Wi-Fi Security

Securing Yourself on Public Wi-Fi

- Whenever possible, utilize HTTPS instead of HTTP. HTTPS is the encrypted version of a page and will better protect your data.
    - HTTPS Everywhere is an extension available on Firefox, Chrome, and Opera. This extension forces webpages to browse in HTTPS and will notify you if HTTPS is not available for a webpage.
- Utilize a Virtual Private Network (VPN) if this is financially available to you
    - We recommend Privateinternetaccess (PIA) for multiple reasons. PIA does not maintain records on its users or their searches. PIA costs around $50/year and you can connect up to five devices.
- If the only option is Wi-Fi, limit your browsing to casual content.
    - Logging onto your social media, online banking, or email accounts could make them vulnerable to hackers.

Securing your Home Wi-Fi

- Ensure that your router is WPA2 encrypted. This is the best encryption currently available for Wi-Fi routers. Check your box for your device type.
- Disable WPS (if possible)
    - To disable WPS, you may either push a button on the side of the router or log into the router and uncheck the WPS button. Google your router model to find out more.
- Turn firewalls on
- Change default passwords on your routers
    - All routers come with passwords to allow you to remote into the router to change and fix settings. Default passwords are usually easy to guess (i.e. password, admin, adminpassword, etc.)
    - We recommend utilizing our Password handout to better protect your router
- Do not use personal information or antagonizing names (example: FBI Surveillance Van 9) to identify your network