Want to join IEEE? ieee.org/join

Benefits:

- Life Insurance – Best deal around
- Access to technical resources
- Networking with local technologists
- Local technical talks
- Standards development
- Join an international community of over 420,000 engineering and technology professionals
- sites.ieee.org/msn

Cybersecurity and You

Recommendations on Protecting Your Personal Digital Assets

Introduction

- Nate Toth
- Chair - IEEE Madison, Webmaster – IEEE Madison, Young Professionals Chair – IEEE Madison
- Current position – IT Security Systems Administrator at Alliant Energy
- Education – Herzing College (2007), hundreds of hours of training on all manners of computer networks and cybersecurity topics
- Certifications from Cisco, CompTIA, ISC2, Microsoft
- Advised clients ranging from non-technical individuals at home to highly technical large multi-national organizations
- No conflicts of interest

Notes:
I am an expert on network segmentation, firewalls, intrusion prevention/detection systems, VPNs, and secure wireless communications. And to a lesser extent, on endpoint protection, malware discovery/remediation, and general system maintenance.
I am not a seasoned security researcher, don't have a PhD, I am not a world renowned expert, not a master hacker. This is a free presentation, after all.

What are we covering?

- The Threats
- Assessing Your Risk
- Your Data
- Your Computers, Smartphones, Smart Home devices
- What if I have really sensitive data?

What you will find in this presentation is that being secure and maintaining your privacy, requires a lot of work and vigilance.

The threats

- Nation/State threat actors
- Low skill/high skill individual threat actors
- Low skill/high skill organized threat actors
- Data collectors

Nation/State – governments. Also called APT. They are motivated by the interests of that nation (offensive operations against infrastructure, stealing sensitive intellectual property (defense industry, large corporations), affect elections, suppress rights, and fight crime. Probably not targeting you personally, but need to be aware of them.

Low skill/high skill individual threat actors – an individual with a vendetta against an individual or organization. They will do more of an espionage type operation. Track an individuals activities online or in the physical world, gain access to email/webcam/bank account/social media, business networks, conduct online harassment. Could be individuals trying to prove skills by defacing a website or gain notoriety in some other way

Low skill/high skill organized threat actors – organized crime, hacking collective. They are going after the data/money of a large number of people or many businesses. They use Phishing emails, SPAM, send robocalls, deploy ransomware, and deploy malware to steal passwords/data. They run botnets. Primarily motivated by $$$. Hacktivists – DDoS attacks, could be destructive, political motivations.

Data collectors. Not necessarily malicious. They are in business to acquire data and monetize it. But they often leak that

data. More on that later

Malware

- Keyloggers
- Data harvesters
- Ransomware
- Critical Infrastructure Malware

Keyloggers – record keystrokes, screenshots, mouse movements
Data Harvesters – IP, metadata, browser data
Ransomware – extort money. Cryptolocker. Blackmail (I see you, now pay)
Critical Infrastructure Malware - Stuxnet – Iranian Centrifuges, Crash Override – Ukrainian Electrical Grid, Triton – Schneider Electric equip, malware targeting safety systems
Millions of types and variations of those types exist

Assessing your risk

"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."

— **Sun Tzu, The Art of War**

The internet is a hostile place. And determining how you and your digital assets fit into that is a critical step in defending them.
That is the "know yourself" part. We have covered some of the threats, and will continue to talk about those threats.
That is the "know the enemy" part.

Assessing your risk – things to cover

- You need to inventory your physical and digital assets
- Identify the threats present
- Assessing impact of data loss

Why? You can't protect what you don't understand

Assessing your Risk, continued

- Inventory:
  - Financial accounts
  - Social media accounts
  - Streaming media accounts
  - Entertainment accounts
  - Backup software
  - File storage
  - Email accounts
  - Other cloud services

Financial accounts – bank, credit card, IRS.gov, taxes, PayPal, bitcoin wallet
Entertainment – Xbox live, Playstation Online, online gaming
Backup software, and where those backups go
File storage – including local storage (NAS, removable media, cloud storage)
Other cloud services (Retail - Amazon, Ebay; IEEE account; Health care (Epic MyChart), Google account, software subscriptions)
Email accounts
If you have never done this before, take pen to paper and start a list.
Not electronic (you haven't secured your data yet)

Assessing your Risk, continued

- Identifying threats
  - Is anyone really upset with you?
  - Are you developing a new product?
  - Are you working on any government projects?
  - The organized threats are always present
- You need to know if you are a potential target

If you are a potential target, knowing that will raise your awareness, and you may choose to restrict your online activities, or increase defenses.

