Information Security & the Modern User

- Defenses Against Security Breaches

University of Louisville

CIS Department

Prepared by Brian Martinez

Edited by: Nate Stopinski

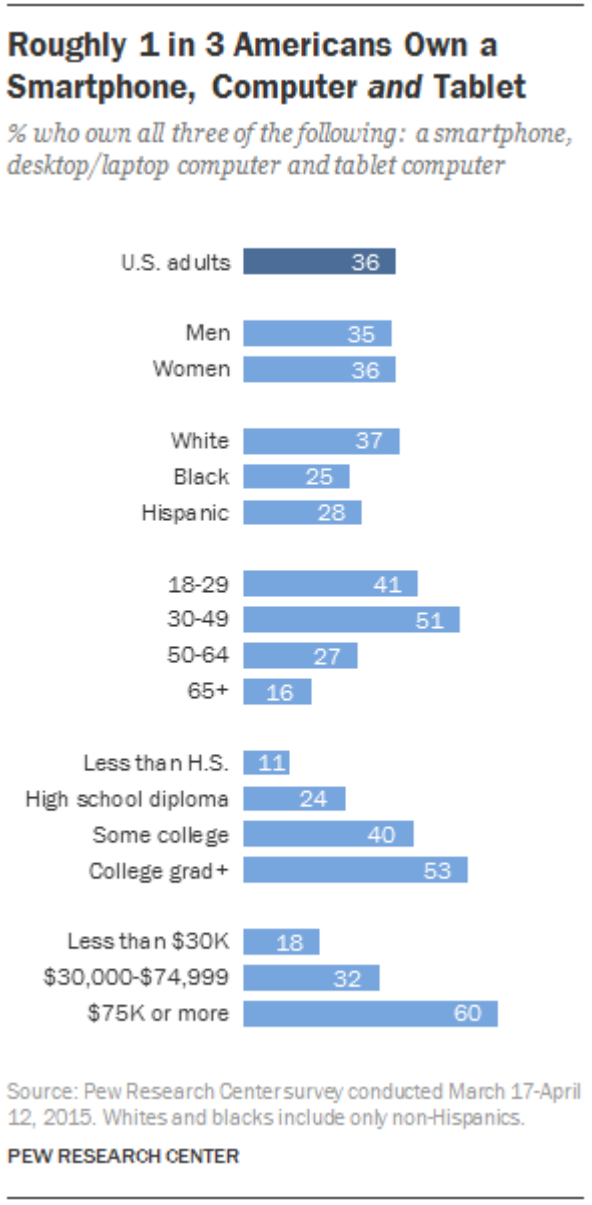
THE ELECTRONIC ENVIRONMENT

- Computers
- Laptops
- Tablets and Phones
- The Internet

HOW MANY PEOPLE OWN MORE THAN ONE ELECTRONIC/DIGITAL DEVICE?

- As of 2015, 1 in 3 Americans owned a Smartphone, Tablet, and Computer!

- 1 in 4 Americans own a gaming console/device



Source: http://www.pewresearch.org/fact-tank/2015/11/25/device-ownership/

The Connected World

- Population of Earth (2015):
  - 7.2 billion
- Number of personal computers (2015):
  - 2 billion estimated
- Number of mobile devices (GSMA 2017):
  - 8.114 billion mobile connections

Source: https://www.reference.com/technology/many-computers-world-e2e980daa5e128d0

Hacking and Security Breaches

- Earliest hack:
  - 1903: Nevil Maskelyne sends insulting Morse code messages with projector and disrupts wireless telegraphy demonstration by John Ambrose Fleming
- Most recent security breach:
  - River City Media backup servers not password protected, exposing 1.37 billion record spam database. Includes names, zip codes and physical and IP addresses

WHAT ARE SOME MISTAKES YOU MAKE ONLINE?

- Using the same password on multiple sites
- Putting too much personal information on websites (FaceBook, Twitter, etc)
- Being unaware of cyber threats (automatic downloads, viruses, etc)
- Scams/Social Engineering through Social Media

Common User Misconceptions and Mistakes

- Don’t share login information with anyone
- Only open emails from familiar contacts
- No backups
- Not reading before clicking “yes” or “Next”
- Not verifying source of download
- Using the same or similar login information to multiple sites

WHY SHOULD YOU CARE?

