AWARE | SECURE | RESILIENT

5 STEPS TO CYBER-SECURITY:

2 MALWARE PREVENTION

Malicious software (malware) is a continual threat to any computer and device. Without adequate protections, it won't take long for a computer to become infected. Malware can cause untold damage to computer systems and networks; recovery can be expensive and in some cases impossible if adequate security measures have not been implemented.

The following guidance covers basic recommendations to reduce the chance of a malware infection.

INSTALL AND TURN ON ANTI-VIRUS AND FIREWALL SOFTWARE

- The latest Operating Systems (Apple iOS, Microsoft Windows) now come with their own anti-virus software already installed, so make sure it is turned on for all computers and devices. It is also recommended to regularly monitor the status of your anti-virus software to ensure it is still running. The features offered in these and other free versions of full anti-virus software can be very basic in comparison to their premium counterpart, however, it is much better to have one installed and turned on than not to have one at all. Organisations should consider researching and purchasing a fully-featured anti-virus solution. Premium anti-virus software typically comes with additional security features such as anti-phishing and credit card theft prevention.
- Firewalls act as a barrier between your network and the Internet, and can block numerous threats before they become an issue. Basic firewalls typically come with the latest Operating Systems – ensure your firewall is turned on. Your anti-virus software may also have a firewall built in.
- Ensure your firewall and anti-virus software is regularly updated, and the latest virus definitions are being used. Set these to automatically update where possible.

RESTRICT SOFTWARE DOWNLOADS AND INSTALLATIONS

- Organisations should consider having an approved list of software for staff to use in their daily tasks. This makes it easier to keep track of and maintain so that they can be regularly updated.
- Staff members should be prevented from using third-party apps stores and unknown sources to download and install software on their computers and devices. Software from unofficial sources can contain malware, even if the application works as expected, there may be malicious code hidden within it.

MAINTAIN YOUR SOFTWARE AND DEVICES

- It is important to keep track of the software and devices you have within your organisation. This will allow you to update, patch and upgrade all relevant software and devices in a timely manner. Allowing staff to install unapproved software may mean that it goes unmaintained and result in a security vulnerability being exploited.

STORE AND TRANSFER YOUR DATA SECURELY

- Consider encrypting and password protecting your sensitive and confidential data when storing and transferring files. Plenty of tools are available to choose from to secure your data for transfer to third parties and others within the organisation.
- Consider disabling USB ports and CD drives, and instead provide staff with a secure file sharing area to transfer data internally on the network. There are also many lowcost online file sharing services available that can be configured securely and allow for quick and easy access to shared files.

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//cyber-concerns.