AWARE | SECURE | RESILIENT

5 STEPS TO CYBER-SECURITY:

5 topics to consider for protecting yourself from the most common cyber attacks.
These are easy to implement, low-cost and could help to prevent both minor and major incidents.

1 PROTECT YOUR DATA

Strong passwords and additional account security measures are an effective way to prevent unauthorised access to computers, devices, networks and data.

- Keep all your devices secure using password or PIN protection.
- Use strong passwords, resetting them when required, and changing default passwords.
- Use multifactor authentication when available. This provides an additional layer of security to your accounts by confirming the identity of the user.

2 PREVENT MALWARE

Malicious software (malware) can cause untold damage to computers, devices and an organisation's data. The following steps will assist greatly in preventing malware attacks.

- Ensure your anti-virus software is turned on, kept up to date, and regularly perform system scans.
- Don't download or install third party software and apps from unknown sources.
- Patch software regularly, and set software to update automatically, if possible.
- Encourage staff to only transfer files over the network, via email or secure cloud storage, rather than removeable media.
- Always keep your firewall turned on.

3 AVOID PHISHING ATTACKS

Phishing attacks are scam emails, usually masquerading as a trustworthy person or organisation. They might ask for personal information, or provide links and attachments to malicious websites or malware.

- Don't browse the web or use email on accounts with administrator privileges.
- Perform anti-virus scans for malware and change passwords if you suspect or identify an attack or compromised account.
- Is the sender's email address legitimate? Is the email unexpected or suspicious?

4 BACKUP YOUR DATA

Backing up your data regularly and testing restoration will reduce the impact and inconvenience of any data lost from theft, physical damage or malicious software such as ransomware.

- Consider complete backups of systems and data, but if this is not practical, decide what data your organisation needs to keep running and how often this data should be backed up.
- Store your backups in a different location to your original data – consider using the cloud.

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.

- Protect your devices using a password/PIN/fingerprint recognition.
- Set up device tracking and remote wiping to prevent your data being compromised if you lose your device.
- Keep all your devices and apps up to date.
- Use 3G or 4G, rather than connecting to public Wi-Fi hotspots when sending or receiving sensitive data.
- Out of date devices that no longer receive updates should be replaced.

USEFUL RESOURCES

For more information about these five topics, look for the 'Resources for Businesses and Charities' section in our OCSIA Knowledge Base

If you have any concerns, or have been affected by a cyber-related issue, report it to OCSIA by submitting a Cyber Concerns Online Reporting Form at www.gov.im/cyber-concerns

Office of Cyber-Security
& Information Assurance
Oik son Shickyrys Lectraneagh as Sauçhys Fysseree

www.ocsia.im

@cyberiom

IOM Government Office of Cyber-Security
& Information Assurance