Assessing your Risk, continued

- What could you lose if your data is misused?
  - $$$
  - Trade secrets/Intellectual Property
  - Patents, competitive advantage
  - Your job
  - Your privacy

$$$ - your bank accounts/credit card accounts. Someone could also use your data to create new accounts. You could be the victim of a scam

Trade secrets – your proprietary data, proprietary methods/procedures, source code, system passwords, schematics/blueprints/design documents

If you are developing a new technology, losing the data could mean you lose out on a patent, or lose a competitive edge

If you mishandle data/digital assets that are the property of your employer, you could lose your job

Your privacy. This could be something as simple as accidentally revealing what you got your spouse or significant other for their birthday. Or your entire location history that was recorded by your smartphone could become public. The websites you have visited, the conversations you have at home, the messages you send to your family, friends, collogues, spouses. You have a right to privacy (1st, 4th Amendments to the Constitution, various federal and state laws are supposed to protect us by limiting the actions the government can take). IEEE also has very strong privacy rules.

Your data

The most valuable thing you own

Data

- Data is a piece of knowledge about something. Information is data put into context
- Data is the new resource, it is to the 21st century what oil was to the 20th century
- Who values your data?
- https://www.weforum.org/agenda/2017/09/the-value-of-data/

It stands to reason that since data has value, data in context (information) has more value. Your birthday might not be worth much as a data point. But your name, date of birth, place of birth, mothers maiden name, SSN, and current address combined make some very valuable information. Your phone number and your likelihood to fall victim to a scam is valuable information.

Data is valuable. Companies want it (the largest companies in the world make money on data). Criminals want it (sell the data or use it to steal money from you). Governments want it (intelligence operations, repression). Google and Facebook are 2 of the largest companies that make their money on data

World economic forum estimates that all of the personal data on earth today is worth $3 trillion.

Data – protecting it

- File sharing sites (Dropbox, Google Drive, etc)
- Backups
- Email accounts

- Need strong passwords, 2 factor/multifactor authentication

Who are you sharing files with? What permissions do they have? Have you read terms and conditions/EULA?

The EULA of some sites give them the rights to your data, including for their own marketing purposes, or selling information for the purpose of advertising. So if you upload your family photos, you might see your pictures in marketing material for that company, or another company. And you will not receive any royalties. READ THE EULA/terms and conditions

Same thing with online backup services. Read the terms and conditions. Carbonite, for instance, will scan your backups for certain types of content, namely illegal content and malware. But they scan all files, not just the illegal or dangerous ones. If you want your data protected, but need it backed up, encrypt those files. More on that later

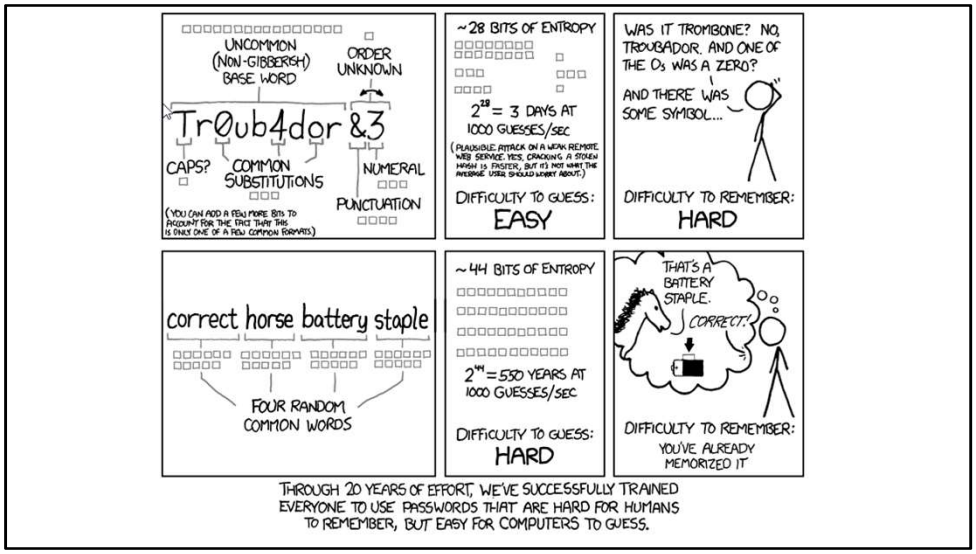
Protect your email account. Google and many other major services offer 2 factor authentication or multifactor. Use that. Beware that Google, Yahoo, Microsoft, and many other services, will scan your inbox to offer you advertising. This is email is offered for free, but it costs money to maintain.

