Information Security Top Tips whilst Homeworking

The Office of Cyber-Security & Information Assurance (OCSIA) is an advisory office sitting under the Department of Home Affairs. OCSIA provides advice and guidance for data protection and information security matters within Government, the private sector and general public.

The following advice has been produced for staff to best protect themselves and Government information whilst homeworking.

Physical security

The first tip is to make sure your work devices are physically safe, and that you avoid offering unauthorised views of confidential information. Here are a few ways to support physical security whilst homeworking:

- If you need to leave your home for supplies or other reasons, make sure your work devices are either shut down or locked—including any mobile phones you might use to check emails or make work phone calls.
- If you live with others, be sure to lock your computer even when you step away even for a short time. Don't tempt your family members or others you live with by leaving your work open. This is true for the workplace, so it is imperative for homeworking.
- Do not leave your laptop or other devices in your car.
- If you don't have a separate work space in your home, be sure to collect your devices at the end of your workday and store them somewhere out of sight. This will not only keep them from being accidentally opened or stolen, but will also help you to separate your work life from your home life.
- Consider installing a privacy filter on your device(s). This is a shield that attaches to your screen and makes it difficult to read what is on your screen unless you are right in front of it. This should also be considered if, for instance you are working remotely from a Café or Airport.

Security Settings

- Make sure that you keep your device up to date with security updates and that you have anti-virus software installed.

Use of passwords

- Ensure your computer and devices are protected with a passphrase or other security measure.
- Shut down your laptop or work mobile phone when you have finished using them. This helps keep information safe if the devices are lost or stolen.

Information Security Top Tips whilst Homeworking

Secure your wi-fi

- Ensure that you are using a strong password for your Internet router, using at least WPA2 for network encryption – check the instruction manual if you are unsure.
- Use a Virtual Private Network VPN when using a wi-fi network that does not belong to you.

E-mails

- Do not use personal email accounts to send or receive work related information. Be careful not to mix work and personal emails.
- Only use Isle of Man Government approved methods for communicating and sharing files.
- Be wary of "phishing" emails. Do not open emails from unknown sources, download attachments or click on links unless you are sure that they are genuine.

Conference Calls (MS Teams, Zoom, etc)

- Take care when sending out the meeting invitation and ensure it only goes to those who are invited.
- Do not record meetings.
- Be mindful of the audience and tailor content accordingly.
- Clear your screen before presenting to make sure that anything confidential, personal or commercially sensitive is closed down.
- Close down meetings when you have finished to prevent accidental sharing of your desktop activity.

Security Awareness Training

- Ensure that you have completed the Security Awareness Training on E-Learn Vannin.
- Ensure you have read and familiarise yourself with the requirements of the IT Acceptable Use – Staff Handbook.

For more information and advice on information security in the workplace and homeworking, contact OCSIA by email (ocsia@gov.im) or by phone (685557).