Cyber Security Q & A:

Overall Risk:

- **How much risk does the average person face?**
    - The polling company Ipsos conducted a study that found nearly one-third of Americans claim to be a victim of cybercrime and fraud. The study found that of the One-Third of Americans facing cybercrime, 64% cited credit card fraud, 32% experienced data breaches, 31% were victim of account hacking, 23% experienced banking fraud, and 14% cited phishing attacks. In addition to this study, the FBI received 880,418 complaints about cyber fraud in 2023 alone, which is a record number. The FTC received more than a million reports of identity theft in the same year. This goes to show that with the rise of an interconnected world, also yields a rise in cybercrime.

- **I already use two-factor authentication, make sure not to click on sketchy links or phishing emails, and regularly update my passwords. What should I do specifically to my computer to supplement protection and prevent hacking?**
    - To supplement protection and ensure you are doing everything you can to prevent hacks, you should make sure that your computer is running with the most up to date operating system and make sure that the automatic update setting is enabled. By doing this, you are ensuring that your computer has the most up to date protection for new cybercrime tactics. Also ensure that the built-in firewall is active. This limits what hackers can access if they do get into your system.

- **Are third-party antivirus programs necessary if you keep your computers security features up-to-date?**
    - Brand name computers such as the offerings from Microsoft and Apple come with a variety of protective measures that are akin to that of third-party antivirus software. With that being said, experts advise that it is beneficial to add the layer of protection that third party antivirus softwares offer to supplement the protective measures that are already offered with your computer right out of the box.

- **Does using "incognito mode" or "private mode on my browser protect me from cyber-criminals?**
    - No. When these modes are enabled, the browser is only ceasing to store things such as websites visited. The only real use for these modes is to prevent someone from looking into your browsing history but even then, it is not full proof because an employer or service provider can still view your browsing history if you are using a company network. These modes also lack protection against hackers.

Wi-Fi Risk:

- **Can home Wifi-networks be an entry way for hackers?**
    - Yes, hackers can obtain access to devices that are connected to your home Wi-Fi but experts claim that you can mitigate this by:
        - Refraining from using the default password with the router.
        - Turning on the router's WPA3 Encryption.
            - This blocks unauthorized users from access.
        - Setting up a guest Wi-Fi network which is isolated from the main Wi-Fi network.

- **What are the risks of using public Wi-Fi networks?**
    - Using public Wi-fi networks, whether at the airport or hotel, can increase the likelihood of being a victim of cybercrime. Most public Wi-Fi networks do not use encryption which makes it easier for criminals to attempt to breach the network.

- **Can using a VPN when connected to public Wi-Fi increase security?**
    - VPN's can help increase security. They do this by acting as an intermediary between the device and the website that you are visiting. Online activity cannot be traced back to the user due to the encryption of your transmissions, meaning a cyber criminal would not be able to obtain any information.

- **What are the alternatives to a VPN to mitigate risk when using a public Wi-fi network?**
    - Using a phone's cellular data network is much more secure than public Wi-Fi because it encrypts transmissions much like a VPN. To ensure that you are not automatically connecting to public Wi-fi,

make sure that you shut off the phone's Wi-Fi access when in public. If you want to go online with a laptop, using the mobile hotspot is a good substitute to a VPN that uses it's own private network that only you have access to. The final option would be to use a public hotspot that uses technology called Passpoint. These systems encrypt transmissions and provide other security measures.

Security-Monitoring services:

- **Given that identity theft is on the rise and thieves are able to obtain credit cards, and loans under someone else's name, should I subscribe to a credit-monitoring or identity-protection service?**
    - Credit monitoring services alert you to changes in your credit report which could help catch any suspicious activity. Some also offer tracking to see if your social security number is being used. Identity theft monitoring uses a variety of different ways to protect you from identity theft. Such as, monitoring social media to see if someone is falsely using your name, or appearing falsely on court records.

- **Are there downsides to using monitoring services?**
    - These services can be pricy, costing hundreds of dollars a year in some cases. The main downside is that they do not prevent Identity theft from happening but merely alert you to warning signs that may help prevent it from spreading more severely if caught early enough.

- **What no-cost ways are there to mitigate my risk of credit damage?**
    - A credit freeze can be achieved by going to each of the three major U.S. credit reporting companies (Equifax, Experian, and Transunion) websites and requesting a freeze. This prevents anyone from using your credit reports to obtain a loan or credit card, Credit report monitoring is another no cost way to make sure your credit is not being used by fraudsters.

- **What are some other options to protect your identity?**
    - Being mindful of what information you give out to different websites is a good start in protecting your personal information. For instance, do not give out your social security number unless it is absolutely

necessary, such as government forms. Experts also advise people to be wary about giving out their birth date on websites as it is often used by hackers when trying to get access to your internet footprint.

Passwords and Biometrics:

- **What makes a password hard to crack? What is a good way to remember passwords without writing them down?**
    - Strength is determined by a password's length, unpredictability, and complexity. Length creates complexity by its very nature. A good way to make a password unpredictable is to make sure the password is not connected to you in any certain way. Often people like to use a significant birthdate or their own for number purposes. This is a very predictable practice and should be avoided. For the strongest passwords, it is advised to use a random sequence of letters and numbers, however this makes passwords harder to remember. To combat this issue, a password manager is the easiest way to keep track of all your passwords. Not only do these password managers store your existing passwords, but they also create new ones that are unique and unpredictable.

- **What else can I do to protect my passwords?**
    - A good first step in protecting your passwords is to avoid using the same one for different websites or accounts. This allows hackers to gain easy access to multiple accounts if they can crack the password. Another way to protect your password or login is to create a unique username if the website allows you to generate your own. This makes it harder to access your account if the username is unpredictable. Perhaps the most secure way would be to us a two-factor authentication app. These apps make sure that the person logging into the account is actually you by using a unique code to log you in.

- **What are the pros and cons of biometrics, such as face ID or fingerprint readers?**
    - Experts claim that using biometric features such as a facial scan or fingerprint is much more secure than a standalone password because biological features can not be hacked or guessed like a password can.