Creating a cyber epidemic from your mobile device

Author: test

Do you know the consequences of finding yourself in a situation where you urgently need to share or copy information held on a personal mobile device?

Whether it’s a photo, video, spreadsheet, word document, PDF or presentation, it seems like an innocent, convenient and fast way to transfer data; whether at home or at work.

However, in today’s world of cyber terrorists and hackers, the reality is that, rather like a rapidly spreading infection, if the data or device contains a virus, malware or other malicious program or code it can cause lasting and widespread damage; which can have a real damaging effect on our company systems.

In the event of serious breaches in security, vital functions could grind to a halt. We know how long it takes to control a medical epidemic and to some extent a cyber-epidemic is no different.

Cisco, a worldwide leader in IT, carried out a study and found that 46% of employees transferred files between work and home when working from home.

Add to this the idea of losing a mobile device containing sensitive commercial data and the risks becomes obvious. Every year, 20 million USB sticks are lost globally and more than a third contain at least 20 files – UK dry cleaners find around 9,000 USB sticks in customers’ clothing every year.

There is another thing to think about too. If you have personal information on a business or personal mobile device that you regularly back up or charge on your work laptop, be totally aware of what may automatically download. The audience for your data might end up being wider than you’d planned!

In some organizations, personal or mobile devices have been found to be used as a way to steal confidential information from the company network.

So, what constitutes a personal mobile device?

This can be anything from a camera, mobile phone, tablet, disk drive, USB or thumb drive, SD cards or, less commonly, CDs or DVDs.

Some golden rules

- Only store confidential information on mobile devices as a temporary storage method with a justifiable business needs to do so. The storage device must be encrypted, and permission obtained from your line manager.
- USB devices should not be used for normal information back-up – only use encrypted IS approved devices.
- Encrypt or (as a minimum) password protect important files before storing them on removable media.
- Adhere to appropriate standards of information classification.
- Always handle and dispose of electronic media securely.

Remember, secure is safe – we all have personal responsibility for how we use data.

[yop_poll id=”10?]

Date: 13-10-2015