Internet & Web Security, the Evolutionary Model

Avi Avivi
VP, Technology Area Manager
Enterprise Information Security - Architecture

Stanford University

10/9/14

Together we'll go far

Evolution of the security landscape

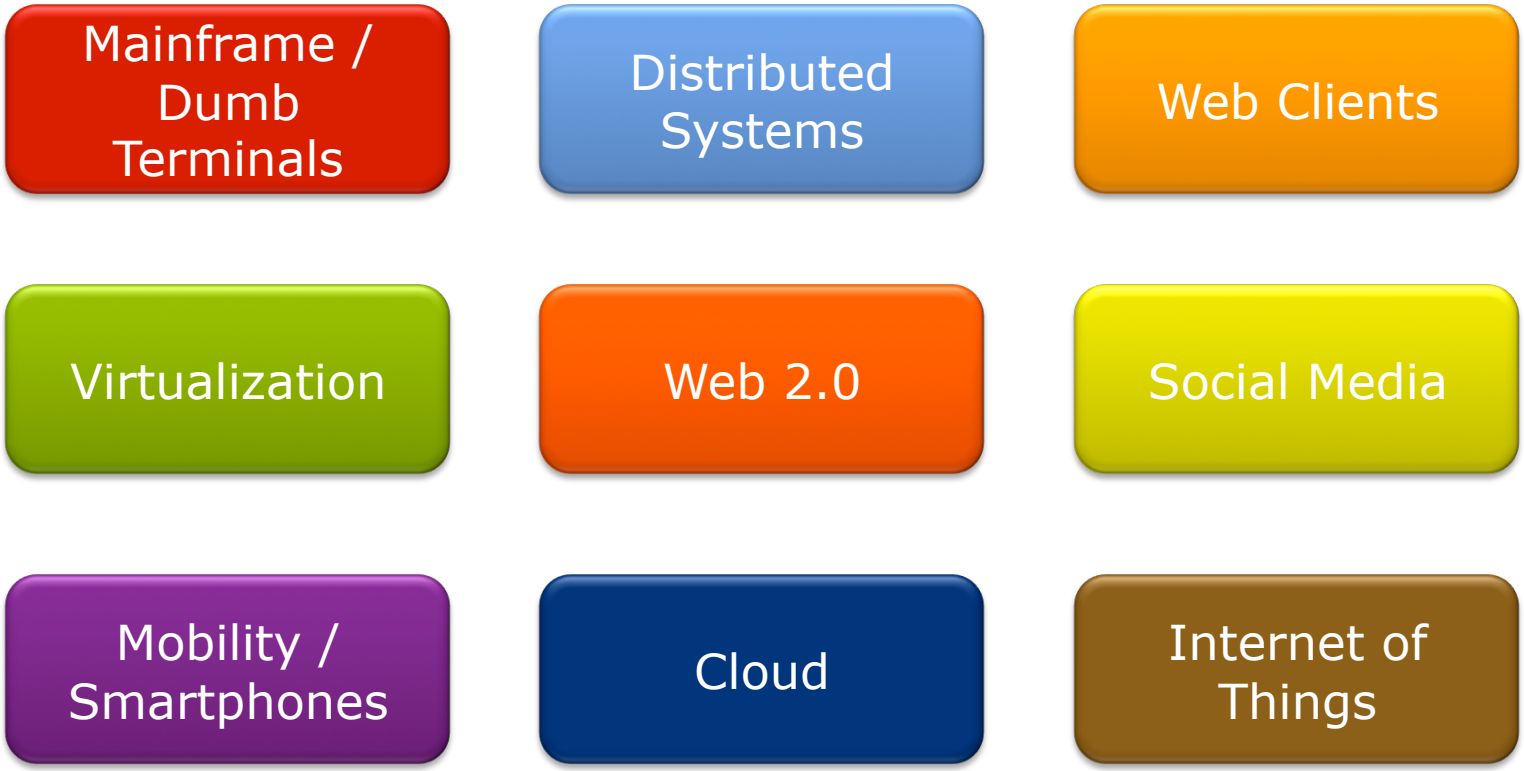
- Information Assets
- Cyber Adversaries and Motivators
- Cyber Attacks
- Defense Mechanisms
- The Arms Race
- Public Service Announcements

Information Assets

What are the adversaries after?

