Security 2026

For Apple Devices (Mac, iPhone, iPad, etc)

Introduction:

- Many seem to think there is a magic setting, or a magic program to install that will make your Apple devices 100% secure now and into the future.
  - This is not the case.
- Let's give an analogy. You don’t ever want to get into an accident in your vehicle.
- Maybe there not one solution, but no more that two will handle it.
- Have a mechanic inspect your tires and your brakes on the wheels. If so, you are perfectly safe.
  - The mechanic will need to fix the broken ABS system too!
  - What about worn shocks and suspension. A bumpy off camber downhill road in the mountains could send you over the cliff
  - What about burned-out stoplights.
  - I could go on and on with things that need to be right in your vehicle

Introduction (cont'd):

- But, the most important thing you can do is to take responsibility to be a good driver
  - Don't just go past stop signs without stopping
  - Stop for red lights
  - Don't drive too fast for conditions
  - Don't drive while impaired (Alcohol etc)
- There are some things out of your and your vehicles control
  - Hit by a Meteor (yes very unlikely)
  - Large rock lands on your vehicle in the mountain roads
  - Elevated freeway transition road collapses from an earthquake while you are on it
- Security for your Apple devices is like this.
- I will not get into a privacy discussion here, too much to cover. Yes, good security helps in your privacy

Basic Advice: (Wash your hands and Brush your teeth):

- First off use passwords. You can have iPads and iPhones, and even Macs with some effort now, open without a password.
  - Very dangerous on mobile, devices, even on homebound Mac desktops. Someone gets into your house, or the hacker friend of you grandchild comes over for a visit.
  - Can't imagine most banking, government, financial institutions etc. would not require a password now a days, but if you find one, don't go without needing authentication.
- Don't Share passwords
  - More people knowing a password means more chances for it to be intercepted, phished, or accidentally leaked.
  - If the cleaning lady goes on vacation, shares the password with her temp replacement, the temp replacement does something illegal on your computer, guess who will get blamed.

Basic Advice: (Wash your hands and Brush your teeth) (cont'd):

- Don't reuse passwords. A data breach at one website, will mean the criminals will try it other other popular websites.
- Use strong passwords. If you create your own passwords, use strong passwords. No 12345, cat, dog monkey. Use upper- and lower-case letters, numbers, and punctuation symbols mixed. Long passwords, I would not use 4 or 6 characters if allowed, go longer
- Two factor: More on this later
- Keep software up to date. (Router software if you maintain the router) Security updates are often part of a software update.
- Keep backups.

VPNs:

- VPN Virtual Private Network
- “Creates an encrypted tunnel between your device and a private server, hiding your IP address and online activity from ISP’s and Hackers” per Google AI summary
- Helps with privacy. Obscures your location letting you access geo restricted contents
  - But if the company is on to this happening, may just block VPN traffic
- May be of use if using public WiFi or you don’t trust your internet provider
- Many question use in home environment
- Issues:
  - Slows connections, some sites will reject VPN traffic
  - Does not prevent malware installation, won’t prevent malware affecting your machine
  - Most internet traffic is encrypted already, (https)
  - Link to the VPN, and from VPN to website is still subject to vulnerabilities
  - Won’t help if your end website is criminal or even just shady

VPNs (cont'd):

- Can't delve into all involved in choosing a VPN
- Big concern on "Free" – They need to make a profit. So, in many cases the free VPNs will sell your browsing habits to companies for profit.

Data Breaches :

- We are talking about data breaches that happen to companies you deal with on the internet.
- A data breach is a security incident where unauthorized individuals access, steal, or expose sensitive, confidential data—such as personal information (PII), financial records, or intellectual property.
- There is not a lot you can do other than use strong passwords, and Multifactor Authentication (next set of slides), or Passkeys.
- You may read about it in the news, get a written letter from the company, or an email
  - Be sure the email is legitimate. It should address you by name, and should have you check your account by you going to it. Not a click here or call a phone number.
- What you need to do depends on what was taken.

