Business Go Digital

WHAT IS RANSOMWARE AND HOW TO PROTECT YOUR BUSINESS AGAINST IT

Contents

Introduction

Cybercrime, ransomware and malware are on the rise and businesses are advised to be more prepared than ever.

Anti-virus alone is not sufficient to provide protection against ransomware and malware.

There are several products and security measures a business can use to limit their risk to being exploited by ransomware.

What is ransomware?

Ransomware is malicious software. If it accesses your computer systems, it will do one of two things;

- **Locker**: Locks you out of your computer so you cannot access it.
- **Encrypter**: Encrypt your files so you cannot access them.

Whichever action is taken, the ransomware will require you to make a payment (ransom) to release the lock or to decrypt the files.

On average, a cyber crime incident costs a small business nearly £3,000, and takes 2.2 days to recover from.

The Federation of Small Businesses (FSB)

How ransomware infects your PC □ □ □ □ □

How ransomware infects your PC

Attacks are becoming more widespread.

Cyber criminals are always trying to find new and different ways to infect your computer and ultimately extort your hard-earned money.

They do not target a specific company, they search for vulnerable systems as they are the easiest to infect. They can also manipulate and trick users into revealing confidential information.

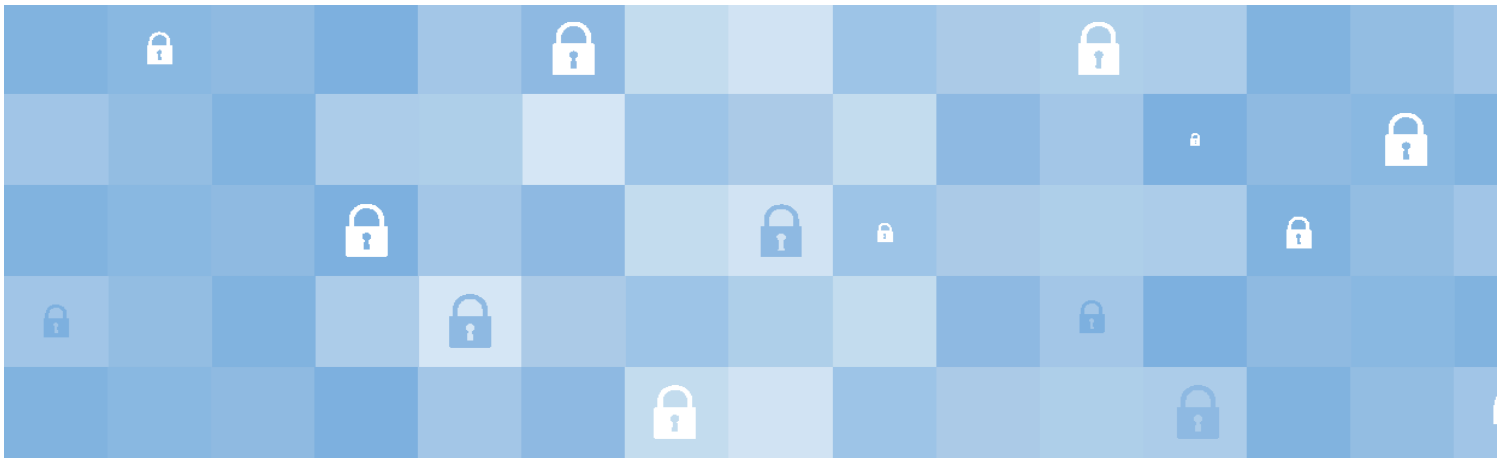
Here are some of the main methods ransomware infections occur:

- **Vulnerable Software:**
Unpatched software and operating systems allow security exploits.
- **Spam Emails:**
Emails that contain malicious attachments or links.
- **Social Media:**
Messages in social media can contain malicious links.
- **Malicious Web Sites:**
Web sites could contain malicious software or links.
- **Compromised Web Sites:**
Legitimate web sites could be infected and spread ransomware.
- **Self-propagating:**
Spreading from one infected computer or device to another.

Seven million cyber crimes are committed against smaller businesses in the UK every year. That's 19,000 every day.

The Federation of Small Businesses (FSB)

The aim of the attack is to infect a target quickly without the user realising. This white paper will help to inform, what to look out for and how to protect your business from attacks.



What you can do to protect your business against ransomware

There are several solutions that can benefit you and your business.

Here are some suggestions to enhance your Security protection.

Use anti-ransomware

One of the best ways to protect your business is to use anti-ransomware software. There are various solutions available including free and paid for, but consider using an enterprise solution that will protect your whole computer network.

Anti-ransomware works in conjunction with your anti-virus package and you should use both types of products.

Backup your files

If you do not back up your files and you are hit with a ransomware attack, you could lose your data.

The best way to recover from a ransomware attack is to recover your data from a backup. This will minimize business downtime. You also need to decide how often to back up your files; hourly, daily, weekly?

Be vigilant and educate your staff

Phishing emails, malicious adverts, etc. can easily fool you and your staff. Ensure your staff are suitably trained in how to spot malware and the risks of using the internet.

59% of ransomware attacks are hidden in emails and 40% of all email spam contained ransomware (Osterman Research).

Keep your software up-to-date

Software updates are essential. They are designed to close vulnerabilities and maximise protection. You are more prone to attacks if you fail to keep your software up to date. This is the main reason the NHS were hit by the WannaCry ransom attack in 2017 for example, and it caused major disruption.

Never pay the ransom

Even if you pay the ransom, there is no guarantee the hackers will release your files. For example, in May 2016, a hospital in the USA paid a ransom to unlock their data. However, the cyber criminals subsequently demanded more money. Paying the ransom encourages the attacker to continue with cybercrime.

What to do if you're hit □ □ □ □ □

What to do if you're hit

The first 5 steps are as follows:

1. Disconnect your computer from the network.
2. Disconnect any external drives.
3. Disable any shared drives.
4. Inform all other users and your IT team.
5. Update and run your security software.

Next, answer the following 3 questions to check your backups:

- For each device affected, do you have a backup?
- What is the most recent backup? An hour, day or week old?
- Check the backup to ensure all files can be restored.

Collate information about the Ransomware

1. Take a photo of the ransom screen. It may be useful later.
2. Find out which ransomware you are dealing with.
3. See if there is any decrypting software or tools available.
4. Report it to the Police and any other necessary authorities.

Finally:

- Formulate a plan to either restore from a backup or use decrypting tools.
- Create a revised security policy to close any loopholes for future attacks.

More information?

If you are concerned about cyber security in your business, we can help. We perform security assessments for any type of business and ensure a comprehensive strategy is in place.

Protect your business, book an appointment today on 07778429591 or email us at info@businessgodigital.uk.