- Protect your identity
- Protect your data and privacy
- Protect yourself from scams and social engineering

IMPORTANT THINGS TO WORRY ABOUT

- Personal Information
- Protect yourself from Identity Theft
- Changing passwords regularly
- Keep your devices up to date regularly
- Don’t share any login information with anyone
- Avoid “sticky notes” with passwords on them with a Windows PC

HOW TO TELL YOU'RE COMPROMISED

- Slow/Sluggish performance
- Strange/new errors
- Changes being made without permission
- Files being changed, moved, deleted without permission
- Unknown programs or services running in the background
- Unauthorized activity on system or across network
- Strange, unfamiliar emails being sent to or from you or your contacts

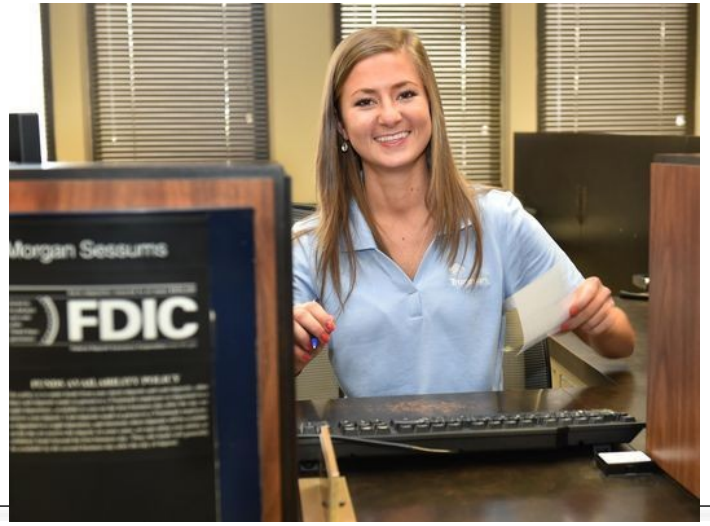
Threats and Vulnerabilities

Threats

- Person or event with potential for impacting a resource in a negative manner
  - Example: Bank robber

Vulnerabilities

- Quality of a resource or environment that allows a threat to be realized
  - Example: Bank teller



Common Vulnerabilities

- Out of date operating system
- Out of date software
- Out of date antivirus definitions
- No scheduled backups
- Inactive or incorrectly configured firewall

Common Threats

- Malware
- Spyware
- Viruses
- DoS and DDoS
- Social engineering
- Phishing
- Pharming
- Ransomware
- Spam
- Spoofing
- Worms
- Botnet
- Trojan horse

Bulletproof Glass

- Update Operating System regularly
  - Check software and hardware manufacturers websites for updates if automating isn't possible
- Install Antivirus software and update regularly
  - Automate antivirus scans
- Install firewall and configure to legitimate traffic
  - Configure firewall after installing new software
- Filter emails
  - Proofread emails for strange grammar, spelling mistakes, formatting, etc as it may be a sign of a scam or spoof

Bulletproof Glass

- Check the URL of websites you visit, especially those that require a login and password
  - Spoofing sites, which masquerade as legitimate sites, maliciously collect your information
- Check the source of software you download
  - Spoof sites will also look like legitimate software sources and even buttons on legitimate sites are made to look like the intended button
- Scan recently downloaded software, files, and email attachments
  - Never open any downloaded programs or files without scanning first, especially email attachments from known contacts
- Install an anti-spyware program and keep updated
  - Spyware can be installed on your computer even visiting legitimate sites and clandestinely save and send your information to third parties

Bulletproof Glass

- Ignore or close ads and pop-ups
  - This is especially important with fraudulent pop-ups claiming an infection on a computer and to call the provided number.
  - Installing a pop-up blocker will reduce these incidents
- Unless the user has specialized knowledge to remove it, the fastest way around ransomware is to format and re-install from a back up or image file
- Update drivers for hardware including those for network devices like routers, network interface cards, and wireless interface cards

BEING PROACTIVE

- Monitor email and other accounts
- Credit monitoring
- Use 2 Factor Authentication when available
- Know the steps you need to take to recover in case your system is compromised
- Never give out more information than is absolutely necessary
- Implement the use of a password manager to keep track of unique logins and passwords

Any questions?