Information is the Asset

Moving the data (and the risk) closer to the end user

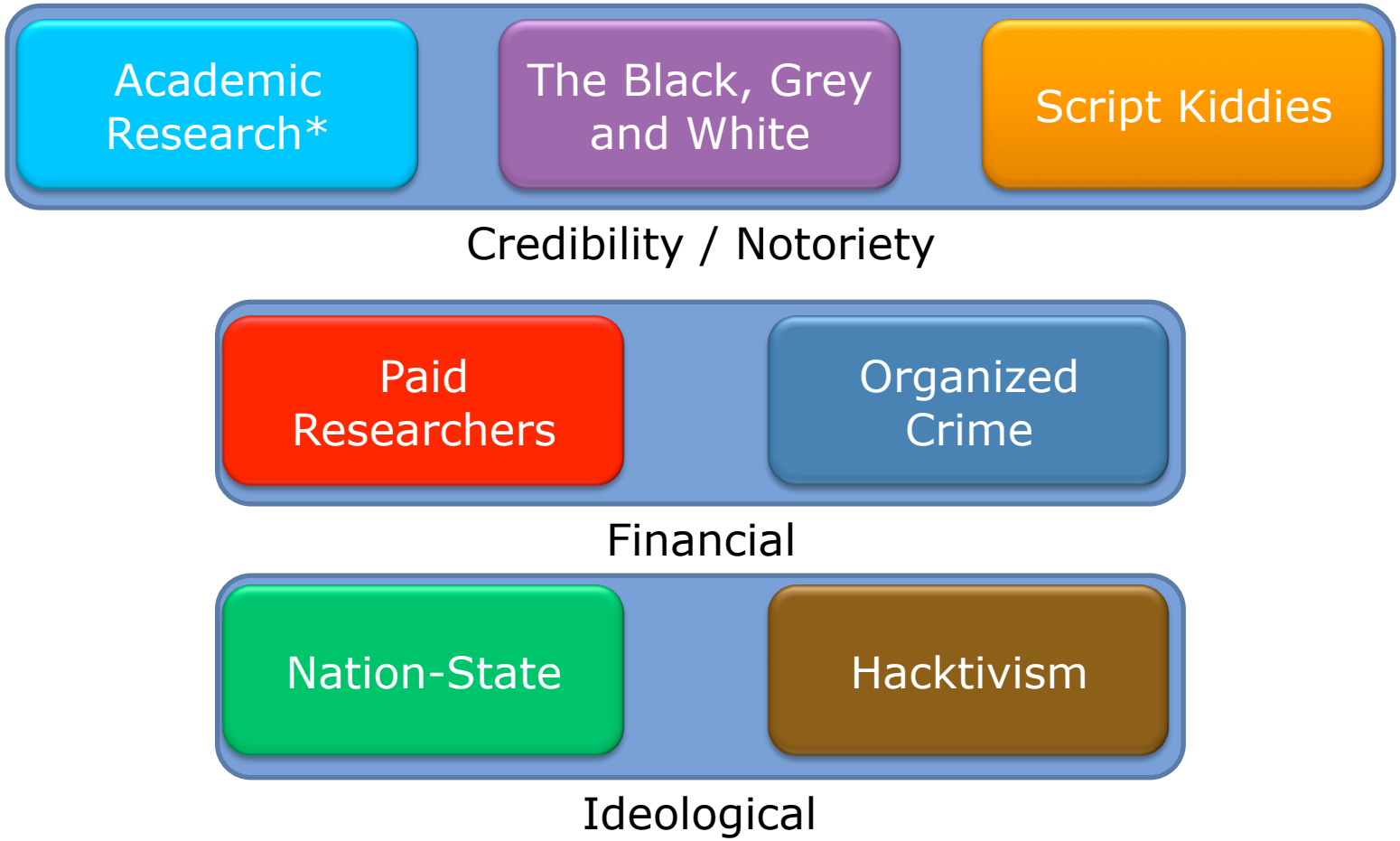


Cyber Adversaries

The Villains?

