Cabrillo College

Personal Information Security Basics
Session 1: Hygiene for Your Digital Life
https://github.com/infosecirvin/pisb

Irvin Lemus
Cybersecurity Professor; Computer Information Systems Department
Bay Area Cyber Competitions Regional Coordinator

irlemus@cabrillo.edu (831) 479-6296
@infosecirvin

Topics for Today

Terminology and Activities

Online Safety

Securing the Home

Mobile Security

Tying it all together

All topics come from SANS OUCH! Newsletter

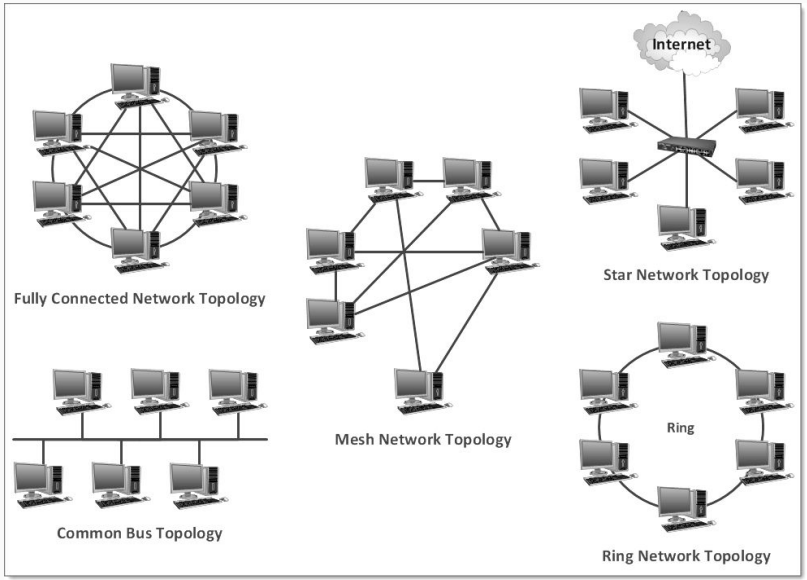
Terminology and Activities

Devices

- Any electronic system used to connect and access services

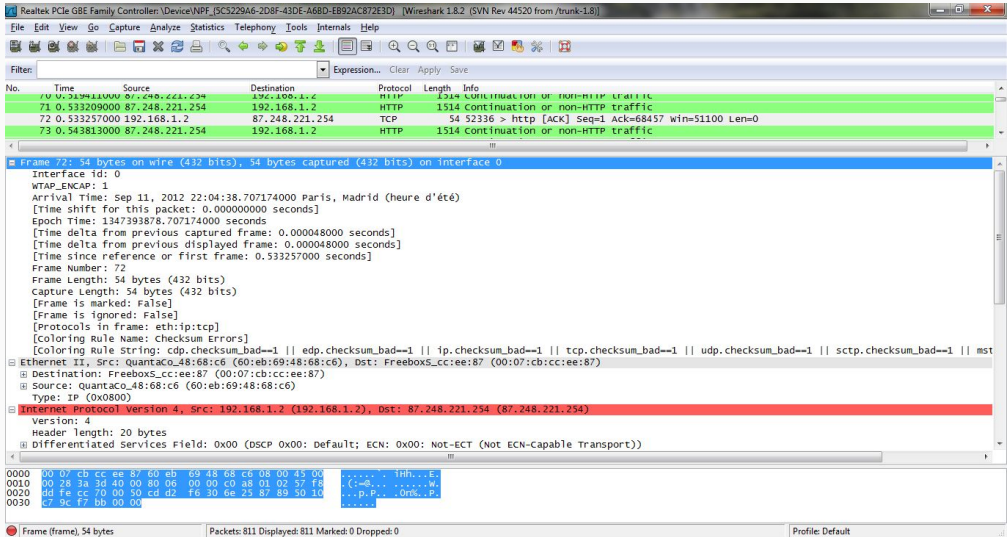
Network

- Devices connected via common medium
  - Wireless (Wi-Fi)
  - Wired
  - Cable (coax)
  - Fiber



