Staying Safe with Apple Products

1. **Protect your network**
    - 1.1. Open network (no password required)
        - 1.1.1. Starbucks, etc.
        - 1.1.2. Anyone can join, anyone can sniff
        - 1.1.3. Probably not best to access websites that need passwords
        - 1.1.4. VPN (Virtual Private Network)
            - 1.1.4.1. Encrypts data between your device and the internet
            - 1.1.4.2. Pay a fee for the service
            - 1.1.4.3. May slow down network speed slightly
            - 1.1.4.4. Search App Store for apps (express VPN, etc.)
    - 1.2. Closed network (password protected)
        - 1.2.1. Typically, your home network
        - 1.2.2. Could be sniffed by anyone with the password
        - 1.2.3. Guest networks
            - 1.2.3.1. Runs alongside a wi-fi network with separate name and password
            - 1.2.3.2. Access only the internet, not network devices (printers, file servers)
    - 1.3. Hidden network
        - 1.3.1. Probably not needed; discoverable with right tools
    - 1.4. Best network practices
        - 1.4.1. Firewall on the network
            - 1.4.1.1. Blocks incoming connections that are not a response to a request from someone on the network
            - 1.4.1.2. Allows all outgoing connections and requests
            - 1.4.1.3. Personal firewall probably not needed
        - 1.4.2. Password-protect the network
            - 1.4.2.1. With iOS, easy to share access to network with known contacts
        - 1.4.3. Password-protect the router
            - 1.4.3.1. Prevents access to the device where settings are stored

2. Protect your devices

2.1. Passcodes on all devices, particularly mobile devices

2.2. Implement Touch ID or Face ID

2.2.1. Set up multiple fingers in Touch ID

2.2.2. Require attention for Face ID

2.2.3. Temporarily shutting off Touch ID and Face ID (iOS 11.2 or later)

2.2.3.1.1. On iPhone 5s to iPhone 7

2.2.3.1.1.1. Click the Sleep/Wake (On/Off) button five times in succession

2.2.3.1.2. On iPhone 8 and any iPhone without a home button

2.2.3.1.2.1. Hold either volume button and the on/off button for a second or two until the Power Down screen appears—then let go of the buttons lest you trigger Emergency SOS

2.2.3.1.2.2. Tap the Cancel button

2.3. Know how to use Find my iPhone

2.3.1. Turn on Find my *Device* in Settings > *Your Name* > Find My

2.3.2. Use Find My app on one device to locate a missing device

2.3.2.1. Can also use a Mac or PC via iCloud.com

2.3.3. Use Lost Mode to lock a device, Erase Mode to wipe a device

2.4. Consider access to lock screen

2.4.1. Settings > Touch ID/Face ID and Passcode —Allow Access When Locked

2.4.2. Settings > Notifications > Show Previews when Unlocked to protect the content of notifications

3. Protect yourself

3.1. Accounts and passwords

3.1.1. Every entity wants you to create an account

3.1.1.1. User name is often an email address

3.1.1.2. Password for each account should be unique and strong

- 3.1.1.3. The passwords you need to remember: for your Apple ID and your devices

3.2. Use a password manager

- 3.2.1. Suggests passwords, offers to store and sync login credentials, credit card info
- 3.2.2. iCloud Keychain
  - 3.2.2.1. Settings > *Your Name* > iCloud
  - 3.2.2.2. Keychain data is encrypted in transit to and from your devices and iCloud and while at rest in iCloud
  - 3.2.2.3. Tap/click in user name or password fields to apply login credentials
  - 3.2.2.4. Touch ID and Face ID to access passwords
- 3.2.3. Third party products (1Password, Last Pass, etc.) often offer more features and are good for cross platform devices (e.g., Apple, Android, Windows)

3.3. Two-factor authentication

- 3.3.1. Something you know (password) and something you have (device, key, etc.)
- 3.3.2. An extra layer of protection
- 3.3.3. Used by Apple ID, banks, and others
- 3.3.4. One-time confirmation code delivered on one device (text, pop-up window, third-party app like Authy) entered on a second device

3.4. Sign In with Apple

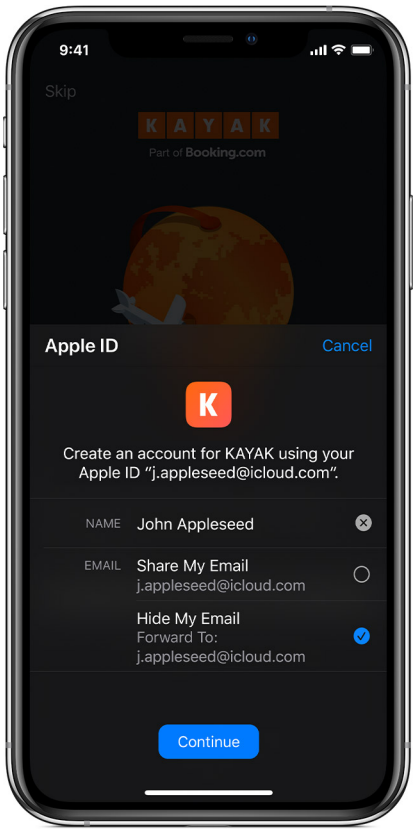
- 3.4.1. Similar to Sign in with Facebook and Sign in with Google
- 3.4.2. Use your Apple ID to create an account on a vendor's website or in the vendor's app
- 3.4.3. Sign in with Face ID, Touch ID, or your device's passcode
- 3.4.4. Requirements: Be signed into iCloud and have Two-Factor Authentication turned on for your Apple ID
- 3.4.5. How it works:
  - 3.4.5.1. Tap the Sign in with Apple button
  - 3.4.5.2. An account will be created using your Apple ID user name