Cyber Adversaries

Motivations and bad guys evolve too



"The heroes have to win every time. The villain only has to win once."

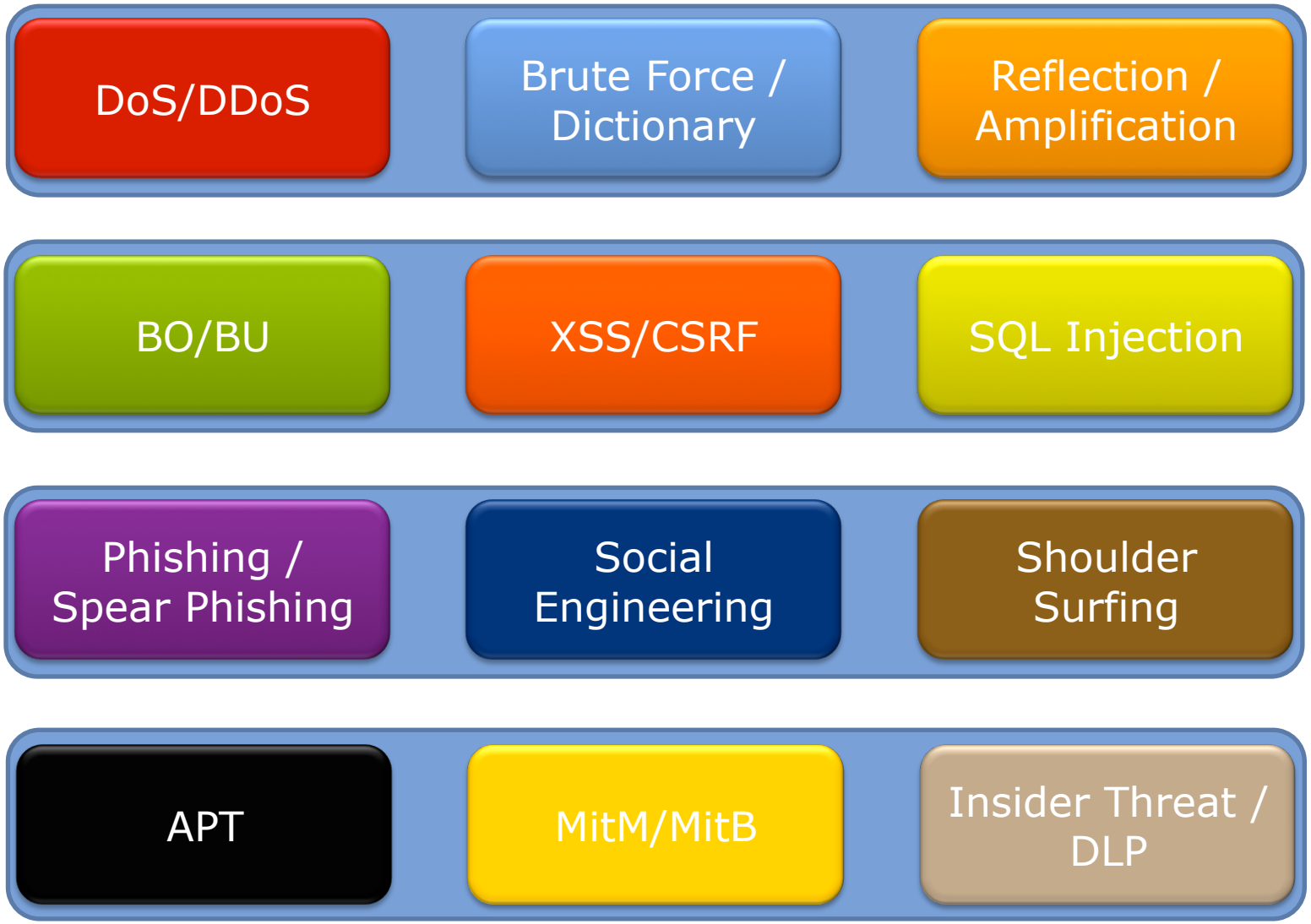
– Dan DiDio, Sr. VP, DC Comics
DC Villain Month