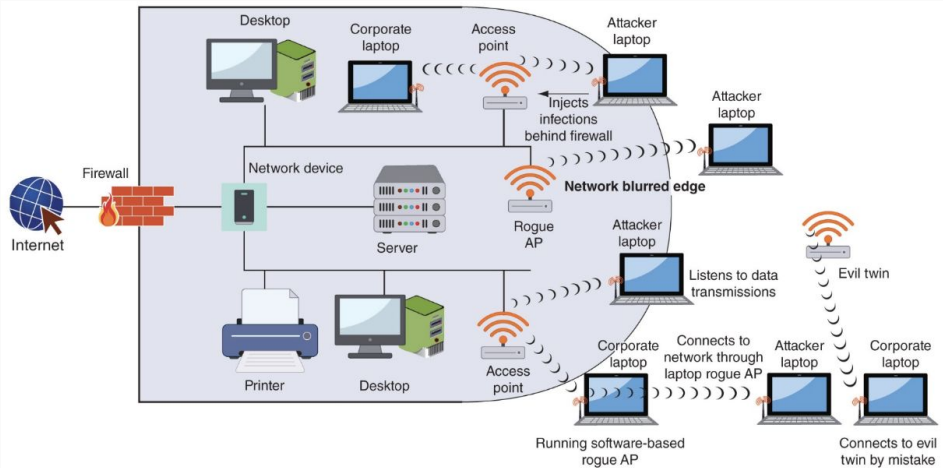
Wireshark Demonstration

1. Download and analyze trace files
   a. https://github.com/infosecirvin/pisb
2. Surf to unsecured website
3. Surf to secured website



Wireless Fidelity (Wi-Fi)

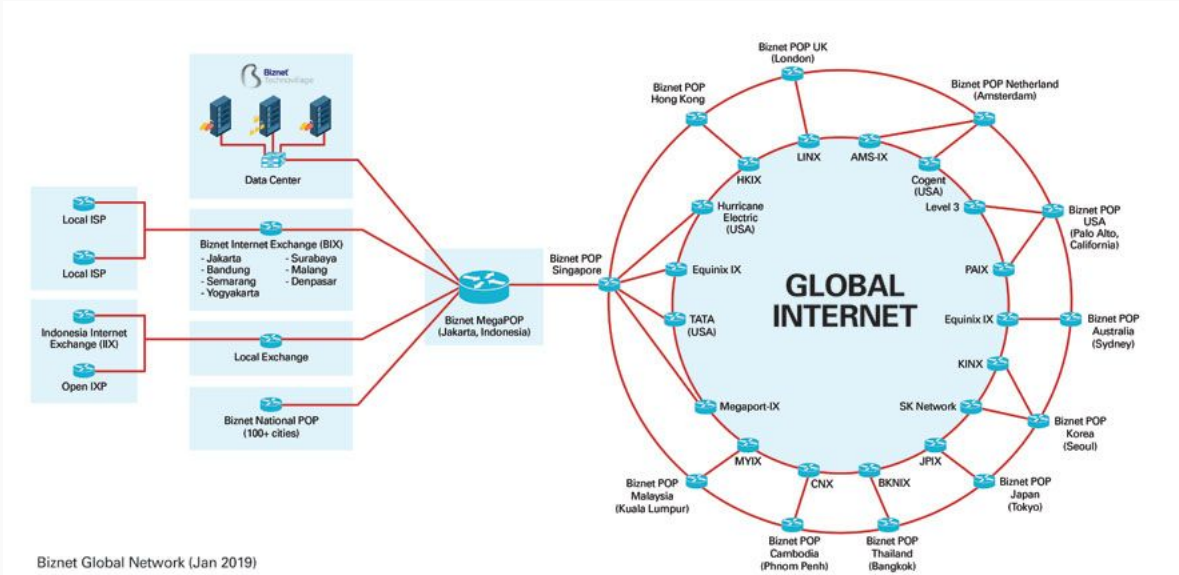
- Radio Local Area Network
  - Extends physical network areas
  - Blurs the edge of the network
  - Susceptible to outside interference and manipulation
  - https://www.wigle.net