Google maintains great SPAM, malware, and phishing detection service. The risk of having ad keywords harvested from your inbox could be a fair trade-off.

Detour - Passwords

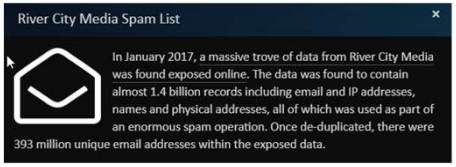
- Password management
  - Never reuse a password
  - Strong passwords (12 char minimum, 20 or more char for bank/email)
  - 2 factor (something you know and something you have)
  - Multi-factor (strong biometric)
  - Use password manager
  - Schedule password changes
  - For hints, use false information
  - Okay to write passwords down! (with caution)

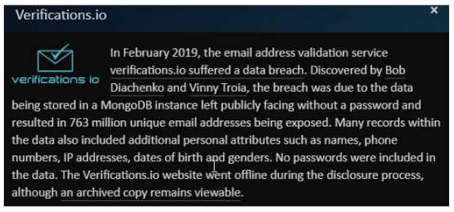
Use unique passwords for every site, never re-use passwords
Use strong passwords/passphrases - minimum of 12 characters, use 20 or more for your bank/primary email
Use 2-Factor/Multifactor if possible
Use a password manager (KeePass, LastPass, etc) – it can generate very secure passwords
Password saving in Chrome/Firefox/IE/Edge is easy, but might not be real secure. Many password managers have browser plugins
Writing down a password is OK (as long as you secure that paper)
-you could use a secret word for the second half of a password, and write down the first half
-come up with a code-name for the site (your bank can be called "cookie jar", Netflix can be called "Blockbuster", etc)
-Good idea to write down your security questions/answers (use unique fake information, unless you are REQUIRED to use real information)


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 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 O's WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER:
HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 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.

Back to your data….

- Data breaches – what do they contain?
- Why breaches matter





Your data HAS been breached (accessed by an unauthorized individual) (https://haveibeenpwned.com/)
This data can be used to create accounts in your name, recover your passwords and break into your accounts

Data from many breaches can be aggregated - this aggregated data is enough to steal your identity/your kids identity
Following good password/privacy/security practices will limit the amount of data that is exposed, which will limit the damage done in a breached
Verifications.io: **Compromised data:** Dates of birth, Email addresses, Employers, Genders, Geographic locations, IP addresses, Job titles, Names, Phone numbers, Physical addresses
Apollo: **Compromised data:** Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Salutations, Social media profiles
Adapt: **Compromised data:** Email addresses, Employers, Job titles, Names, Phone numbers, Physical addresses, Social media profiles

Data protection continued….

- Use fake answers to security questions, and document
- Limit data sharing if possible
- Follow this general rule: if it doesn't need to be on the internet, don't put it on the internet, or even on your internet connected device.
- Browser enhancements – more on that later

For security questions, use fake information. You grew up on State Highway 139, your first dog was Henrieta, you went to Malibu High, your birthday was January 10th 1907.
-limit sharing, if possible (opt out of having your data shared with 3rd parties)
Ancestry.com/23andMe.com
Background check sites
Social media – Facebook – check your privacy settings
Google, check privacy settings - chrome://settings/, Advanced, Privacy and Security

Your Computers, Smartphones, Smart Home devices

Safe configuration, maintenance, use

Your computer needs maintenance

- Keep your computer, smartphone up-to-date
  - OS updates should be automatic
  - Application updates, including the free ones
  - Browser updates (including plugins)
  - Firmware/drivers (PC's)
- Make a recurring calendar event (like the 2nd Saturday of the month) to check your computers

What about My old computer?