Cyber Attacks

What do they do?

Cyber Attacks

Land of the acronyms and ominous terminology



An attack I wouldn't mind see working…

Defense Mechanisms

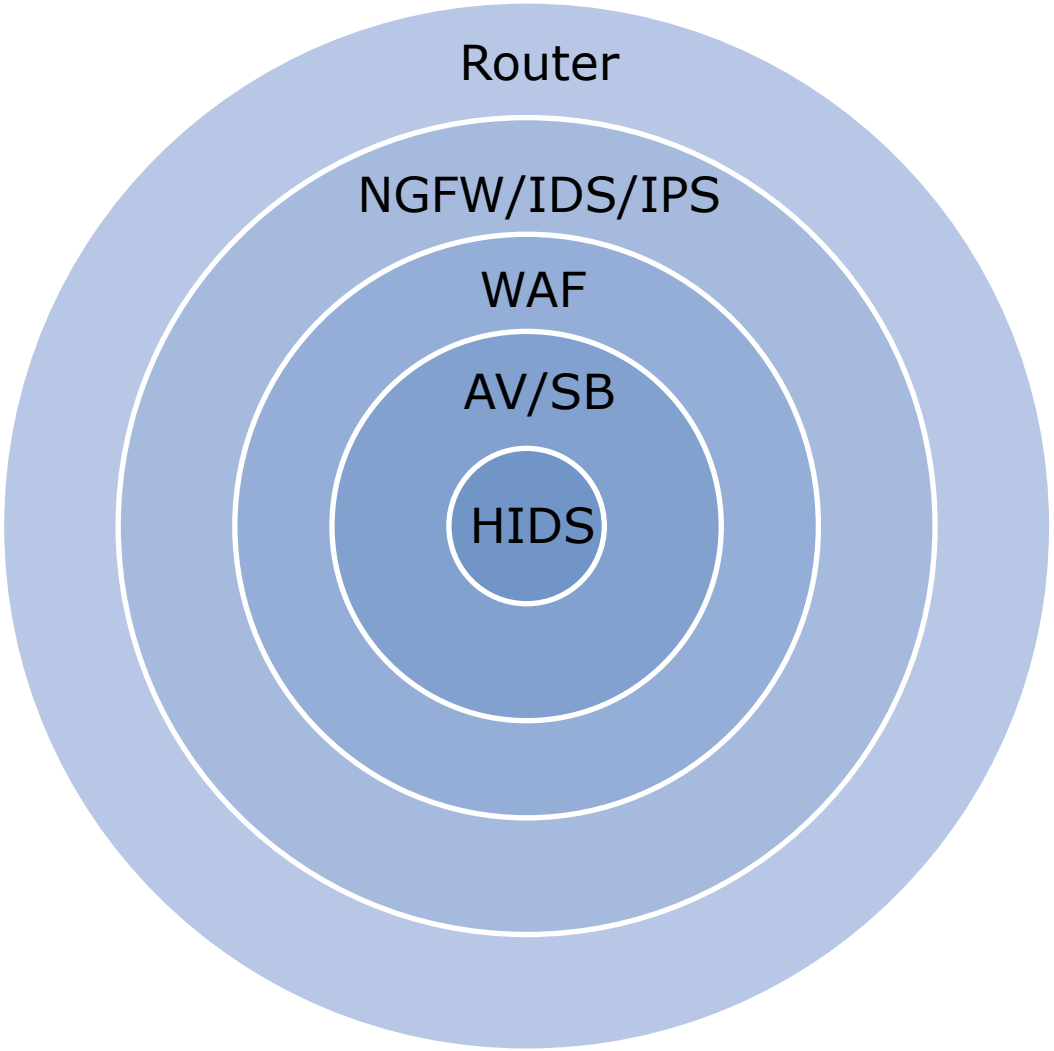
Avoid being the Target (Pun intended)

