AWARE | SECURE | RESILIENT

5 STEPS TO CYBER-SECURITY:

5 KEEP YOUR DEVICES SAFE

Businesses are using mobile devices more and more to perform work tasks. This can introduce risks, so it's important to ensure the appropriate security measures are implemented.

The following recommendations should be considered when providing mobile devices to your staff members.

USE PASSWORD/PIN PROTECTION AND OTHER SECURITY MEASURES

- Every computer and mobile device should be protected with a password or PIN. This will protect your data when working outside the office.
- Passwords should be long and not easy to guess. The UK National Cyber Security Centre (NCSC) recommends using three random, but memorable, words. By using a mixture of upper and lower case letters, numbers and special characters (£, $, !), the password strength increases, e.g. B1cycleSh0ePark!
- Additional security measures such as facial recognition and fingerprint scanning may also be implemented.
- Consider setting up device encryption or encrypted storage areas on your devices. This will further protect your data in the event of the phone being lost or stolen.

UPDATE AND UPGRADE DEVICES AND SOFTWARE

- Regularly check that your devices and apps are up to date. Security vulnerabilities are often patched by updates.
- Avoid downloading old apps or apps from third party app stores as these may no longer receive updates or could even contain malicious code.
- It is recommended to have a list of approved apps. This makes it easier to keep track of apps available to staff which can be monitored and updated when required.

DEVICE TRACKING AND REMOTE WIPING

If a device is lost or stolen, you will be able to find it or delete any sensitive data if you have device tracking and remote wiping features enabled.

- Most of the latest branded smartphones and tablet devices have tracking and remote wiping capabilities built in to them. You can usually find these features in the security settings of your device to set it up.
- Phones linked to a Google account may also allow you to perform tracking and remote wiping from your Google account settings.

USE SECURE CONNECTIONS

- Don't connect to public Wi-Fi hotspots when sending or receiving sensitive data. Use 3G or 4G connections (with tethering), or use a Virtual Private Network (VPN).

  A VPN is a service which encrypts your data before sending and receiving data.

  Tethering is a feature found in most smartphones. It provides 3G/4G Internet access to connected devices such as your laptop. This may also be referred to as a feature called 'Mobile Hotspot' which acts like a wireless router.
- Ensure you choose strong passwords for your mobile device's hotspot access.

If you have any concerns, or have been affected by a cyber-related issue, report it to the Office of Cyber-Security and Information Assurance (OCSIA) by submitting a Cyber Concerns Online Reporting Form at www.gov.im/ocsia.