- You might need it
- Only use it for the legacy software, then turn it off
- Securely wipe hard drive, or destroy hard drive
- Recycle your computer (File13 E-Waste)

On your old computer, keep it updated as long as possible, but don't browse the internet on it
Windows XP, old Linux/Unix

Disk wiping – most of the utilities out there were designed for magnetic hard drives, not SSD's. SSD's write data differently, and the methods of wiping the drives are different. Best course of action might be to physically destroy the drive by shredding. Take the plasma cutter to it?

Maybe IEEE Madison could sponsor an e-waste collection/destruction event this spring/summer

Security software

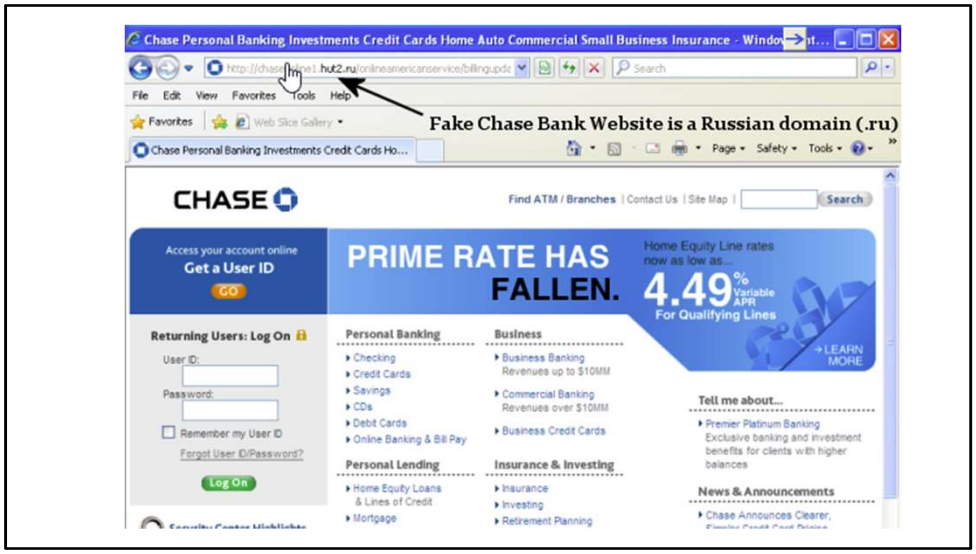
- If you use Windows 10, Windows Defender is an excellent product
- Malwarebytes can be used along side Defender
- OSX and Linux need Antivirus too!
- VeraCrypt – encryption software to maintain privacy
- Fileshredder – fully delete a file - unrecoverable
- Browser plugins – use HTTPS Everywhere and Ghostery, DuckDuckGo

Antivirus - Windows Defender is excellent software for Windows computer
Malwarebytes anti-malware (if malware is installed on your computer)
Browser plugins
-Ghostery (blocks trackers/add-ons/scripts)
--Increase security by blocking malicious web items
--Increase privacy by reducing data collection
-HTTPS Everywhere
--Forces the strongest https connection to sites, mitigates sloppy programming
-DuckDuckGo (mobile browser too)
--Very privacy focused, similar features as Ghostery and HTTPS Everywhere
--They do not collect data

Safe browsing

- Use Safe Search
- Browser plugins
- Do not click on ads!
- Facebook/Google/LinkedIn permissions
- Verify you are going to the correct sites (fake bank sites)
- Maybe a separate computer just for banking?