"All models are wrong, but some models are useful ."

– George E. P. Box

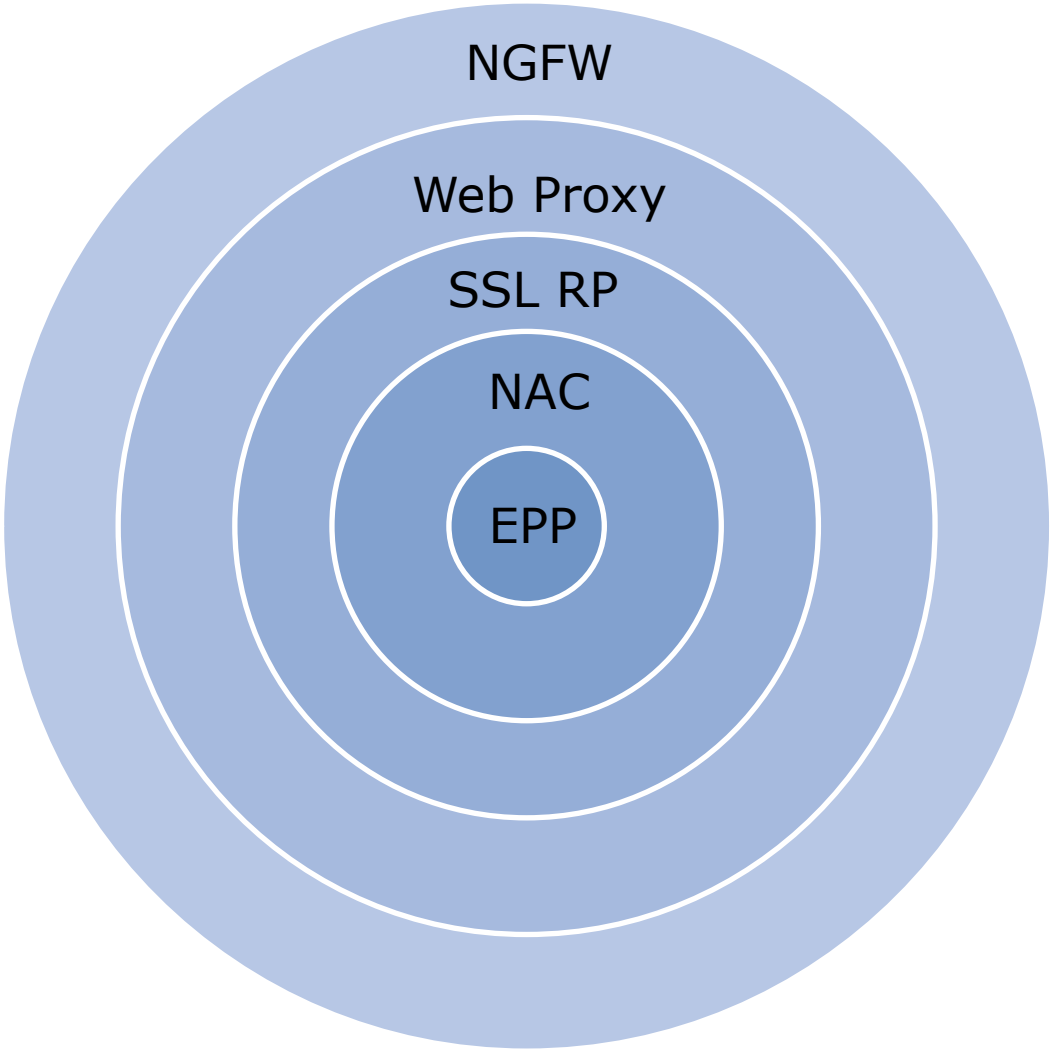
Ingress Defense

Traffic direction matters!



