POLICE DIGITAL SECURITY CENTRE ADVICE GUIDE

Do's and Don'ts on using removable media

Removable media, such as USB devices, external hard drives, CDs and memory cards, are frequently used by businesses to store data and information. However, they pose a risk of allowing malware to be introduced into a device/system or exporting sensitive data out of an otherwise secure network, whether it is done deliberately or accidentally. Every business must have clear guidelines for the handling of removable media, compatible with proper security controls to protect the organisation's data.

Here are PDSC's Do's and Don'ts when using removable media.

Do's

1. Develop and implement a security policy to control the use of removable media. This ensures your staff are informed of all the responsibilities implicit in the use of removable devices at work. Consider including this in staff's induction training.
2. Limit the use of removable media. When using removable media to support a business requirement, allocate devices to employees on a case-by-case basis. By restricting the use of removable media you are protecting your network from a potential breach.
3. Keep an inventory of all removable media and a record of users. Equally important as identifying who has been issued with a removable device is recording when it has been returned. Review this list regularly to be certain of the whereabouts of your devices and where your business data is stored.
4. If sensitive data is stored on removable media, the device should be encrypted. If encryption is not possible, ensure that the device has appropriate physical protection e.g. is stored in a secure cabinet.
5. Rigorously manage the reuse and disposal of removable media. Appropriate steps need to be taken when removable media is to be reused or destroyed to ensure that previously stored data becomes inaccessible. You will need to consider how to effectively sanitise a device depending on the sensitivity of the data it previously held.
6. It is important to scan all removable media for malware. This should be done automatically when any device, whether old or new, is introduced into the network system.

Don'ts

1. Never connect any removable media device to your computer that you do not trust or recognise. These devices may be carrying malware and, if connected, it could infect not only the device but the whole network.
2. Do not leave removable media devices unattended. Lost or stolen devices could result in the loss and/or compromise of your data stored on it. Always store removable media in a secure place.
3. Do not store work data on your personal devices. ALWAYS keep your personal and work devices separate.
4. Do not use removable media as a default method to store or transfer information between devices, especially when dealing with sensitive data. Consider using physically secure data back-up, such as corporate storage or cloud-based storage.