Erase browser history and cookies periodically
Use Incognito mode/Private Browsing mode – won't save your session data
Shortened URL's – use an unmasking site (checkshorturl.com or unshorten.it)
Using Ghostery and HTTPS Everywhere will severely limit the amount of metadata and data that websites collect on you
Location sharing in Chrome


Chase Personal Banking Investments Credit Cards Home Auto Commercial Small Business Insurance - Windows...
http://chaseonline1.hut2.ru/onlineamericanservice/billingupda
Search
File Edit View Favorites Tools Help
Favorites
Web Slice Gallery
Chase Personal Banking Investments Credit Cards Ho...
Page Safety Tools
Fake Chase Bank Website is a Russian domain (.ru)
CHASE
Find ATM / Branches | Contact Us | Site Map |
Search
Access your account online
Get a User ID
GO
PRIME RATE HAS FALLEN.
Home Equity Line rates now as low as...
4.49% Variable APR
For Qualifying Lines
LEARN MORE
Returning Users: Log On
User ID:
Password:
Remember my User ID
Forgot User ID/Password?
Log On
Personal Banking
Checking
Credit Cards
Savings
CDs
Debit Cards
Online Banking & Bill Pay
Business
Business Banking
Revenues up to $10MM
Commercial Banking
Revenues over $10MM
Business Credit Cards
Personal Lending
Home Equity Loans & Lines of Credit
Mortgage
Insurance & Investing
Insurance
Investing
Retirement Planning
Tell me about...
Premier Platinum Banking
Exclusive banking and investment benefits for clients with higher balances
News & Announcements
Chase Announces Clearer,


www.lolomgz.a.gp/?_fb_noscript=1
facebook
Sign Up
Facebook helps you connect and share with the people in your life.
This is a Phishing Scam. This web site looks like Facebook.com, but if you note the web address in the the browsers address bar you can clearly see this is not Facebook.
Facebook Login
Email:
Password:
XXX
Keep me logged in
Login
or Sign up for Facebook
Forgot your password?
English (US)
Español
Português (Brasil)
Français (France)
Deutsch
Italiano
Facebook © 2010
About
Advertising

Safe email

- Phishing – trying to get you to click on a fake website
- Questionable email attachments
- Use good judgement
- Keep a separate email account for family/friends
- Have a “SPAM” email account
- Have an email account just for banks/financial institutions
- Shortened URL’s – use an unmasking site (checkshorturl.com or unshorten.it)

Backups

- Backup your computer securely
  - External backup drive
  - Carbonite
- Test your backups
- Have copies of your paid software, OS key, OS software
- Transfer files from your smartphone to your PC

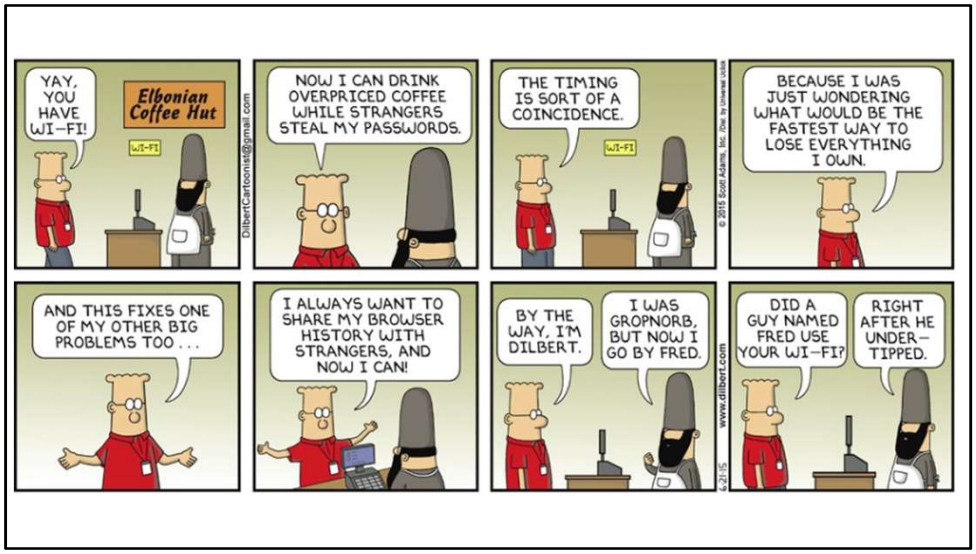
Home network equipment

- Apply updates regularly
- Use WPA2 with strong password
- Guest network option?
- Change default password on router
- Serious about security? Get a PFSense appliance