Egress Defense

Attacks can manifest on the outbound



The Overlay: Intelligence

Putting it all together and making sense of it

- Smart Logging
- SIEM
- Log Analysis (Big Data)
- Automated tools / Remediation
- Threat Feeds

The Big Data Challenge

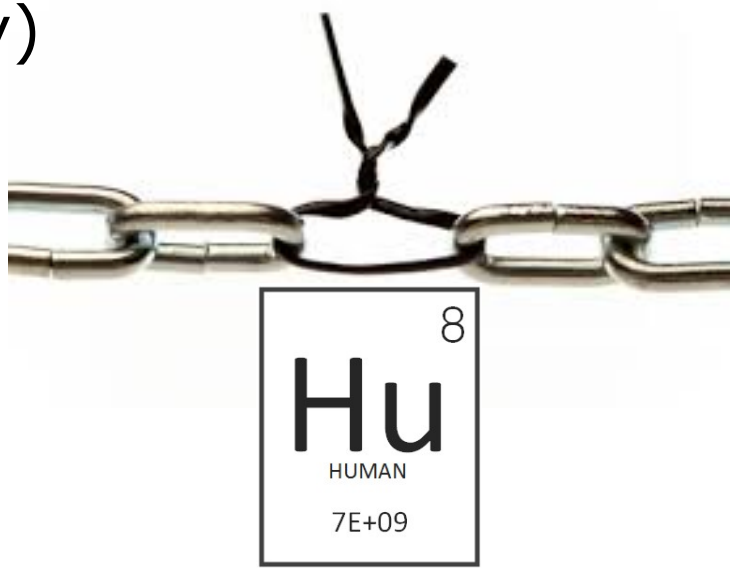
Some numbers to think about

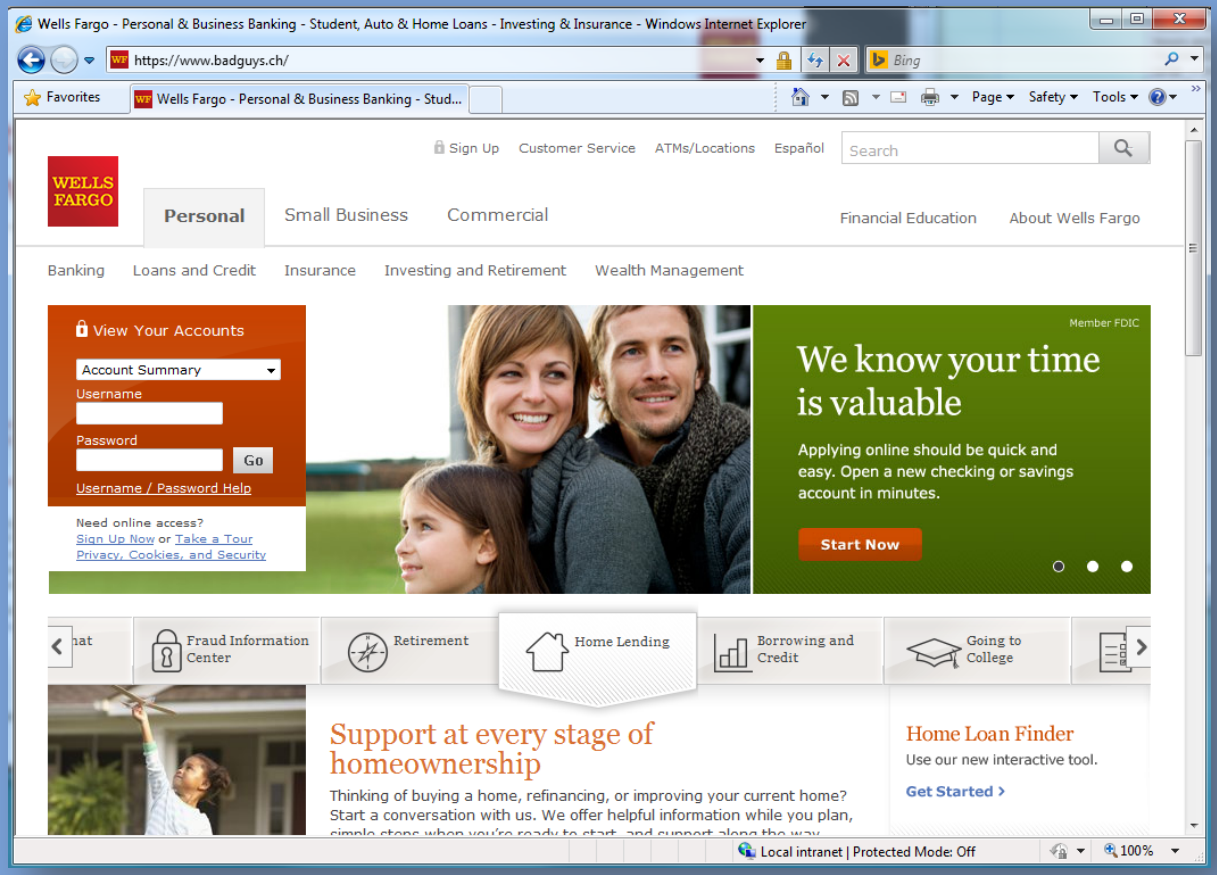
- Wells Fargo has almost 300,000 Team members
- Our CIO has over 24,000 reports
- We operate over 80 different lines of business
- More than 10,000 locations
- Hundreds of web 'properties'
- Hundreds of web-facing applications
- Over 50 active Information Security initiatives
- Just 30 days of compressed web-proxy logs from 47 proxies @ 5 datacenters = ~1TB of data
- How much data do you retain? For how long?

