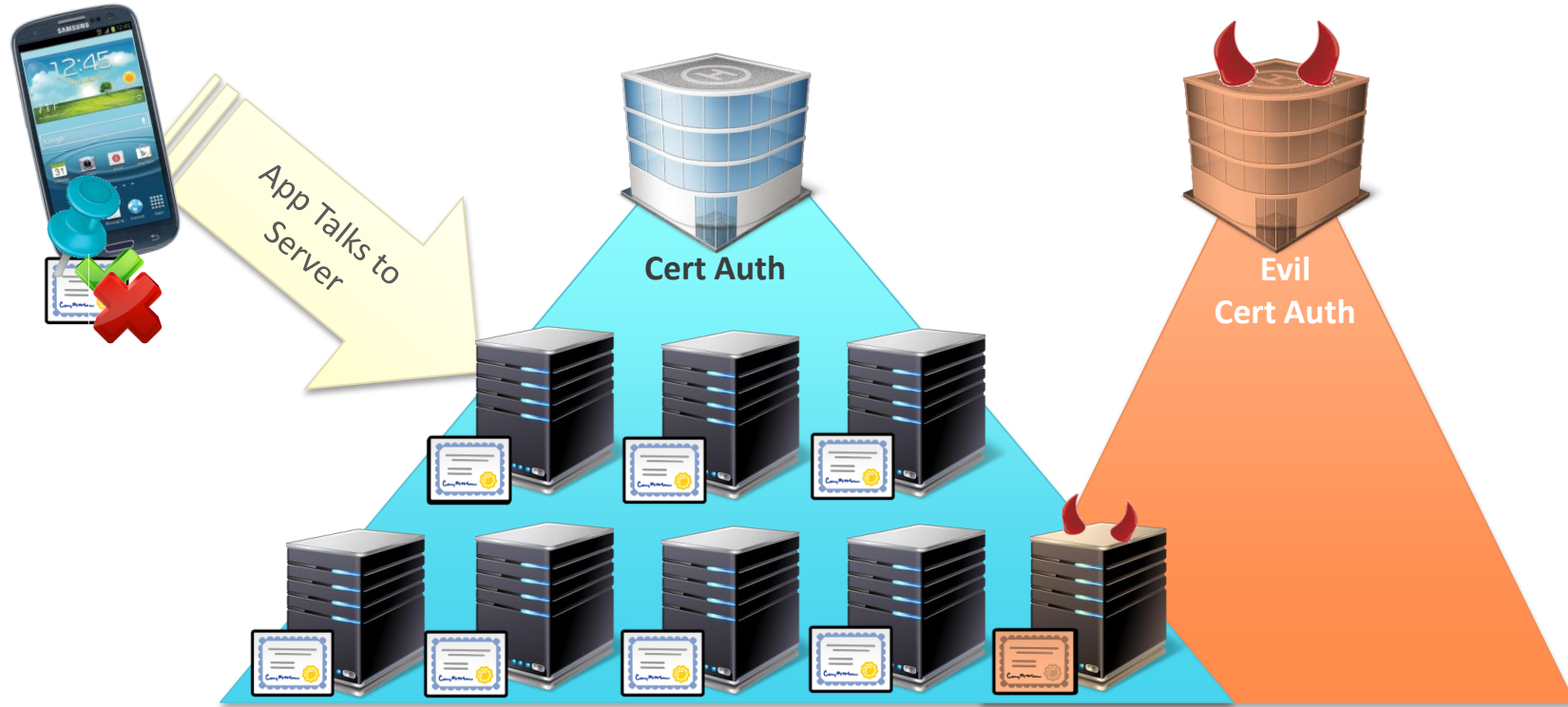
# Certificate Validation



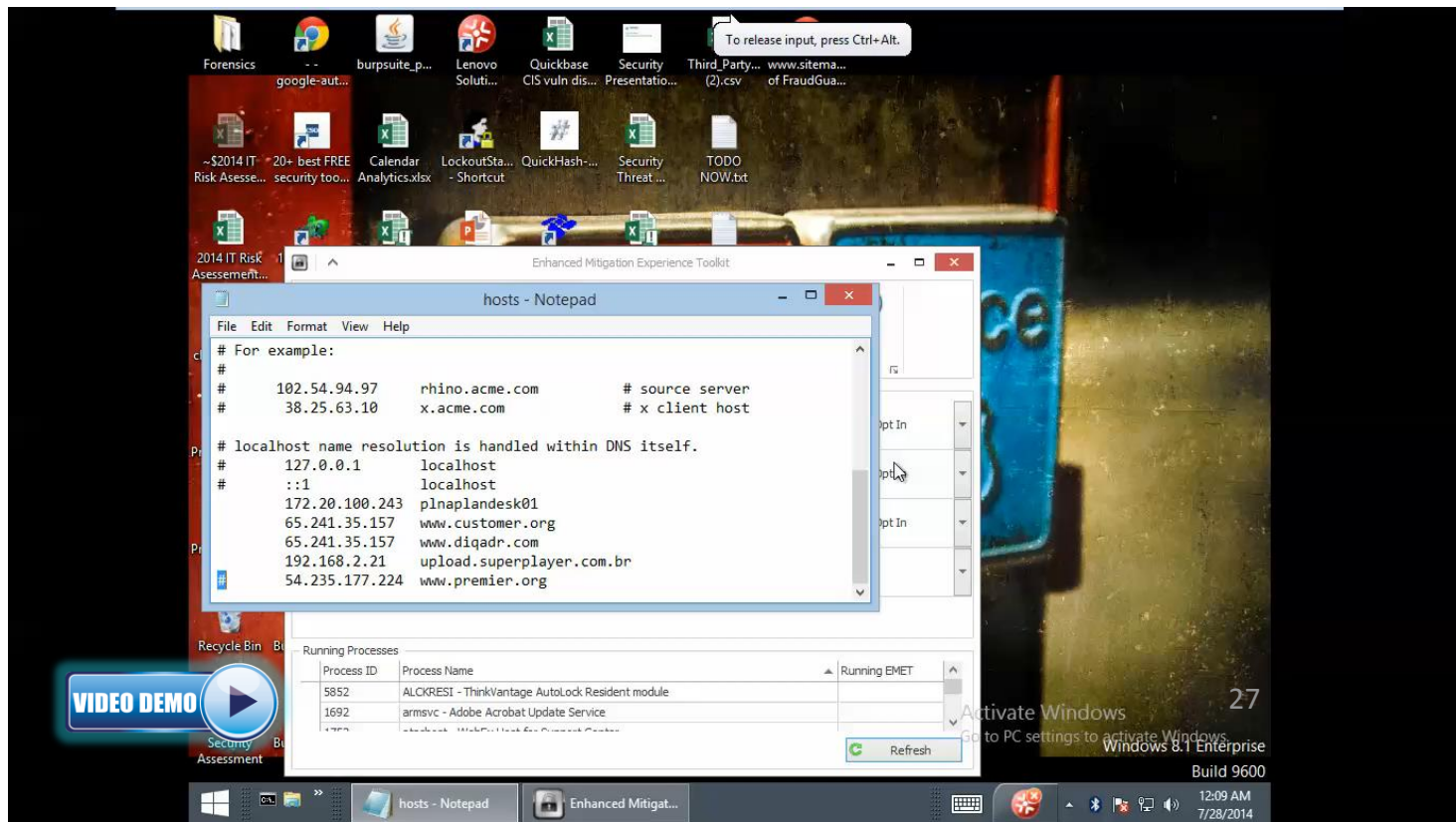
# Certificate Validation



# Pinning – How does it work?



# Pinning for end users - EMET



Advanced Security Tips for End Users

**Thank You!**