Pineapple Demonstration

Internet

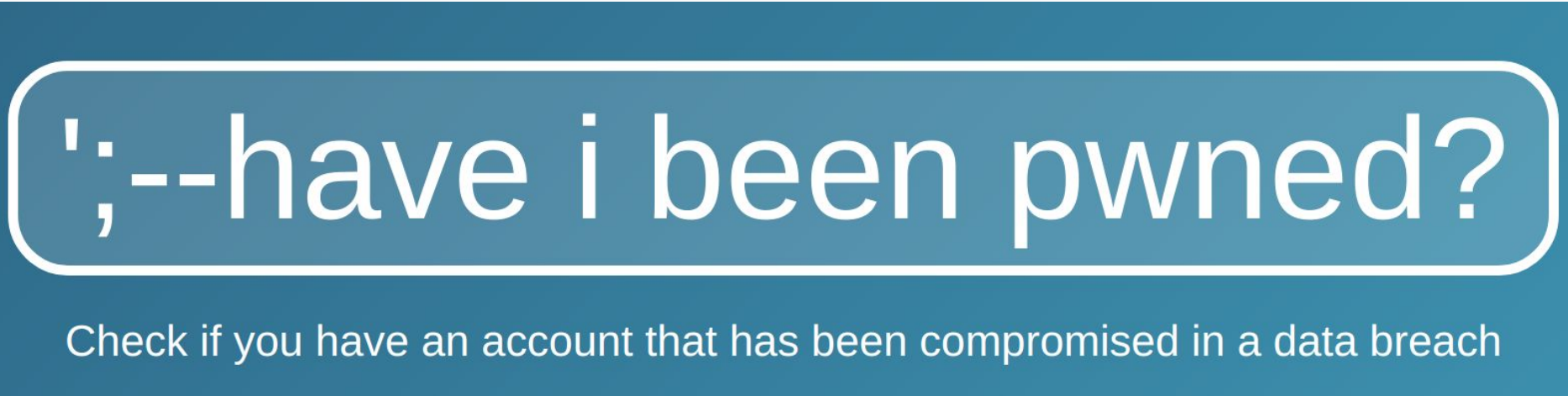
- A network of networks



Biznet Global Network (Jan 2019)

Passwords

- Have I Been Pwned?
  - Depending on Time, we can work through some Cryptography work



Online Safety

Phone Call Attacks and Scams

Stop that Phish

Shopping Online Securely

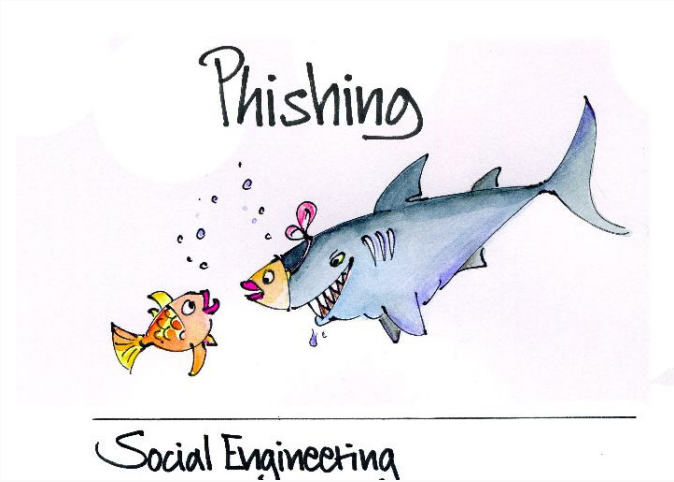
Tips to Securely Use Social Media

Phone Call Attacks and Scams

- Cyber Criminals use email, messaging and phones
  - Phones have fewer security technologies to detect attacks
  - Easier for bad guys to convey emotions
- How do they work?
  - Attackers *usually* want money, information, access to computer or all of the above
  - Attackers create urgent situations to get you off-balance
    - Don't think clearly and rush into making a mistake

