Protecting your business against ransomware

While ransomware attacks are currently all over the news, it can be confusing to understand what they mean for smaller businesses.

Naq Cyber's practical 5 step guide outlines actionable steps you can take today to keep your data secure and protect your business.

What is ransomware?

Ransomware is a type of malicious software which encrypts the files on your computer. Usually installed by clicking a link on a phishing email or malicious software, attackers will usually state that to unencrypt your files, you must pay a ransom.

Ransomware can spread from one computer to any others connected on the same network, spreading within seconds across an organisation.

1 Back up all your files, regularly.

The biggest impact of ransomware is the loss of data.

Ensure that all your files stored on all computers in your company are saved in some form of cloud storage (One Drive, Google Drive, Dropbox etc.) Ideally, you should back up your cloud storage using a service such as CloudALly.

2 Update your computers & devices.

The malware primarily infects your computer by taking advantage of vulnerabilities in out of date software.

For this reason, it is essential to keep your computer and its' software up to date. Ensure automatic updates for your operating system are enabled.

3 Train your team against phishing attacks.

Phishing can take many forms, but most phishing attacks use psychological tricks to try and convince recipients to either download something, visit a malicious website, divulge sensitive information or perform an action.

Your team must always be vigilant, but this vigilance must be taught. This is why the combination of policy, training courses and phishing tests are a critical part of the Naq subscription.

4 Prepare for a potential incident.

It is critical that you have a robust incident response plan in place should your business fall victim to one of these attacks.

This incident response plan should include what you need to do both from a technical and legal perspective to ensure any potential damage is minimised.

5 Practice!

Policies and plans are useless if you never read them and more so if you never practice what is in them before you actually need them. This is especially true for any incident response and data recovery plans.

Regularly go through your response plan with your team, identifying any areas which could be improved and outlining responsibilities.

Ransomware protection is just one of our areas of expertise. Secure your business, train your team and achieve data compliance from as little as £99 per month.

Click here to find out more.

Cyber Accelerator Alumni

in association with National Cyber Security Centre

CYBER ESSENTIALS