

RANSOMWARE

Ransomware is a type of malware¹ that locks a computer's content and holds it for ransom. Attackers then demand ransom (payment) from the computer user in return for "unlocking" the computer's files so they can be used again. The attacker may claim that the computer is locked due to illegal or questionable conduct by the user.

Ransomware is often distributed through phishing emails – it can get onto your computer in the same way as any other malware.

WHAT DOES RANSOMWARE DO?

Ransomware can:

- Prevent you from using your system.
- Encrypt² files so you cannot use or access them.
- Stop you from running certain applications.

It can be very difficult to decrypt the files without the original encryption key used by the attacker.

SIMPLE STEPS TO DEAL WITH RANSOMWARE

1. Turn off your computer. Disconnect it from the network (remove the cable), turn off wireless connections, remove any connected devices (USB sticks etc.) and turn off any cloud back-ups (e.g. Dropbox or Office 365). This is to prevent the malware spreading. Never hand over remote control of your machine, (other than to the IT helpdesk in your own organisation).

2. Clean up. The process for cleaning up the computer and removing the ransomware depends on the type of ransomware. There are a variety of clean-up tools available which you may need to load onto a USB stick from a

different, clean computer and load onto the infected computer in "Safe Mode". It may require re-formatting the hard-drive (e.g. by restoring to factory settings). If you've backed up your data, you can reinstall it once the computer has been cleaned. If you're unsure of what to do, seek technical assistance from an expert.

3. Don't feel pressured to pay. It is not advisable to pay the ransom (usually required in bitcoins). There is no guarantee the cybercriminal will unlock your files and, even if they do, they may come back again once they know you are prepared to pay.

SIMPLE STEPS TO PROTECT AGAINST RANSOMWARE

1. Update your software regularly. Software updates include "patches" to prevent against the most recent threats, which will keep your system more secure.

2. Anti-virus software. Use the latest anti-virus software and update it regularly. Each update includes protection from the most recently known malware and viruses. Keep your firewall updated and patched to prevent threats before they enter your network.

3. Back up your data and test it. Regularly schedule routine back-ups of your data and files to an external hard drive or the cloud (online storage platform). Make sure these are not kept connected to the computer and are stored separately. This can help you keep your information secure if you are locked out of your computer and unable to recover encrypted files. Regularly test that you can retrieve data from your back up source. You should consider keeping a physical copy of the back up off site.

¹ **Malware:** is malicious software designed to facilitate unauthorised access to a system, or cause damage or disruption to a system. Malware is often downloaded to a user's computer or system by clicking an unsafe link or attachment.

² **Encryption:** Encryption is the process of encoding digital messages so only authorized parties with a decryption key can read it.