Phone Call Attacks and Scams

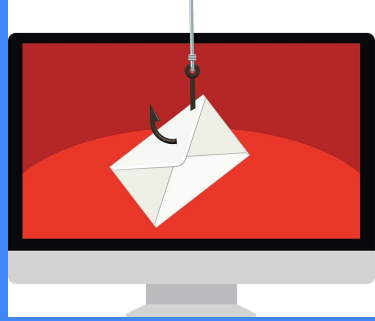
- Examples
  - Caller pretends to be from a government tax department or tax collection service regarding unpaid taxes
  - Caller pretends to be from Microsoft Tech Support to explain your computer is infected
  - Automated voicemail message that your bank account is cancelled and must call to reactivate

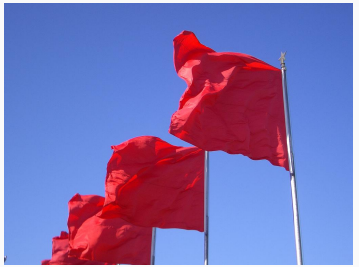


Phone Call Attacks and Scams

- Protect Yourself
  - Tremendous sense of urgency, pressuring you to act
    - If you believe the call is an attack, hang up
    - Call legitimate business' customer support line
  - Never trust Caller ID
    - Phone numbers can be spoofed
  - Never allow a caller to take temporary control of your computer or download software
  - If you don't know the number, let it go to voicemail

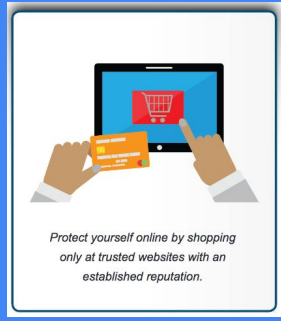
Stop that Phish





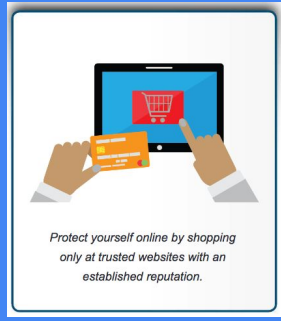
- Phishing: email/messaging attack
  - Can use legitimate logos, forge email addresses, etc.
- Red Flags
  - Too good to be true
  - Generic salutation
  - Requesting highly sensitive information
  - Message from an official organization, but has poor grammar, spelling or ends with @gmail.com
  - Message comes from official email (boss) but has Reply-To as a personal account
  - Message comes from someone you know, but the tone/wording doesn't sound like him/her

Shopping Online Securely



- Fake Online Stores
  - When possible, purchase from websites you already know, trust, and have done business with
  - Verify
    - legitimate mailing address and phone number for sales or support-related questions.
    - Type store's name/URL into search engine to verify
  - Deals too good to be true, poor grammar and spelling are warning signs
  - Before purchasing, ensure your connection is encrypted

Shopping Online Securely

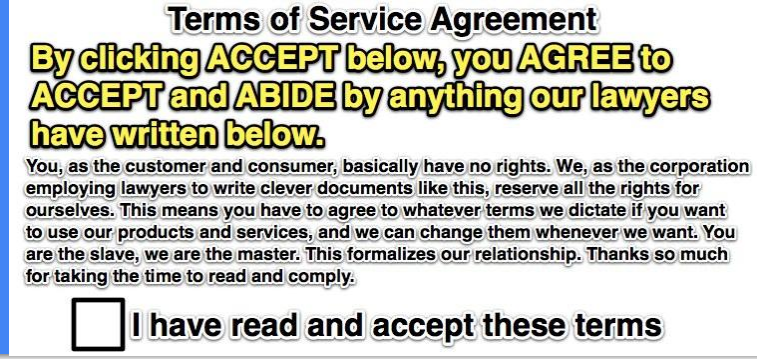


- Your Credit Card
  - Regularly review your credit card statements to identify suspicious charges
  - Use email/text notifications when a purchase is made
  - Consider using well-known payment services like PayPal which do not require you to disclose your credit card to the vendor