Using Wi-Fi

- Public/unsecured Wi-Fi should never be trusted
- Hotels, restaurant/bars, convention centers, airport, airplane, coffee shops, retail, casinos, mass transit
- Use hotspot or teathered phone instead
- If you MUST use unsecured Wi-Fi, NEVER log into your primary email or bank

Public/Open WiFi
-Use with caution - unsecured wifi should NEVER be trusted. Never log into anything you care about on public WiFi
-If you MUST use public wifi, use a VPN service (work, to your home, commercial VPN service)
-Use teathering on your phone or use a hotspot instead (but follow the same security as you would at home with a strong password)
-Hotels, restaurants/bars, convention centers, airports, coffee shops, retail establishments, casinos, mass transit, etc all offer wifi
-You don't know everyone connected to that
-Some places use it to collect data (retail, casinos) that they will use to market items or sell that data
-Numerous people have had their email or bank account credentials stolen while on open wifi
-even your VPN could be compromised while on open wifi


YAY, YOU HAVE WI-FI!
Elbonian Coffee Hut
WI-FI
DilbertCartoonist@gmail.com
NOW I CAN DRINK OVERPRICED COFFEE WHILE STRANGERS STEAL MY PASSWORDS.
THE TIMING IS SORT OF A COINCIDENCE.
WI-FI
© 2015 Scott Adams, Inc. (Dist. by Universal Uclick
BECAUSE I WAS JUST WONDERING WHAT WOULD BE THE FASTEST WAY TO LOSE EVERYTHING I OWN.
AND THIS FIXES ONE OF MY OTHER BIG PROBLEMS TOO . . .
I ALWAYS WANT TO SHARE MY BROWSER HISTORY WITH STRANGERS, AND NOW I CAN!
BY THE WAY, I'M DILBERT.
I WAS GROPNORB, BUT NOW I GO BY FRED.
www.dilbert.com
DID A GUY NAMED FRED USE YOUR WI-FI?
RIGHT AFTER HE UNDER-TIPPED.

VPN

- Encrypts your data so that it remains private
- VPN services can protect you on public Wi-Fi
- Use with caution (read terms and conditions)
- Work VPN/VPN to your home router instead

A VPN encrypts your connection between your VPN client and the VPN server. This could allow the operator of that server to have unprecedented access to your data. Is that better or worse than the network you are on?

Smartphones

- iOS or Android?
- Need to keep updated
- Update your apps too!
- Use Google Play Store/Apple App Store only
- Remove unused apps
- App permissions
- Location data
- Encrypt phone storage

no platform is generally more secure (iOS and Android both have vulnerabilites, but more common in Android)
Pixel phones from Google, Samsung Galaxy S phones are very good. Android powered Blackberry is the best (no rooting, no malware)
Think of a Smartphone as a version of a computer that was redesigned for the sole purpose of ease of use and rapid access to information. Your privacy or the security of your data was an after thought (if that).

Location tracking is used for advertising, can be used by a stalker. It can help you (GPS, weather alerts, finding nearby businesses). But that data is constantly being used for things you may not want it to be used for. Apps can use this!

Can I use the free Public wifi on my phone?

- NO
- NO
- NO
- NO
- NO
- Seriously, no.

Reducing SPAM Calls

- DoNotCall registry (Federal and State) – somewhat helpful
- Do Not Disturb feature
- Free apps/paid apps from App Store/Play Store
  - RoboKiller – decent app, ~$26 annually
- Carrier apps/service
- Call whitelisting – a feature of some smartphones
- Real fix will be STIR/SHAKEN

DoNotCall – will keep legal telemarketers from calling you, penalties can be severe
Do Not Disturb – allow only contacts to ring/vibrate/light up your phone, not perfect
Apps- there are numerous free and paid apps that will claim to block spam calls. Some are just very clever marketing platforms that will steal your calling information.
Your cell phone carrier might offer a service, Verizons was not very effective at $3 per month
STIR/SHAKEN – will end the practice of caller ID spoofing
Estimated that in 2019, half of all calls to mobile phones will be fraudulent

