

# Security tips when using your mobile phone

Dear Valued Customer,

We use our Smartphones/tablets for virtually everything, from casual Web browsing, connecting to social media, and streaming movies and music, to banking to online payments and so much more.

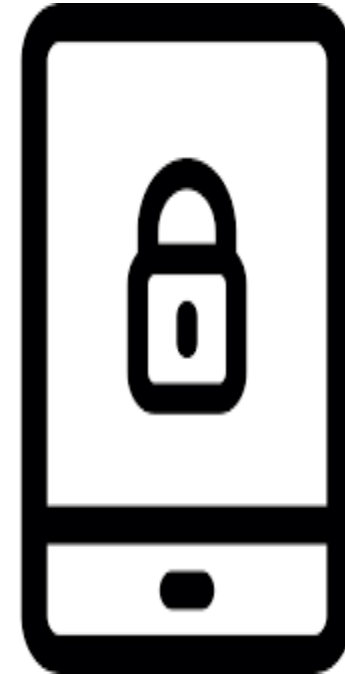
With their increased usage, especially during these times when the World is hit by the COVID-19 pandemic, Smartphones/tablets are faced with cybersecurity and data privacy challenges if not properly used.

Below are some general security tips which will help to secure your mobile devices.

# Security tips when using your mobile phone

## Always lock your phone when not in use

- Make use of Automatic Lockout feature
- Or set up Touch ID
- Or set up Facial Recognition
- Have a unique PIN as an alternative



# Security tips when using your mobile phone

## Avoid connecting to public Wi-Fi networks



- Public Wi-Fi are in general less secured networks and are easily exploitable by cybercriminals. Always set your phone to forget networks when no longer in use.
- Public Wi-Fi should not be used to transact online, like Internet/Mobile Banking. In extreme cases, use “virtual private network” which encrypts data transmission
- Configure your phone to automatic turn on/off wireless by using location-aware smartphone app

# Security tips when using your mobile phone

## Do not open/reply to suspicious email or SMS links

- Beware of suspicious or unknown email senders.
- Embedded URLs in suspicious email or SMS should be deleted



# Security tips when using your mobile phone

## Never make use a common password for all Email Accounts

- This practice makes all your email accounts vulnerable if one account is hacked
- Never make use of the 'Remember Password' feature offered on internet browsers

# Security tips when using your mobile phone

## Always back up your critical data

- Make sure the feature 'backup and sync your data' is enabled, in case your phone is lost or stolen

# Security tips when using your mobile phone

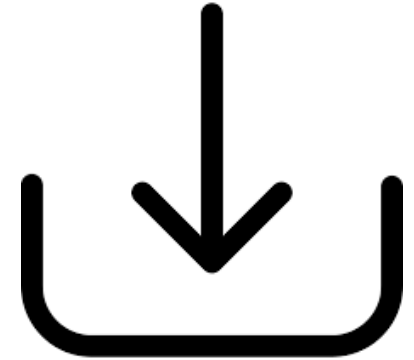
## Always update your phone Operating System when prompted

- These security updates often include important system vulnerability patches and are meant to protect your device and data

# Security tips when using your mobile phone

## Do not download Apps from unknown websites

- Always make use of official apps like Google Play or Apple Apps Store/iTunes for software downloads
- Downloads from non-trusted source can be re-directed to fake websites, proliferating malware or spyware onto your devices



# Security tips when using your mobile phone

## Install antivirus software on your mobile device

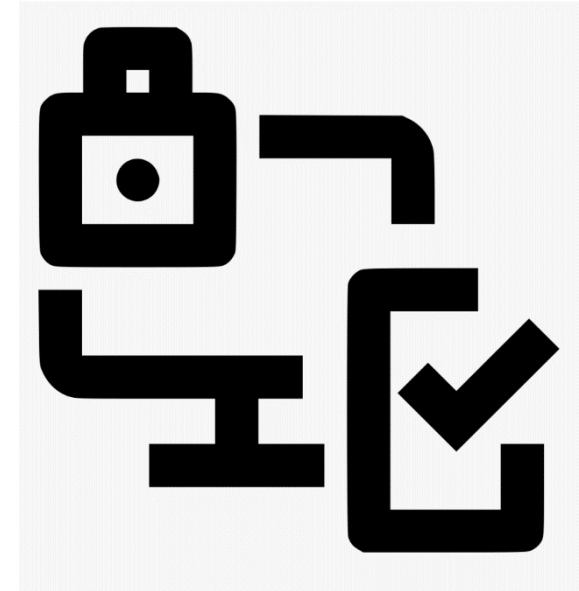
- As a best practice for any mobile devices (phones, tablets, or other), consider installing an antivirus software for additional security against malwares/viruses



# Security tips when using your mobile phone

## Enable two-factor authentication (2FA)

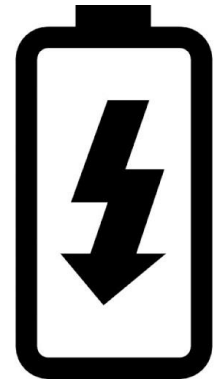
- 2FA adds another layer of security to your mobile devices
- It should be enabled for your key accounts, like mobile banking and peer-to-peer payment apps



# Security tips when using your mobile phone

## Avoid public charging stations unless there is an emergency

- Your device may be hacked through fake charging stations scams known as “juice jacking”



# Security tips when using your mobile phone

## Turn on remote tracking in your mobile device settings

- Apple users have Find My iPhone and Android users can enable Find My Device to see the last known location of the device
- Both features allow you to remotely wipe your smartphone data if stolen or cannot be retrieved

# Security tips when using your mobile phone

## Turn off Bluetooth and Near Field Communication (NFC) when not in use

- Keeping your Bluetooth and NFC 'ON' can lead to interception attacks and is not recommended to effectuate payments through such type of connectivity
- Be careful when pairing devices. Never accept request from unknown devices



# Security tips when using your mobile phone

## **Regularly audit your Apps to see what information are being accessed**

- Be cautious about what permission you grant application during download and installation as your phone data may be compromised

# Security tips when using your mobile phone

## Do not “Root” your Android or “Jailbreak” your iPhone

- This is a process which gives you complete control on your device through privileged access. It also removes many of your phone default security features that the manufacturers put in place
- In some instances, rooting even voids your phone warranty