Tips to Securely Use Social Media

- Posting
  - Anything you post will most likely become public, impacting reputation and future
  - Be aware of what others post and share about you
- Privacy
  - Almost all sites have strong privacy options; enable when possible
- Passphrase
  - Have unique passphrases to all accounts

Tips to Securely Use Social Media



- Lock down your account
  - Enable two factor authentication on all accounts
- Scams
  - Bad guys will attempt to trick you using social media messages via links
- Terms of Services
  - Know the Terms; anything you post might become the property of the site
- Work
  - If you post anything about your work, check with your supervisor first

Securing the Home

Securing Today’s Online Kids

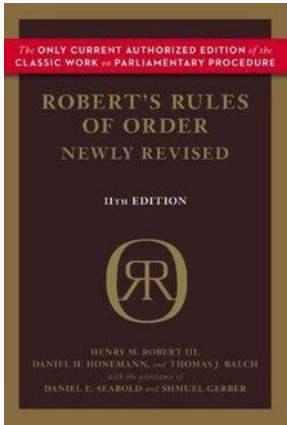
Gaming Online Safety & Security

Creating a Cyber Secure Home

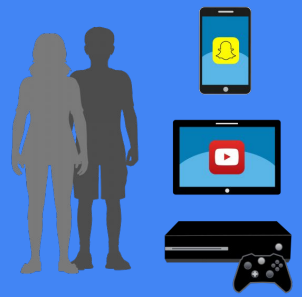
Internet of Things

Securing Today's Online Kids

- Some rules to consider
  - Times when they can & cannot go online and how long
  - Ask how their online friends met
  - Talk about types of websites/games that they should/shouldn't visit/appropriate
  - What information they can share with whom
  - Who they should report problems to (bullies, creeps)
- Talking Points
  - Treat others as they would want to be treated
  - There is no anonymity online
  - People online may not be who they claim to be



Securing Today's Online Kids



- Technology
  - Technical solutions work best for younger children
  - Older kids need more access to Internet and are often given devices that you do not control or can't monitor
    - School devices, gaming consoles, computers at friend's house
  - Education is important!
- Have dedicated computer for kids
  - If accidental infection, it does not affect your sensitive activities
  - Keep computer in high-traffic area to monitor their activities
  - Ensure children don't have administrator rights
  - Consider central charging station for mobile devices

Gaming Online Safely & Securely

- Securing Yourself
  - Be cautious of any messages that ask you to take action (link, downloading a file)
  - Many online games have their own financial markets
    - There are fraudsters who will attempt to trick you and steal your money and/or virtual currency
    - Strong passphrases on accounts; two factor authentication as well

Gaming Online Safely & Securely

- Securing your System
  - Secure your computer with latest version of Operating System and gaming software
  - Use an anti-virus and keep it updated
  - Download gaming software from trusted websites
  - Download gaming add-ons, packs from trusted websites
  - Underground markets tend to have infections for computers

