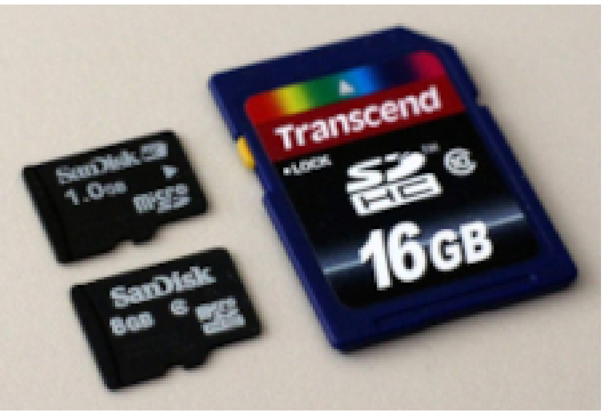
Cyber Security Newsletter May 2024

Removable media

In this month's security newsletter, we outline the pitfalls of using removable media such as USB sticks, SD cards, external drives and CFast cards.



Removable media have long been an opportunity for attackers to deliver malware into a computer or network. While very simple to use and able to hold large amounts of data, cards and drives pose a huge problem for security. With casual use, small size and ports on many IT devices, removable media and their control should be part of any robust security strategy. Some consultants say to never use or allow these data devices. Certainly, we need to think about the issues involved before we use them. Is using online data storage safer? Yes! Is leaving unsecured removable media in the office safe? No!

Many organisations fail to control and manage the import and export of data, possibly exposing themselves to:

1) Loss of information.
2) Introduction of malware.
3) Information leakage.
4) Financial loss.
5) Reputational damage.

General safeguards for our company.

Possible safeguards include:

1) Putting into effect data loss prevention policies (DLP). These policies can help prevent sensitive information being stored on removable media.

2) Implement access controls. These controls on all computers and servers help prevent unauthorized access from removable media.

3) Encryption: encrypting the data on removable media ensures that it will be unreadable to anyone without the correct key.

4) Carry out regular security audits. This system auditing ensures that media usage is in compliance with security policies.

5) Use endpoint security software which can detect and prevent malware spreading through removable media.

Basic personal security.

Best practice is:
1) Never plug in removable media that has no security history or you are not completely certain of its origin and/or contents.

2) Never plug in removable media that is not owned or controlled by our company into a computer that’s part of its network unless directly approved by the security team.

3) Never plug in removable media that you have found on a computer at home and/or work. Find a member of staff who is able to access the media securely.

4) Have up-to-date antivirus software enabled on your devices that might have removable media usage.

5) Where removable media is being reused, or destroyed, appropriate steps should be taken to ensure that any previous contents will not be accessible.

What's expected of us?

Keeping our company's information safe is everyone's responsibility. Anyone using removable media must take particular care to safeguard equipment and the information stored on it. All-in-all, it is best not to use removable media for sensitive and/or personal data.

Links to relevant information:

1) National Cybersecurity Alliance (USA).
https://staysafeonline.org/online-safety-privacy-basics/best-practices-for-removable-media-and-devices/

2) UK GDPR:
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources

Fellow employees that are safe from malware!