How do I use my computer safely in today’s world?

Suggestions on how to manage the complexity of the online environment in a non-destructive way.

There is no single silver bullet

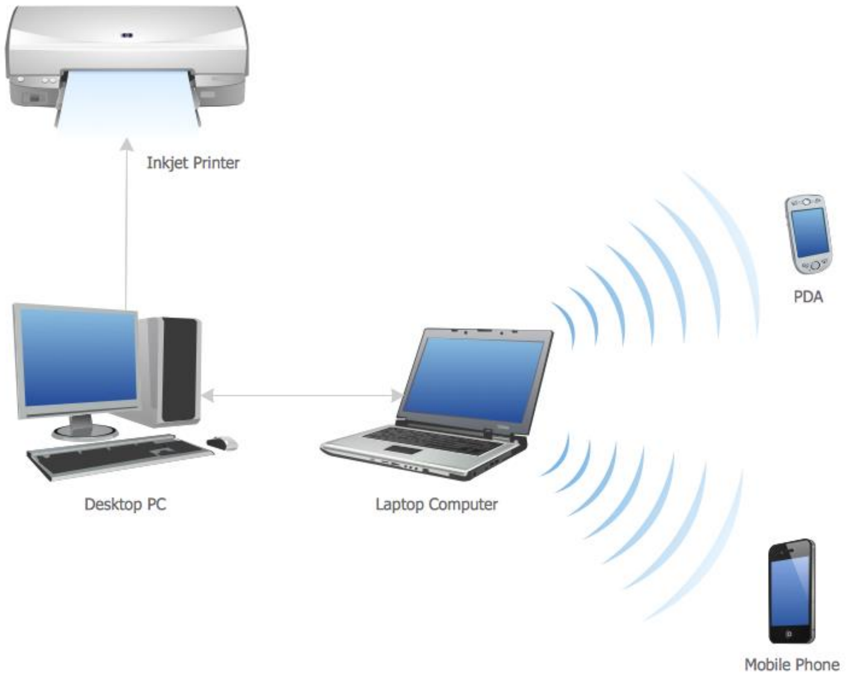
- Think of good online practice like living healthy
  - One meal at McDonald's will probably not kill you. Likewise, using public wifi to look at Wikipedia will probably not give you virus.
  - Conversely, drinking a red bull after drinking a coffee might give you a heart attack. Likewise, a single click i email may cause really bad things to happen.
- Like being healthy, there is more than a single variable that y must address.
  - For health, there is not only diet, but exercise, mental well-being, not being overweight, etc.,
  - For computing, running an anti-virus is NOT enough.
- Do not confuse insecure with less secure
- Generally, convenience and security are inversely related

Things to do on your computer

- Make sure your anti-virus is running correctly (duh)
- Keep your applications / operating systems relatively up to date
- Remove applications and browser extensions that you are not actively using
- Do regular backups so you can recover when/if bad things happen
- Look at task manager to see what is running
- If you use a laptop, consider turning on Bitlocker (will require a Pro version of windows)

Local Network

- Wifi should be WPA
    - WPA3 is currently most secure, but is has compatibility issues
    - WPA3 is required for Wifi 6e
    - Avoid open APs
- If you have an older router, consider upgrading
    - Security will probably be enhanced
    - Newer routers have more processing power / features
- If you have router firmware upgrades, apply them.
- If available, look at connected devices (Disable MAC randomization for the local network)



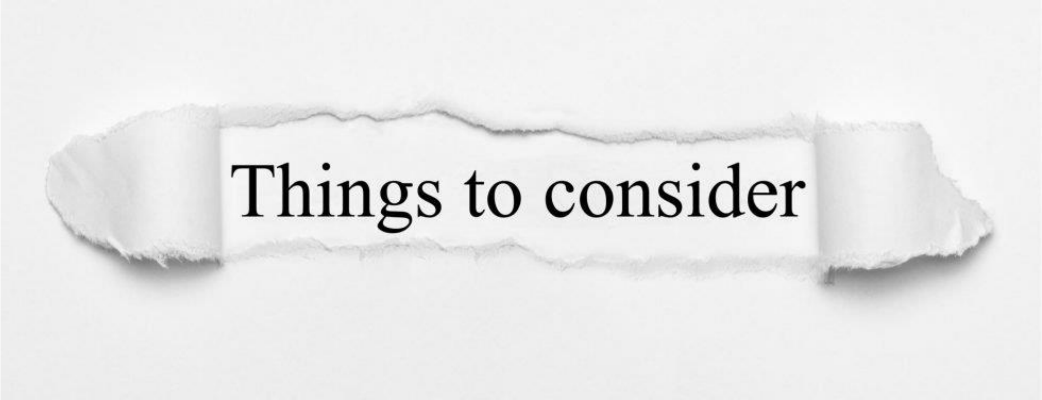
Offsite WIFI

- Consider using VPN
- Avoid connecting to “important” sites unless you trust the AP and the AP isn’t “open”.
- If available, enable MAC randomization
- When in doubt, just use mobile data
    - For devices with only wifi, see if your phone can tether.

- Use a password manager
  - Use passkeys if it is supported
  - Use 2FA wherever it is offered
    - Serious 2FA requires a hardware key and not the phone
      - Asking the device where you are logging in from if it is OK is not a good thing
      - Phones can get lost / SIM jacked / upgraded
    - If 2FA is on, remove other methods of authentication
  - Avoid “security questions” answers that can be found in facebook
  - Change your online passwords at least once in a couple of years
  - Disable password saving in browsers / apps
- Use separate email address/accounts for financial/personal messages
- Obvious stuff
  - Look to see where links go before you click on it
  - Don’t go to unknown sites
  - Be very careful with attachments

Dangers out there

- Phishing (and other methods to get you to do bad things)
  - Be aware of red flags
    - Asking for SSN, bank account #s or any PII (Personally Identifiable Information)
    - Asking for login information
    - Trying to get you to act now.
  - Avoid situations where they contact you.   Try to initiate the contact
  - Consider using alternate email for financial sites.
- Avoid physical attacks
  - Do not insert untrusted thumb drives
  - Do not use untrusted charging stations (or have a data blocker)
  - Be careful of Access Points



Things to consider

- Examine your credit report (annualcreditreport.com)
- Lock/Freeze your credit (go to TransUnion, Equifax, and Experian)
- Getting a separate cell phone for legacy 2FA
- Get a hardware fob and a backup
- Consider minimizing traffic through physical mail *
  - Empty your trashcan
  - Empty Trash and compact mail folders
- Delete credit card info where possible
- Tap credit cards instead of inserting / swiping
- Delete accounts you don’t use
- Examine/clear google/amazon/… stored info

fin