Milestone: Company Policies - Cybersecurity

Research & Learn

1. What are **common cyber security threats** in a remote work environment?
Common cyber security threats in a remote work environment include falling for fake emails, as everything is online and remote it slows down the pace to corroborate the information. It could potentially lead to many workers falling for these attacks and surrendering confidential information about the company to these attackers. Other common cyber security attacks include having easily guessed and common passwords which remain the same across all platforms. This risks the entire company's information as if the password is leaked it could potentially allow access to all of the platforms they use.

2. What are **best practices** for keeping your devices and accounts secure?
Best practises to keep devices and accounts secure is utilising strong passwords which pass multiple strength checks and having two factor authentication enabled.

3. Why is it important to **lock your computer** when away from your desk?
As anybody can access all the files and passwords if the computer is left unattended to.

4. How should you **handle phishing attempts and suspicious links**?
Checking if it is coming from a valid and sensible address, if they are not it is best to not open the links as it could lead to the attacks occurring. Filtering emails to ensure that no phishing emails are present in the inbox.

5. What makes a **strong password**, and why should you use a password manager?
A strong password includes a mix of alphabets(both upper case and lower case), numbers and characters, and which passes all the security measures. It is important to use a password manager as it helps store all passwords in the same place, notifies if a password is leaked or is used in multiple websites as well. It is a much organised and secure way to store passwords.

6. Why is **two-factor authentication (2FA)** important, and when should you enable it?

Two-factor authentication is important as it adds another layer of security when logging into other platforms. It adds another level of verification ensuring that it is only you who is accessing your account. It should be enabled as it makes your account less likely to get hacked or be part of attacks.

📝 Reflection

1. What security measures do you currently follow, and where can you improve?

The security measures I currently follow are having strong passwords which include various different characters, using a password manager and regularly updating my passwords if they are leaker, moreover I also have two-factor authentication enabled for some platforms.

2. How can you make **secure behaviour a habit** rather than an afterthought?

I can make secure behaviour a habit by knowing all the serious consequences that can be a result of inefficient practises for securing my information online. By doing so, I will actively ensure that I am following all measures routinely as opposed to once in a while.

3. What steps will you take to ensure your **passwords and accounts** are secure?

As I already used password manager and two-factor authentication, I will definitely enable two-factor authentication on all my platforms as opposed to only a few. Moreover, I will keep up my habit of regularly updating any passwords which have been part of leaks.

4. What would you do if you suspected a **security breach** or suspicious activity on your account?

I would firstly change my password, and then contact the organisation to inform them about my current issue and what steps to take next to secure my account.