Are you Ransomware Ready?

What is Ransomware?

Ransomware is a type of malware that prevents you from accessing your data until you pay a ransom. The number of Ransomware attacks have been growing rapidly since 2015.

For the safety and health of your business, you need to be aware of the risks and take the necessary steps.

Facts

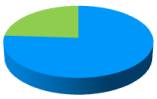
Ransomware exploits the weakest link in a company: ***their employees***

54% of UK companies have been hit by Ransomware

39% of organisations hit by Ransomware came from email

29% of companies said that the attack hit lower-level staff

42% hit mid-level managers



76% of UK adults don't know what Ransomware is

Ways to prevent Ransomware:

Educate your employees

Do not open attachments included in unsolicited e-mails and check all links contained in emails.

Only download software (especially free software) from sites you know and trust. If possible verify the software through a digital signature prior to download.

Invest in training for all staff so they are aware of how Ransomware works.

Actions for your IT Department

Ensure application patches for software, firmware and operating systems are kept up to date.

Automatically update anti-virus and anti-malware solutions and scan regularly.

Disable micro scripts from files transmitted via email.

Implement software restrictions to prevent the execution of programs in common Ransomware locations, such as temporary folders supporting popular Internet browsers.

No users should be given administrative access, unless absolutely needed.

Ensure there is a centralised patch management system on all endpoint device operating systems, software and firmware in place, as vulnerabilities are discovered.

Configure access controls with least privilege on mind.

Use virtualised environments to execute operating system environments or specific programs.

Categorise data based on organisational value and implement physical / logical separation of networks and data.

Require user interaction for end user applications communicating with websites uncategorised by the network proxy or firewall.

Only allow systems to execute programs known and permitted by the security policy.

Put a Disaster Recovery Plan in Place

In spite of all the preventative measures you take, you still need to plan for a possible Ransomware attack.

Your disaster recovery plan should include:

- A backup of your data
- Cloud replication
- Testing
- Recovery

We can offer your business a secure and reliable backup and disaster recovery solution in the event of a Ransomware attack on your systems. Please call us to discuss how we can help protect your data.