3.4.5.3. Enter your name

3.4.5.4. Enter either your email address, or choose to hide your email

3.4.5.4.1. If you choose to hide your email, a random email address (such as dpdcnf87nu@privaterelay.appleid.com) will created for you and email sent to that address will be forwarded to your personal email address.

3.4.5.5. Tap Continue and authenticate with Face ID, Touch ID, the device passcode, or your Apple ID password



4. Dos and Don'ts

4.1. **Do** be smart and cautious

4.1.1. Pause and think before you act

4.1.2. Who asked for this?

4.1.3. If it's too good to be true, it probably is

4.2. **Don't** rise to the bait of an email phishing attempt by replying

4.2.1. Phishing— an attempt to trick you into giving up some valuable information, such as:

4.2.1.1. Someone in Ghana needs your help setting up a bank account and will pay to millions to help

4.2.1.2. Your bank login credentials have been compromised

4.2.1.3. You need to reset your password immediately

4.2.2. Check the email address of the sender. On the Mac click the name of the sender to see the email address. On iOS, tap the name of the sender twice to see the email address.

4.2.3. If you have an iCloud email account, forward phishing email to reportphishing@apple.com

4.3. **Don't** open an unsolicited or unexpected attachment

4.3.1. Likelihood that it contains a Mac virus is low, but it may trigger a script that could contain malware

4.4. **Do** bookmark this scam/hoax website

4.4.1. snopes.com

4.4.2. Or search the internet for text that appears in a suspicious email

4.5. **Don't** click on links in suspicious emails

4.5.1. On the Mac, hover the pointer over the link to see its destination

4.5.2. On iOS, touch and hold the link to see its destination

4.5.3. If you think the email may be legitimate, type the web address into a browser window to access the website

4.6. **Don't** automatically unsubscribe from marketing emails

4.6.1. If the marketing emails are from a legitimate business, then the unsubscribe link in the email will probably, maybe, eventually work

4.6.2. If the email is from a company you've never heard of, clicking the unsubscribe link probably maybe won't work—and the company will know yours is live email address and send you more email

4.6.2.1. Train the junk filter instead

4.7. **Do** use apps that encrypt your data

4.7.1. For example, Messages encrypts messages that are sent, both at rest and in transit

4.7.2. FaceTime audio and video conversations are encrypted end-to-end so only participants can hear or view them

4.8. **Do** keep sharing settings off until you need them (hotspot, file sharing, etc.)

4.9. **Don't** share passwords and logins

4.10. **Don't** fall for ads that suggest your Mac has been infected by a virus
- 4.10.1. These are often scary ads that pop up in a browser window or in front of a browser window
- 4.10.2. Someone is probably trying to sell you a protection package you probably don't need. Close the window and move on.

4.11. **Do** consider running MalwareBytes on your Mac if something with your web browser seems amiss (e.g., internet searches seems to go to unfamiliar web pages)
- 4.11.1. Free download from malwarebytes.com

4.12. **Do** consider privacy when using a web browser
- 4.12.1. Private windows/tabs won't save your browsing history and asks websites you visit not to track you
- 4.12.2. Prevent Cross-Site Tracking and website tracking
  - 4.12.2.1. Settings > Safari > Privacy & Security
  - 4.12.2.2. On a Mac: Safari > Preferences > Privacy
- 4.12.3. Consider using Duck Duck Go—which does not track you—as your search engine
  - 4.12.3.1. Settings > Safari > Search Engine
  - 4.12.3.2. On a Mac: Safari > Preferences > Search

4.13. **Do** software updates; they usually include security updates and improvement

4.14. **Do** consider ApplePay
- 4.14.1. Requires Touch ID or Face ID on iPhone or passcode protected Apple Watch
- 4.14.2. Credit card info is encrypted and stored in secure enclave on the device

4.14.3. When used at checkout or at an ATM, a one-time encrypted code is transmitted wirelessly; the card number is not transmitted

4.14.4. Faster and safer than using a card with a magnetic stripe

4.15. **Do** take a look at apple.com/privacy for more details about how Apple handles your data and protects your privacy

4.16. **Do** download a copy of Apple's guide to Device and Data Access When Personal Safety is at Risk from https://manuals.info.apple.com/MANUALS/1000/MA1976/en_US/device-and-data-access-when-personal-safety-is-at-risk.pdf

mm
12/18/2020