BLIZZARD ENTERTAINMENT

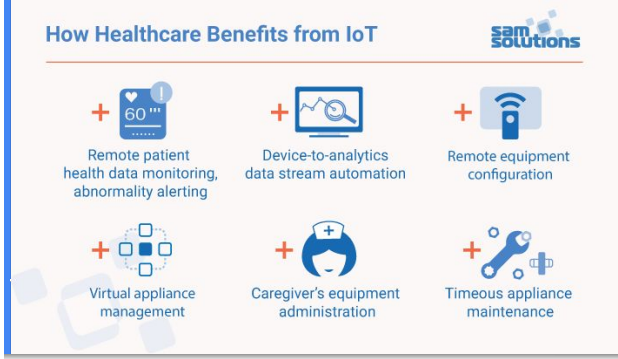
EA GAMES

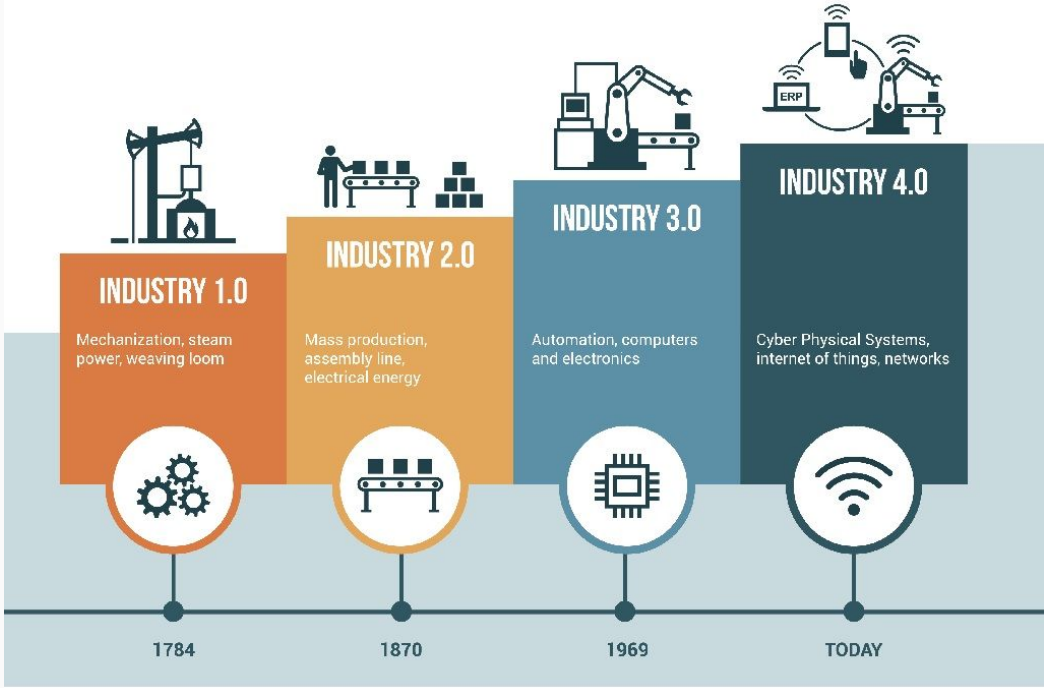
EPIC GAMES

Creating a Cyber Secure Home

- Your Wireless Network
  - Change default administrator password to your Internet router/Wireless Access Point
  - Ensure only people you trust can connect to your wireless network
    - Implement WPA2
  - Ensure password used to connect is strong and different from administrator password
  - Implement Guest Network
- Devices
  - Know what devices are connected to the network
    - Fing
- Backups
  - Implement backups; you never know when you'll need to recover data!

Internet of Things

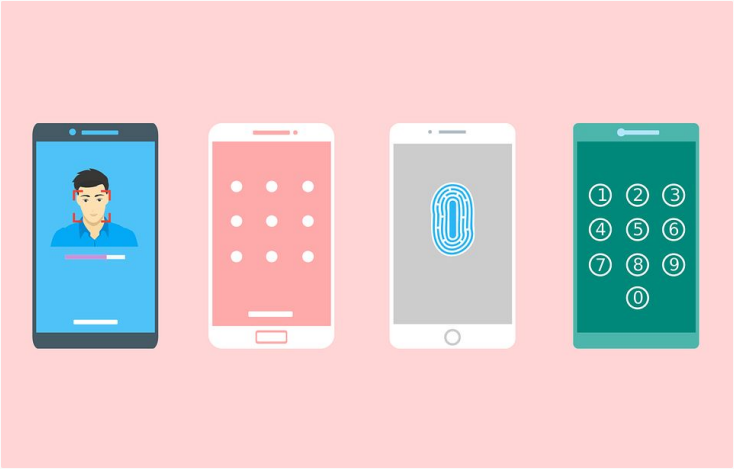




Smart Home Devices

- What can you do to protect your home?
  - Connect only what you need to the Internet - do you need the toaster sending notifications?
  - Know what you have connected - turn off wireless network to see what stops working
  - Keep Updated - just like any other device
  - Passwords - strong unique passphrases
  - Privacy Options - limit amount of information it collects/shares or disable
  - Vendor - buy from company that you know and trust
  - Always Listening - Project Alias
  - Implement Guest Network

