Cyber security awareness involves understanding threats like phishing and malware and practicing good digital habits such as using strong, unique passwords, keeping software updated, and being cautious of suspicious links and attachments. Key practices include enabling two-factor authentication, using a password manager, and regularly backing up data to protect against data theft and unauthorized access.

General best practices

- **Use strong passwords:** Create strong, unique passwords for all accounts and use a password manager to help manage them.
- **Enable multi-factor authentication:** Use two-factor or multi-factor authentication whenever available for an extra layer of security.
- **Keep software updated:** Ensure your operating system, applications, and security software are always up to date to benefit from the latest security patches.
- **Back up your data:** Regularly back up important data to protect it in case of a cyber attack.
- **Be wary of unsolicited communication:** Do not click on suspicious links or download attachments from unknown or untrusted sources, such as in emails or social media.
- **Use secure networks:** Avoid using public or insecure Wi-Fi networks for sensitive activities, as they can make you vulnerable to attacks.

Protecting your information

- **Avoid oversharing:** Be mindful of how much personal information you share online and with whom.

- **Limit access:** Grant access to sensitive information only to those who need it and limit administrative privileges on devices.
- **Be cautious with financial information:** Never share your credit card number, CVV, or OTP over phone calls, SMS, or messaging apps.
- **Protect your devices:** Install antivirus and antimalware software on your devices and keep it updated.

Recognizing and recovering from attacks

- **Identify phishing attempts:** Be cautious of emails that ask for personal or financial information or contain suspicious links.
- **Spot malware indicators:** Watch for suspicious pop-ups, slow performance, or unexpected program behavior that could indicate malware.
- **Report suspicious activity:** If you suspect an attack, report it to the appropriate authorities, such as the FTC at ftc.gov/complaint.
- **Check financial statements:** Monitor your credit card and bank statements for any unauthorized charges and contact your bank or credit card company immediately to report them.