Data Breaches (cont'd):

- Ideally it is something like "only user names and which plan regular or premium information was obtained. No emails, passwords, personal, or financial info was compromised"
- If it says they have your credit card info (worse with CCV) then you will need to contact your bank to cancel and get a new card
- If they obtained your passwords, follow instructions when you log into your account on how to deal with it
- If they got personal and financial information like name, phone numbers, date of birth, address, bank account numbers, credit cards etc., then you need to watch out for loans, mortgages etc. being taken out in your name. If the breached company offers complementary credit monitoring, take it, or if not get it yourself.

Multifactor Authentication:

- Multifactor Authentication is a more generalized application of Two Factor Authentication (2FA)
- Multi-factor authentication (MFA) is a security mechanism requiring users to provide two or more credentials—something you know (password), have (token), or are (biometric)—to verify identity. It enhances security by preventing unauthorized access, even if one factor, such as a password, is compromised.
- There are several ways to get the second authentication:
  - Via your email
  - As a text message
  - Using a software authentication program on something like your iPhone
  - Use a Hardware device. Most plug into a USB port

Multifactor Authentication:

- The email is least secure. If your password and email are compromised, they may use your email to claim to be you. Better than not using MFA
- SMS is better but not fully secure in transit. SIM swapping occurs when the bad guys get your phone company to transfer your SIM to their phone
- Dedicated software apps are more secure. However, you will need to specify this to each website you need a password to log into
- Hardware keys are likely the best. Again, you need to specify this to each website you need a password to log into
  - Examples are YubiKey or Google.
  - They are not that expensive (~$30 to $50ish)
  - If you have a work device, the company will often supply them

Passwords:

- Again, use strong passwords. No dictionary words by themselves, numbers, punctuation, upper, and lower case and so on.
  - Some sites may limit what you can use, so use what you can. If the maximum numbers are 12 and the minimum 4; well, have your password closer to 12.
  - Consider longer numeric passcodes for iPhone or iPads. Use pass phases if you can.
  - Think about going to Settings and tapping Face ID & Passcode (on iPhone with Face ID) or Touch ID & Passcode (on models with a Home button) and turning on features like stolen device protection, short auto lock times, and erase data after 10 attempts.
  - If you want to create your own passwords here is Bart Busschots xkpasswd generator. Let's you use easy to use words numbers and symbols
    - https://www.xkpasswd.net

Passwords Managers:

- Well, it is hard to remember tens or hundreds of passwords and it would help if there was a way to automatically create strong passwords.
- This is where password managers solve the problem. You just need to remember one password for the manager and the manager handles the remainder.
- While there have been paid third party apps to handle this, starting with Mac OS 15, Apple introduced the Passwords App.
  - The app interfaces with Apple's Keychain. Keychain goes back quite a few years back. In Mac OS 11 Big Sur keychain could autofill saved passwords into websites. Passwords app expands and eases access to keychain.
  - Passwords app handles web passwords, (via icloud passwords extension for non safari browsers) WiFi passwords, Passkeys, permeant verification keys, and more
  - You can share limited passwords with people you trust

Passwords Managers (cont'd):

- There are paid third party password manager programs. They are programs like 1password and Dashline.
  - There is a program called LastPass. Opinion here, don't use it based on how they handled a security issue in the past. Trust issue.
- 1Password does have some features that Apple's Password App does not
  - Works on other devices such as Android. Let's you share passwords with these other devices.
  - Save and secure documents (insurance papers and the like)
  - Save and secure other sensitive data that are not passwords. (Drivers license number, Passport number, Credit care numbers etc)
  - Remove vaults when travelling to places of concern

Passkeys:

- Wouldn't be nice to get rid of the problems and issues with passwords? That is what Passkeys do.
- The Fast Identity Online (FIDO) Alliance developed passkeys several years ago
- Uses public and private keypairs. Stored in keychain
  - Migrating to a new device and signing in your Apple account will transfer the passkeys
- The website you are trying to log into uses your public key to encrypt a one time use unique code. Your device uses its private key to decode. Only the private key can decode the unique code. The code is sent back to the to the site to validate.
  - You don't know the unique code so you can't be tricked into giving it up.
  - Passwords are not stored at the site, so if the site is hacked, the hackers don't have anything.
  - The process can determine if a site is fake

Passkeys (cont'd):

