Wiltshire Police

Cyber Advice on Removable Media

This document will outline ways in which you can protect yourself against potentially malicious **REMOVABLE MEDIA**, but also some advice on best practice when it comes to using your own. Removable media can carry **MALWARE** and could damage networks or cause a compromise of data, if introduced to personal devices or home networks. They can also use devices such **KEYLOGGERS** to record information from your device (emails, passwords etc.) and forward this directly to the criminal.

REMOVABLE MEDIA: Removable media is any type of storage device that can be removed from a computer while the system is running. Examples of removable media include CDs, DVDs and Blu-Ray disks, as well as diskettes, floppy disks, hard drives and USB drives. Removable media makes it easy for a user to move data from one computer to another.

MALWARE: Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

Types of Malicious Removable Media

There are two types which are **COMMONLY** used:

- **KEYLOGGER** – USB to record victims keystrokes
- **MALICIOUS USB** - Loaded with **MALWARE**

Attack Methods

Cyber Criminals will often manually add malicious **REMOVABLE MEDIA** to networks

Cyber criminals will leave **REMOVABLE MEDIA** in the open for people to discover and plug into their own devices.

Cyber criminals will also look to steal your **REMOVABLE MEDIA** that is unattended, unsecured or thrown out.

Cyber Protection Advice

Keep software up to date on your devices, this will help protect against potential Malware introduced to your network

Scan **REMOVABLE MEDIA** for viruses when introducing to your network

Dispose of your personal **REMOVABLE MEDIA** properly to prevent your data being stolen.

Be aware of what is plugged into your device, unexpected **REMOVABLE MEDIA** could be malicious

If you discover **REMOVABLE MEDIA** which is not connected to a device, **DO NOT** plug it into any of your machines.

If you receive **REMOVABLE MEDIA** from someone else, consider carefully whether or not it is from a trusted source.

Cyber Crime Reporting

If you spot or fall victim to any cybercrime please report it to **Action Fraud** (the national reporting centre for Cybercrime) and your employer if this occurs on work email address or device.

Phone: **0300 123 2040**
Website: **https://www.actionfraud.police.uk/**

Created by Kieran Hall

Cyber Prevent & Protect Officer, DIIU