Text messaging

- SMS is not encrypted
- Assume that SMS is being monitored/tracked
- Use Signal
  - Free (donations)
  - End to end encryption, not possible to break
  - Will work overseas, and keep foreign governments from snooping
  - Works on wi-fi, not SMS platform

SMS encryption – don't send anything that you don't want public
It is being monitored/tracked by carrier, google, government, isp's
Signal, also provides encrypted calling

Smart assistant

- Siri, Bixby, Google Assistant
- Assume they are always listening
- Google account – Data and Personalization – Voice and Audio – Manage Activity: you can see all of your recordings

Google activity – some might be unintentional – you didn't push the button intentionally – disturbing?

Mobile payment platforms

- Samsung Pay/Apple Pay/Google Pay
  - Increase in payment security in exchange for privacy

They use tokenization – your credit card number is never provided to the merchant, so if their system is breached your cc is safe
Why do they offer this service? Data! They know what you are purchasing, when, where, how often.

Trade-off might be worth it, especially if you use a debit card (sometimes you won't get your money back if it is stolen, could take a while)

Biometric scanners

- FaceID, TouchID, Iris Scanner, fingerprint scanner
- All are pretty secure
- Set your phone to unlock with PIN, then you can use biometrics
- Legally, PIN is a password/biometrics are a key

Smart Home devices

- Just like computers, these need updates
- And strong passwords
- Use with caution
- Many “SMART” devices have major security vulnerabilities
  - Smart baby monitors
  - Smart TV’s

Smart baby monitors with little to no security, or major back doors
Smart refrigerator that stored passwords in plain text – to all of the accounts you signed in with
Smart TV’s that send your viewing history to somebody

Smart speakers

- Assume they are always listening

Assume they are always listening.
Privacy concerns?
Shown: Amazon Echo, Apple HomePod, Google Home

More Smart home devices

- Security system (burglar alarm/fire alarm) – internet connected?
- Security cameras
- Smart thermostat – need to monitor these and use strong passwords

Security systems that are internet connected might be vulnerable to malware/hacking/ddos
Could cause false 911 calls
Do your research, and don't just get the cheapest thing out there (Even ADT had a major vulnerability, could unlock doors remotely/disarm system)
Security cameras – outside your home only

I have very sensitive data

What do I do?

Top security and privacy

- Data segmentation
  - Use separate computer for sensitive things (IP, Trade Secrets, unreleased technology)
  - Separate backups/storage
- Full disk encryption
- Email encryption (use OpenPGP or GnuPG)

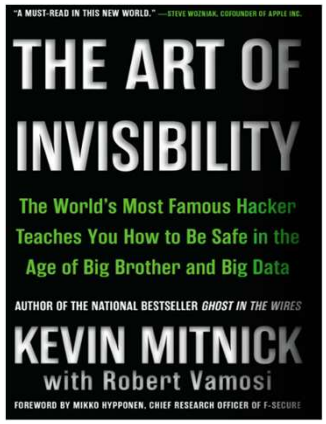
Separate computer – no banking, internet browsing, shopping, etc

Network upgrades

- Separate network/VLAN for your sensitive systems
- IPS/IDS on your firewall (if you use PFSense, this is easy)
- Everything you are doing for your other systems, but you need to be much more vigilant

References for extreme privacy

- Art of Invisibility, by Kevin Mitnick



Conclusion

Takeaways

- To Do List
  - ❑Inventory your accounts
  - ❑Configure automatic updates, check regularly
  - ❑Strong, unique passwords (especially on your primary email and bank)
  - ❑Reduce/eliminate use of unsecured wireless
  - ❑Carefully examine links before you open them
  - ❑Disconnect once in a while

- Cyber security is a series of cumulative steps
- No single thing you can do to be more secure, increase privacy
- Not expensive – most of what I showed today is free, or you already have it
- Requires vigilance
- Requires scheduled maintenance
- Requires accepting risk
- Most of the security incidents I have investigated could have been avoided with timely updates
- Stay safe online, safe at work, and safe at home
- Questions?