- Passkey requirements:
  - iPhone or iPad with OS 16 or greater
    - Two factor ID on Apple Account
    - Face or Touch ID on
    - iCloud Keychain on to save and sync Passkeys
  - Mac with Mac OS Ventura (OS 13) or higher
    - Apple Silicon or Intel machines with T2 chip (2020 iMac, 2018+ Macbook Air, Pro, mac mini 2018+, 2019 Mac Pro)
    - Two factor ID on Apple Account
    - Touch ID or user login
    - iCloud Keychain on to save and sync Passkeys
  - While more and more sites are now allowing Passkeys, not all are. I have Amazon, Google, Paypal, and Yahoo.
  - https://support.apple.com/guide/iphone/use-passkeys-to-sign-in-to-websites-and-apps-iphf538ea8d0/ios

Phishing:

- The biggest way criminals get information from you is by tricking you into giving them it. Phishing
- https://support.apple.com/en-us/102568
- Note the article is specific to Apple products and services But the general principles apply else ware.
- The FTC, Social Security, IRS, Medicare, Local Sheriff or Court official will not contact you via email phone or message out of the blue. Yes, if you have a case with them, they might contact you on that case.
- Above agencies will not ask for gift cards or cryptocurrency as a payment method
- Latest method is asking you to cut and paste programming lines into the terminal or into shortcuts app. On the former, terminal, the latest Mac OS update will now warn of suspicious pastes. This is to get around warnings that exist in the main Mac OS.
- Phishing scams will use urgency to act first without thinking.

Malware:

- Malware includes virus's, trojans, keystroke loggers, ransomware and the like
- Your Mac has quite of bit of protection built in:
  - Since mac OS Catalina (10.15) the APFS file system has your boot hard drive split into a locked system partition and a writeable data partition. While havoc can occur with the data part, the locked systems prevents a lot of malware acting directly on the system
  - Sandboxing: System files, resources and the kernel, shielded from user app space. App store Apps must use API's to access data from other apps.
  - Gatekeeper: All Mac apps must be notarized. App store apps must be signed. Mac will ask about apps downloaded from the internet.
    - If you didn't download it, deny permission to allow the app to open
  - Xprotect: Detects and removes malware. Checks daily for updates

Malware (cont'd):

- iPhone OS and iPad OS has sandboxing, system integrity checking on startup, and can only use signed apps from their respective app stores.
- For iPad and iPhone users don't jailbreak your devices to allow loading of non app store programs.
- For the Mac:
  - Don't install pirated apps, besides ethics, they often contain malware
  - Be aware of download deals too good to be true. (Full Microsoft office or adobe suite for $10) same concern for malware
  - The first time that you open a new app from an identified developer that you downloaded outside the App Store, your Mac asks if you're sure that you want to open it. If you did not download it, say CANCEL
    - Warning may say couldn't identify developer, even more concern, CANCEL
  - Popup warning about malware/virus's during browsing are fake. Do not respond to click here buttons or phone numbers to call. If you seem stuck on the page, force quit the browser (under Apple menu). Hold shift key down when relaunching page. Clear history

Malware (cont'd):

- Third party malware detection software. Not personally a fan of it as with many technical pundits.
  - Can cause issues with instability and crashes, false positives, slowness and the like.
  - Running several different vendors anti-virus at the same time is bad, can interact with each other and cause crashes
- The one I now provisionally recommend is Malwarebytes.
  - https://www.Malwarebytes.com/solutions/free-antivirus
  - Company bought this product several years back. However, since then they really push their other products, and premium paid version of this program.
  - Run the program manually say once a week or slightly more often
- Sometimes see recommendation of running third party anti-virus programs continuously on against hard drives. Good way of wearing out hard drives prematurely

Final Thoughts:

- https://www.bleepingcomputer.com A good site to find security issues with devices
- Bart Busschots Security Bits show Usually every other week on Allison's Nosillacast podcast Some notable security updates flagged, Bart has a professional's viewpoint on stories since he is a **Cybersecurity Specialist at Maynooth University, Ireland**
- Some mac news sites: Macintouch, 9to5 mac, MacRumors, Macworld, and others
- Main stream news, maybe good for Company Breech news, less so on malware. Some sites do get a bit doom and gloom to get folks to click and don't accurately report limits on attack vectors (ie only affects folks running servers, targeted attacks against specific dissidents etc)