

Use secure networks

When using public networks always be careful because they might not all be as secure as you think! always consider using a Virtual Private Network which is (VPN) for short. This helps when you access sensitive information over a public network. (BBC,2024)

Scams

Always be careful when receiving unsolicited emails, sms or phone calls and ask for personal or financial information. (BBC,2024) always at all times verify the identity of the caller or sender before you actually pass on any type of information because it could lead in the receiver being part of a scam.

Be cautious with links or attachments

Always try your best to avoid clicking, accessing or subscribing to any suspicious links or installing any attachments from sources you do not know. as they would probably contain a type of malware or a type of phishing attempt.

Secure your devices

always use a pin or password on all of your devices such as phones, tablets or computers.also always make sure that they are strong and hard to guess, it should contain a mix of letters and numbers so that it is more secure.(Digital Everyone, 2024)This will prevent unauthorized users from accessing your personal files and data

Use 2-FA

Use two factor authentication, even if your passwords end up compromised you will still have an additional security step which will stop unauthorized users. You would either receive a code to your sms or email which you will need to comply with and identify that you are the person that is trying to access the files or data.

Back up your data

Always back up your data ensuring that you back up your data for cases such as you getting hacked and therefore you would not longer have access to your data or either you lost your devices or hardware and therefore you just need another version.

Stay informed

Always stay informed about new cyber security's by joining and subscribing to newsletters, forums or blogs to always be informed on how to stay safe or new threats that might be going around so that you are one step further from protecting yourself.

Update software

Regularly update your software to ensure that everything is running up to date and that the newest security and firewall exist in your device. (Digital Everyone, 2024) This will help you be limiting threats and viruses that might enter your device.

Always only use trusted devices for work

The amount of trust you put into a device should be based on how much information it takes from you. Meaning that if you put too much trust into a device which has access to your data it could lead to unwanted share of data

Reference :

BBC (2024).8 Top tips for staying safe online . Available at:<https://www.bbc.com/ownit/the-basics/8-tips-for-staying-safe-online>. Accessed on:10/04/2024

Digital Everyone (2024) Ten tips for staying safe on the internet Available at :<https://digitalinclusion.salford.gov.uk/resources-learning-jobs/top-tips/ten-tips-for-staying-safe-on-the-internet/>. Accessed on: 10/04/2024

Marian Faramita

student Id Number :2023148791