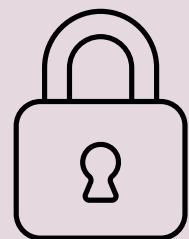




BASIC DIGITAL SAFETY

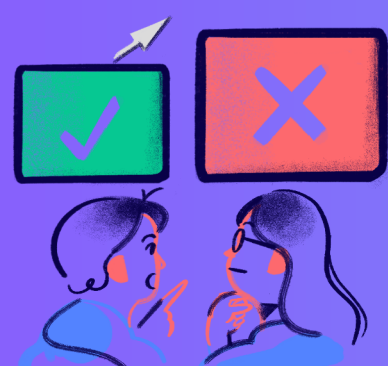
CREATE STRONG PASSWORDS



Passwords are one of the biggest weak spots in cybersecurity. People tend to choose passwords that are easy to remember, making it easy for hackers to decode with their hacking software. Another common practice using the same password for multiple sites leading to further data risk. Use a strong password by mixing letter cases and using symbols and numbers. Do not use your name or date of birth or memorable dates which are easy to guess.

TWO FACTOR AUTHENTICATION

Enable two factor authentication (2FA), for example a code sent to your phone or email. If someone enters your password they cannot access it without extra verification.



DISCLOSING PERSONAL DATA

Be careful about sharing your personal information online. For example, do not disclose your location data on social media. Sharing this information makes it easier for strangers to track you and find sensitive data, making you liable to stalking or identity theft.



USE SECURE WI-FI NETWORKS



Avoid using public Wi-Fi for sensitive activities like online banking. Use a secure, private network, or a VPN (Virtual Private Network) to encrypt your online activities and protect your data. Treat all public Wi-Fi with suspicion, try to verify it's a legitimate wireless connection.

BEWARE OF PHISHING SCAMS



Cyber-criminals will try to trick you by sending emails, attachments or links to websites. Always verify the sender's email address or website before clicking on links or downloading attachments.

DOWNLOADS / SOFTWARE



Cyber-criminals often try to gain access to your hardware by using malware, which is a "backdoor" into your network. Malware may be disguised as something harmless, such as an app or website, tricking you into installing them. This makes your machine susceptible to malicious access. Avoid installing unrecognised programs or clicking suspicious links.