# #BeCyberSmart: Mobile Security Tips to Keep Your Device Safe

You might have been spending a huge amount of time every day on your mobile phone and not know it, whether checking your social media accounts, emails, and messages, scrolling through your gallery, or making financial transactions on your phone. While you may probably know how to secure your desktop and laptop, keeping your mobile phones and tablets secure requires a different approach. #BeCyberSmart by openly navigating your device with a confident protection by following these security tips.

- **Keep your mobile phone and tablet locked** – Secure your mobile phones and tablets by using a passcode, pattern, fingerprint or face recognition. For Android users, you may go to ***Settings > Lock Screen*** to update or change your current lock screen settings. iOS users can find these functions in the ***General*** options.

- **Keep your operating system and apps up-to-date** – Keeping your operating system and apps up-to-date does not only add new features but also improve your phone's security. It is recommended to regularly update your OS and apps as soon as an update is available. To check if your phone's OS is up to date, go to ***about phone*** or ***general*** and click ***system updates*** or ***software update***.

- **Be wary of connecting to a public Wi-Fi** – Always remember that whenever you connect to a public wi-fi, your device is also open in public. If you must use a public wi-fi, be sure to use a Virtual Private Network or VPN to encrypt your activity to possible threat actors. Or better not to connect.

- **Download apps from trusted stores** – Only download apps from the official app stores and make sure to check the developer, ratings and reviews of the app that you like to download. It is also recommended to read the app's privacy policy to check what features on your phone the app will have access to.

- **Do not jailbreak or root your phone** – Rooting your phone means modifying the file system that will allow you to access read-only files or parts of your phone. Though there are advantages in rooting your phone, you may also want to consider the security risks – rooting your phone puts you at high risk of potentially being infected by malware.

- **Backup your data** – Most modern phones now allow users to synchronize data with other devices for backup purposes. Ensure that a regular back up plan is in place and choose the automatic back up to take the hassle out of doing it manually.

- **Install Anti-Virus Software** – Consider installing anti-virus software on your mobile phones and tables for additional security against malware and other viruses.

- **#BeCyberSmart** – Do not open attachments from unverified sender on your email or click any ads on your installed applications.