

It may surprise you to know that the biggest risk to your mobile devices and the data they hold is probably YOU!



We carry our mobile devices everywhere and use them for almost everything. They have all our data and keep us connected through apps to everything from banking to health care information to all our IoT devices – like household appliances, lights, and even the front door!

But convenience comes at a risk - one that increases the more connected you are and the more data you hold. Think about all that data accessible in one place - all held in your hand. You could forget your phone in a restaurant; leave it on the counter while paying for purchases; forget it in a cab or your car, visible for anyone walking by; or in a grocery cart after loading your car. It could fall out of your pocket or purse. Are you feeling lucky?

You can take some simple steps to keep your mobile devices safe and all the data they hold working for you and not the bad guys – no luck involved.

### Protection from YOU:

- Enable automatic screen locking that requires a fingerprint or a passcode that only you know.
- Encrypt your device/data - it may already be the default, but be sure to verify it's enabled.
- Turn off Wi-Fi and Bluetooth features when not in use.

- Turn off all location tracking services when not using them.
- Be alert to phishing – whether from email messages, text messages, or links from someone you don't know. Stop and think before you tap, click, or reply.
- Avoid using autofill when on websites or in apps that fill in user names and passwords for you. Or, if you do use it, only turn it on when needed, then turn it off as soon as possible.
- Avoid using public Wi-Fi and connecting to someone else's network you don't know. Hackers can easily intercept your transmissions and activity – exposing sensitive information.
- Consider using a Virtual Private Network (VPN).VPNs encrypt your connections over the internet.
- Log off your mobile apps after using them, especially if they are linked to one another, like Google apps.
- Setup a "remote wipe" feature in case your device is lost or falls into the wrong hands when unlocked.

### Protection for your devices:

- Keep your mobile device operating system updated regularly.
- Install anti-virus software.
- Back up regularly - they not only backup the data but also the mobile device's configurations.