Mobile Security

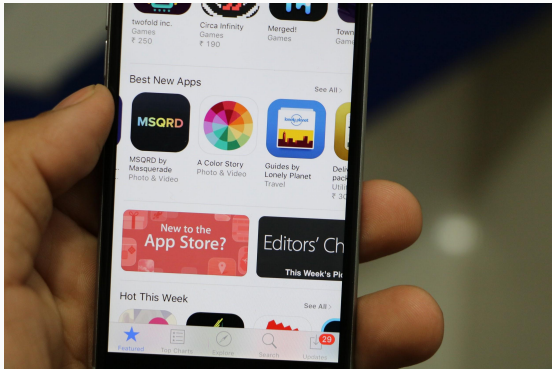


Securely Using Mobile Apps

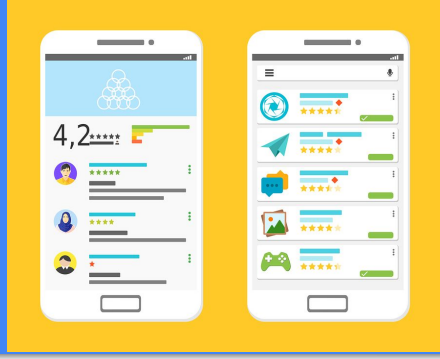
Securing Your Devices

Securely Using Mobile Apps

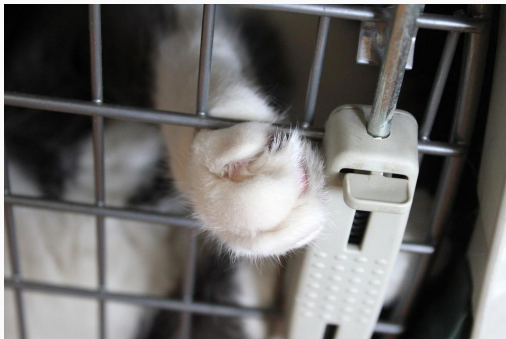
- Obtaining Mobile Apps
  - Always download from safe, trusted source
    - Reduce the chance of installing infected apps and allowing criminals to take complete control of your device
    - When trusted sources find a malicious app, they are quick to remove them
  - Apple (iPad, iPhone): Apple App Store
  - Google (Android): Google Play Store
- Additional protection: install an antivirus
  - Avast, McAfee, Trend Micro, Bitdefender, Avira



Securely Using Mobile Apps

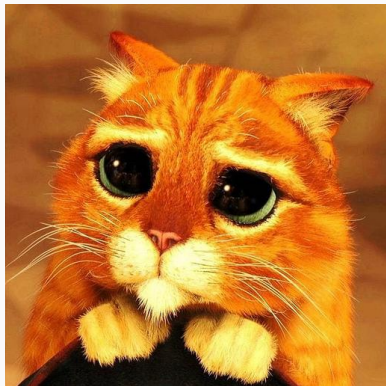


- Trends
  - Avoid new apps with few downloads and few comments
- Use
  - Install applications you need and use
- Jailbreak/Root
  - Never jailbreak or root devices
  - Bypasses and/or eliminates many security controls and voids warranties and support contracts



Securely Using Mobile Apps

- Permissions
  - Always think before allowing an app access
    - If you allow geolocation, the creator of the app can track your movements, even allowing author to sell that information to others
    - It is ok to deny permission requests or shop for another app that meets your requirements
- Updates
  - As developers find weaknesses, they will release those fixes as updates
  - Most devices allow apps to be updated automatically
  - Prevents criminals from exploiting any known weaknesses

