RANSOMWARE

Ransomware is a form of malicious software (malware) which aims to extort money by encrypting computer files and demanding a ransom for the decryption password.

- Usually, the ransom will be a few hundred pounds in bitcoin, a cryptocurrency.
- Never pay the ransom. There is no guarantee you will get your files back!

How can I protect myself?

Ransomware usually exploits known security vulnerabilities. Upgrading to Windows 10, and keeping it and your applications up to date, reduces the risk of malware infection.

Ransomware normally arrives via phishing. Take steps to reduce the chances of phishing emails reaching your staff. Implement technical countermeasures, like DKIM, SPF & DMARC. Train staff to be aware of phishing and how to spot it.

All staff should not be able to access all files. By limiting staff access to the files required to do their jobs, you can limit the impact of ransomware attacks.

Have a back up strategy

The best protection against a ransomware attack is a good back-up strategy. Remember to test your back-ups! The only thing worse than having no back-ups is thinking you have back-ups and discovering you have none or they don't work. We recommend backing up at least weekly. The back-up device should not be permanently connected to the device it backs up. Copies should be held off-site to insure against your office burning down or other man-made or natural disasters.

What to do if your systems are infected with ransomware?

Do not pay the ransom. There is no guarantee that you will get your files back. Report the incident to the police via 101 (ask for the cybercrime team) or via actionfraud.police.uk.

The website nomoreransom.org may be able to help you identify the strain of ransomware and provide the password for your files.

The police will not be able to help you with incident response, however the NCSC website (ncsc.gov.uk) has a list of certified incident response companies who can help you.

The Cyber Resilience Centre
for Greater Manchester