Ransomware

Ransomware is a form of malicious software which aims to extort money by encrypting your files and demanding a ransom for the decryption passwords. Usually the ransom will be a few hundred pounds.

Often asks for payment in Bitcoin, an anonymous currency

Never pay the ransom - no guarantee of getting your files!

How can I protect myself?

Ransomware is propagated mainly through phishing emails and malicious websites. Upgrading to Windows 10 and ensuring that you have the latest updates/patches is crucial. Vigilance and awareness are also required. For example: if a trusted person sends a link or attachment which looks suspicious, attempt to confirm its authenticity.

Have a backup strategy

The best protection against ransomware is a good backup strategy. In the event of ransomware you can easily wipe infected devices and restore from a backup, how much data is lost will depend on the frequency of your backups. We advise at minimum weekly backups, with copies held offsite incase of natural disaster. Backup hard drives should only be connected to the device while the backup is taking place as some ransomware also targets attached USB devices and network shares.

What do I do if I get Ransomware'd?

Do not pay the ransom, there is no guarantee that you will get everything or even anything in return for the ransom. Report the incident to the Police - ransomware is a criminal offence. You can call 101 or report in person at your local Police station. If you are technically inclined, booting the PC in safety mode and running Microsoft Safety Scanner might fix some variants.

www.nomoreransom.org also provides help identifying the variant of ransomware and contains decryption keys for some variants of ransomware.

//curious frank:

www.curious-frank.com

A division of the Scottish Business Resilience Centre