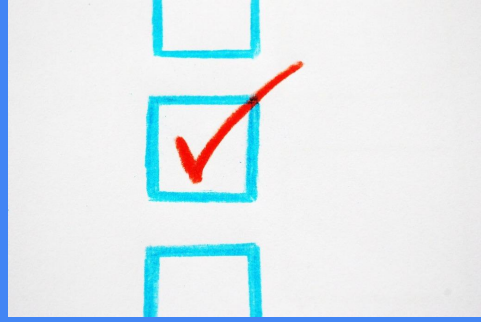


Securing Your Devices

- The biggest risk to your mobile devices isn’t hackers, its you
  - More likely to lose or forget the device than have someone hack it
- Enable screen lock
  - Ensures no one can access your device if lost or stolen
- Enable Tracking
  - Find my iPhone / Find My Device
- Backups
  - Always backup your data
- Work
  - While at work, be careful about taking pictures/video that may accidentally include sensitive information (whiteboards, computer screens)

Tying it all together

Staying Secure on the Road



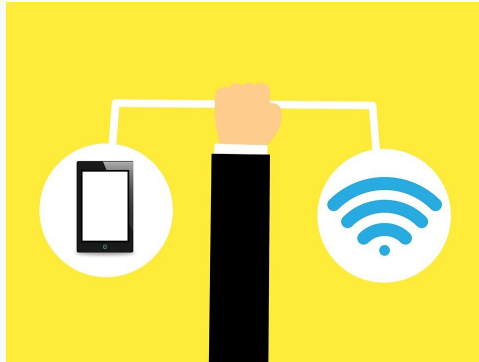
- Pre-check
  - Assume any network you connect while travelling cannot be trusted
    - Don’t know who else is on and what they are doing
  - Safest Information is what you don’t have
    - Identify data you do not need on any devices you are bringing and remove it
    - Reduces impact if device is stolen, lost or impounded by customs or border security
      - If work related, as your supervisor if the organization can provide devices specifically for working while traveling

Staying Secure on the Road

- Pre-check
  - Lock mobile devices with strong password or passcode
  - Install or Enable full-disk encryption
  - Install or Enable tracking software
  - Update devices, applications and anti-virus software
  - Perform a complete backup
- International Travel
  - Check what service plan you have for your phone or purchase a local prepaid SIM card

Staying Secure on the Road

- Lost/Stolen Devices
  - Ensure physical safety of your devices
  - Verizon study in 2017 showed people are 100 times more likely to lose device than have it stolen
- Wi-Fi Access
  - Never sure who set them up and who is connected to them
  - Wi-Fi is radio signals that can be intercepted and monitored
  - Ensure all communications is encrypted (HTTPS://) or Virtual Private Network



Staying Secure on the Road

- Public Resources
  - Do not use!
    - Don’t know who was on it before you
    - Don’t know if they infected the public computer accidentally or deliberately
    - Whenever possible, use devices you control and trust
    - Public computers are good for public information (weather, news)

Two Factor Authentication (2FA)

- Text messages are not a good 2FA as phone numbers can be spoofed
- Consider using a physical key or an Authenticator App
- Google Two-Step Verification
  - Physical Key
    - Yubico
    - Google Titan Key
  - Authenticator App
    - See App Store
    - Generates One Time Keys for security

Virtual Private Network

- If you must connect to a Public Network, use a VPN
  - VPNs keep your communication with the world private to those around you
- Consider Using
  - ProtonVPN
  - NordVPN

NordVPN

ProtonVPN

Cabrillo College

Personal Information Security Basics
Session 1: Hygiene for Your Digital Life

Irvin Lemus
Cybersecurity Professor; Computer Information Systems Department
Bay Area Cyber Competitions Regional Coordinator

irlemus@cabrillo.edu (831) 479-6296
@infosecirvin