Other Defenses

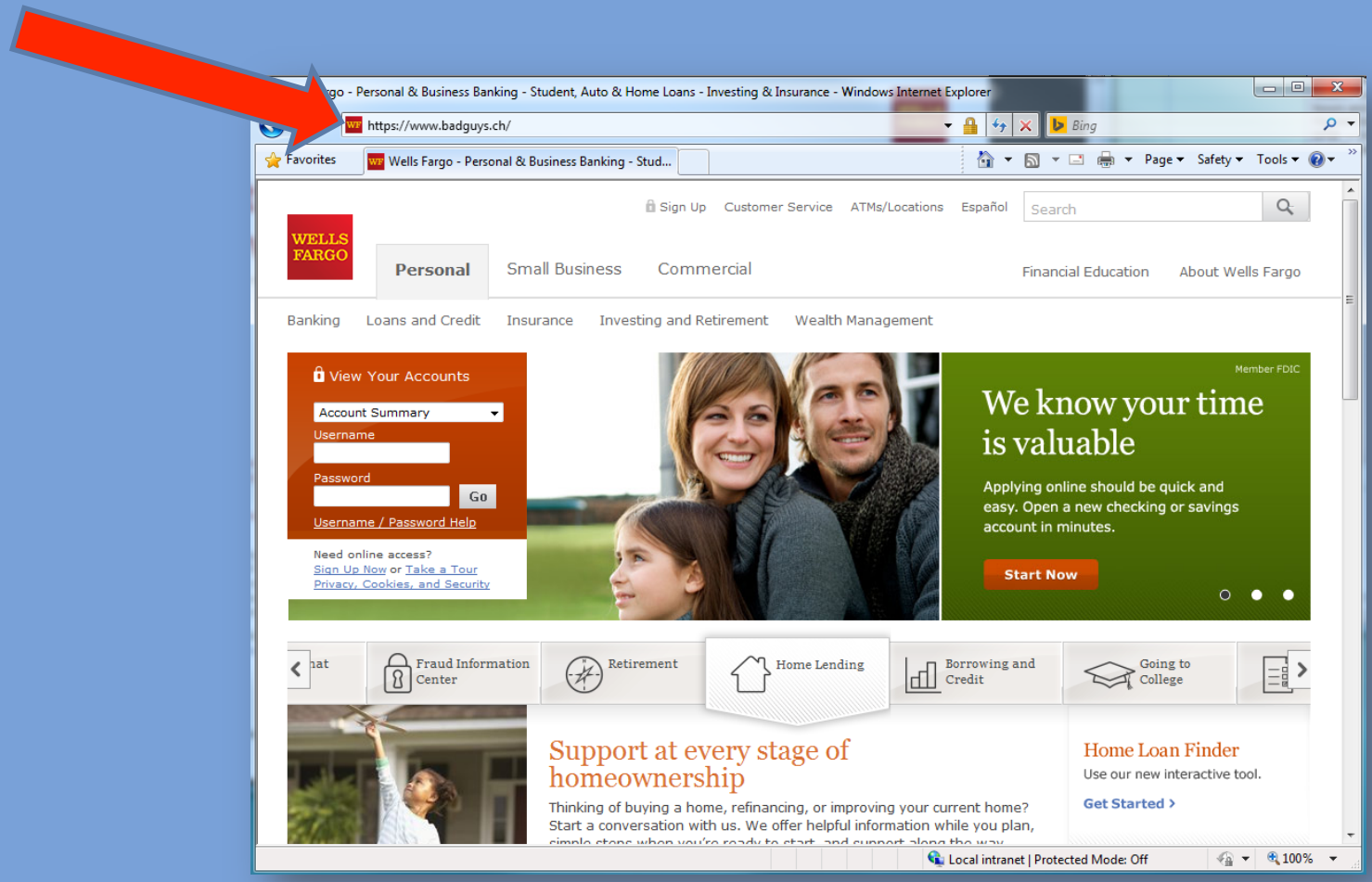
Remember that the weakest link is mostly the human element

- Awareness
- Secure Coding Classes for Programmers
- SDLC (or S-SDLC)
- Static and Dynamic Code/Application Scanning
- Penetration Testing (In-house and 3rd Party)





What's wrong with this picture?



Nothing other than it's not a real

Wells Fargo site...

The Arms Race

Good News! It's called – "**Job Security**"

Continuous Cycle

New Defenses Bring on New Attacks

Public Service Announcements

Please share with your family and friends.

Nothing is Free

Everything Comes With a Price

- Beware the free/found USB
- Free offers in the email are almost always meant to harvest your email address
- If you didn’t sign up for it – most email coupons are simply overt phishing attempts
- Rather than clicking a link automatically, hover over it, right click to see where it is really trying to send you

Treat email With Extra Care

Just Because You're Paranoid – It Does not Mean They're not Trying to Get You

- Treat emails from your bank, credit-card company, eBay, PayPal, etc. as highly suspicious.
- If they tell you, you need to log-in to your account – don't click the link in the email, open a browser and go to the website yourself
- Some of the above companies will try to include just enough personal/account information to convince you they're legitimate – ignore it
- Don't volunteer any information you care about on social media

General Advice

Suggestions for a Safer Digital Life

- When possible, opt for 2-factor authentication
- Traditional passwords may be dying. Until they do, choose them wisely, and rotate them
- Seek to educate yourself, don't give in to breach-fatigue (Washington Post)
- Patch your computer, smartphones and tablets
- Personal preferences:
  - Avoid free-standing ATMs
  - Subscribe to credit/identity monitoring services
  - Make sure your friends/followers are just that
  - Check gas-station/vending machine card slots for signs of tampering

Questions?