Cyber Hygiene 101

3,900 breaches & 7.9 billion records lost in 2019 alone

How to find out if you have been breached?

- https://haveibeenpwned.com/
- https://breachalarm.com/

What can I do?

- Limit the data you give out
  - Free apps are NOT free!
  - Data mining
  - Password recovery questions
- SSN's are not always required https://www.allclearid.com/when-you-can-say-no-to-providing-your-social-security-number/
- Fingerprints can be obtained legally passwords cannot

Use a VPN

- NordVPN OR VyperVPN
  - Security – Encryption, logging?
  - Who owns it?
  - Where is it located?
  - Cost?
  - Speed?
  - Servers and countries?

Use a secure messaging Application

- Aka Signal

Change your privacy settings

- It's your job to assess what apps should have access to
- Limit the data sharing/mining (does this app need to access all my data?)
- Schedule monthly checkups

EULA – End User License Agreement

- Think twice
- Read it (if you have the time)
- What is the company doing with my data?
- Who are they selling it to, can I opt out?

Enable 2 factor authentication

2 factor apps

- Google authenticator
- LastPass Authenticator
- Microsoft Authenticator
- Authy
- Native SMS OTP
- FIDO tokens
  - Yubico Keys

Cyber Hygiene 101

Private Browsing

- Use privacy extensions to block tracking items
    - Adblock plus
    - Disconnect
    - Privacy badger
    - Duck Duck go
- Use Incognito
- Use Google alternative like Duck Duck go

Use Multiple email accounts

- Divide email purpose and usage
    - One email for banking
- One email for shopping
- One email for junk stuff

Use a Password safe

- Don't save passwords in your browser!
- Stop the password reuse!
    - Single point of failure
- Only Remember one password
- Generate super strong passwords
- Try to keep it local – only backup to the cloud when required
- Never have to remember passwords again
    - **Top Apps**
    - https://1password.com/
    - https://www.passwordcard.org/en
    - Passcodes for IOS
    - Enpass

Email links and attachments

- Do you know the sender?
- Where you expecting an email?
- Does it have a link or attachment?
    - Urgent! = Red flag
    - Avoid clicking links at all costs
        - Hover over links to see what address they lead to
- Login to your account directly without using the hyperlink to verify the details
- https://www.itgovernance.co.uk/blog/5-ways-to-detect-a-phishing-email

Antivirus

- Use an AV if possible
    - BitDefender
    - Sophos
    - Don't Use Free!
- Verify websites when browsing
    - look at the domain name for mis-spellings
    - Look at certificates for authenticity
    - If compromised Power off your machine and call someone who can help