USB Drop Attacks

Recently there have been incidents of USB drop attacks in our local area and, as part of our commitment to maintaining a secure study environment, we need your help to avoid any potential risks.

What is a USB Drop Attack?

A USB drop attack involves leaving infected USB device in public areas or mailing them to individuals with the intent of tricking recipients into plugging the USBs into their computers. Once connected, these devices may introduce malicious software that could compromise the security of our systems.

Further risks might include:

- Passing a virus or malware between machines.
- Data falling into the wrong hands simply by losing the device.
- Targeted hacking can be attempted though a found USB device.

How can I help avoid a USB Drop Attack?

1. Do Not Use Unknown USB Drives

Don't use any USB drives that you find lying around, whether in study areas, communal areas, car parks or any other public space. Avoid connecting USBs received from unknown or unexpected sources.

2. Report Suspicious USBs

If you come across any unattended USB device within University premises, please report it immediately to the IT Specialist Helpdesk located at StudyHelp, 1st Floor Sheppard Library. Do not attempt to use or examine the contents of any unknown USB devices.

Be cautious about USBs received through mail or from unfamiliar sources, even if they appear harmless. If in doubt, verify with the IT Specialist Helpdesk before connecting the device to your computer.

We appreciate your attention and vigilance to ensure we continue to work in a safe and secure study environment.

More Information

For further help about staying safe online, please visit our page Two-factor Authentication, Cyber Security and Staying Safe Online on UniHub.