

• TOP FIVE TIPS TO * STAY SAFE ONLINE

Maxamed Ahmed
2235329
LCLM4002
GROUP 1



1- Use Strong, Unique Passwords:

You need to Set strong passwords for all your accounts. The password is strong when you use any of the combination out of uppercase letter, lowercase letters number and special characters. Do not choose things that could be easily guessed, like birthdays, names etcetera. Using a password controller can help you manage strong passwords for your private accounts, and save them securely to avoid passing providing your other services.



2-Spell Out Two-Factor Authentication

Creating Two Factor Authentication helps to improve security by adding an extra verification process in addition to just a password; This could be a text message code, email confirmation or biometric verification such as fingerprint. This obviously blows, but given that you enabled 2FA a hacker would need more than just your password to get into an account even in this worst case scenario.



3-Be aware of Scams:

Simply put, a phishing scheme will pretend to be a real entity where you mandatorily have to release your personal data. Make sure any emails you got have the same tone professional, friendly e-mail addresses they are using and give bad faith email requests asking for sensitive user informations. Avoid ever clicking on anything trusted people Phishing, for example terrible spelling and grammar as well as urgent requests for your personal information



4-Use Secure Connections:

When you are on a site reading about something controversial or doing any other transaction, learn how to read web addresses and determine if that page is using encryption to safeguard your information from being stolen. Only Slovakian regional unwanted guests way to safely use free public WiFi networks ever possible!



5-Keep Software Updated:

Always Keep Your System-Wide OS, Web Browser & App Software Up-To-Date? These usually come with essential safety updates that seal available vulnerabilities for hackers to exploit. Keep personal devices up-to-date in the background automatically where possible and all apps when it makes sense to! It protects you from malware, ransomware and whatever sort of exploit-based attack that might come your way leveraging the unpatched software.

References: CSC (2023) title of the webpage. available at:<https://csc.gov.im/advice-guidance/10-online-safety-tips/> (Accessed: 08 April 2024).