sedcom
Your trusted IT partner

IT'S THE FASTEST GROWING CRIME ON THE PLANET

but what does ransomware mean to you?

IT'S THE FASTEST GROWING CRIME ON THE PLANET

but what does ransomware mean to you?

If you've heard of it, you may have put two and two together. And figured out that ransomware is a form of malware (malicious software) that holds your business to ransom.

Cyber criminals take control of your files, photographs, and any other data that's important to you. They encrypt it, and deny you access until you've paid a ransom of their choosing.

You'll know quite clearly if you've got ransomware. You'll be locked out of your computers. And there'll be a message on your screens telling you to pay a "fine" or the crime gets worse.

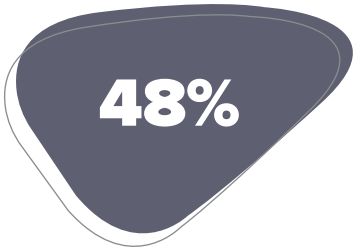
An example of what you might have to pay is £5,000 (in bitcoin, the online currency). If you fail to pay up within three days, the figure doubles. Fail to pay within a week and your data is gone. Deleted.

While anyone can become a victim of ransomware, it's usually small to medium sized businesses (just like yours) that are targeted. That's because they often don't spend an adequate amount of time or money on security for their devices and networks.

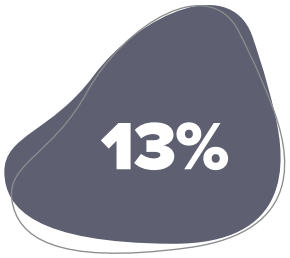
of UK businesses have suffered data breaches in the past 12 months*

small UK business is successfully hacked every 19 seconds **

These breaches cost an average of £25,700 to clear up **



were attacked with ransomware in the last year ***



of these businesses paid the ransom ***

* https://www.carbonblack.com/resources/threat-research/global-threat-report-series/
** https://www.hiscoxgroup.com/news/press-releases/2018/18-10-18
*** https://news.sophos.com/en-us/2020/05/12/the-state-of-ransomware-2020/

So, how does this actually happen?

How does this ransomware get on your device in the first place?

More than half of infections occur when someone clicks on a dodgy link in an email

And that's not surprising, given that one in every **3,722** emails in the UK is a phishing scam. And **55%** of UK email is spam.

The more we go on, the more terrifying this all sounds. Now can you see how important it is to actively protect your business from cyber-crime?

HOW TO PREVENT YOUR BUSINESS FROM BECOMING A VICTIM OF RANSOMWARE

Fortunately, there are five really effective things you can do to protect your business.

It's important to take a long-term approach to this, just as you would with any form of cyber-attack.

It's cheesy, but prevention really is better than cure.

01

BRING IN THE EXPERTS NOW

Having an IT data security expert as your partner will give you the peace of mind that you have all of the latest security, equipment and knowledge to keep you safe.

Also, if things should go wrong, you've got your own emergency service to call upon for immediate assistance.

Take some time to find the right IT service partner for your business.

Ask them questions about:

- How they operate
- Which areas of data security they can help you with
- And importantly, how they would handle a crisis (this can often tell you more about a company than anything else)

We're data security experts and protect lots of businesses round here. And we'd love to talk to you about your business.

02

FIND AN IT SUPPORT PARTNER THAT GETS THE BASICS RIGHT

Update, update, update. Yes, it's a pain, but run all of your updates when they're due, every time (or better still, get your IT support partner to do it for you).

Make sure you're running the latest version of your security protection software. The same goes for your operating system and all other software or applications that you use.

Malware and other types of attack are always evolving and becoming more sophisticated. Your security protection, apps and operating software companies spend huge amounts of money to keep on top of these threats and adjust their software accordingly to keep you safe.

Take the time to run the updates so you benefit from their protection.

03

BE AWARE THAT EMAIL IS THE ENTRY POINT FOR MANY ATTACKS

We've just highlighted that spam email is responsible for almost half of cyber-attacks, so be vigilant when it comes to opening unusual emails or clicking on links or attachments that you're not anticipating.

Pay particular attention if an email asks you to enable macros to view its content. If it's not an email you're expecting do not enable macros. Delete the email immediately and tell your IT partner.

04

MAKE SURE YOUR DATA IS BACKED UP CONSTANTLY. AND CHECKED

This is the single most effective way to protect you and your business from data loss. Because even if a cyber-criminal hacks you and encrypts your files, you've got another copy of them safely in the cloud.

Constantly backing up and checking data means you can access versions from before you were attacked, minimising the chance of reinfection.

Although this is a brilliant way to protect your data, please don't be mistaken in thinking you can skip the other steps and just back everything up.

Remember that even if you still have a copy of everything, you should still be concerned as to where your stolen data actually ends up. You have a duty to protect the data you hold on your customers. And if that's lost you have another big problem to worry about.

You will also still have to go to the trouble of making sure your network and devices are free of malware to prevent a follow-up attack.

05

TRAIN YOUR TEAM TO KNOW WHAT TO LOOK FOR

Even when you hire an amazing IT support provider, keep on top of your updates and check all of your email with a suspicious eye, how can you be sure that your team will all be as vigilant?

You can give them regular cyber-security training.

So many businesses fall at this hurdle. They either don't see the value in training the entire company on this subject, or it doesn't occur to them to do so.

But it makes sense that if someone's using any kind of device for your business (and let's face it, everyone will be), they need to be as vigilant as you are to keep your data safe.

Invest in regular training. Your IT service partner may offer this, either in person or using online training. And ensure that everyone in the business, from receptionist to CEO attends.

Remember, you're only as strong as your weakest link.

BUT WHAT HAPPENS IF, DESPITE TAKING ALL OF THESE PRECAUTIONS, YOU'RE STILL CAUGHT OUT BY RANSOMWARE? WHAT DO YOU DO?

First and foremost:

- Don't panic
- Don't pay the ransom
- Don't hesitate to pick up the phone and call your IT support partner

If you've followed this advice, you'll have a back-up copy of your data elsewhere.

Your IT support partner will need to work their magic to ensure that there are no further infections lurking on your devices or network. And then reinstall any lost data from your back-ups.

If you follow all of the advice and your people are aware of the risks and exercise caution when required, there should be no need to live in fear of ransomware affecting your business.

Yes it can still happen. But you'll find it so much easier to limit, then undo the damage.


BAD RABBIT
If you access this page your computer has been encrypted.
Time left before the price goes up
41:16:04
Price for decryption:
= 0.05
Enter your personal key or your assigned bitcoin address

If you don't already have the above precautions in place, give us a call today to see how we can help you stay protected from ransomware and other forms of malware that could do serious damage to your business.

sedcom

Your trusted IT partner

This is how you can get in touch with us:

t 0207 998 4151 e craig.butler@sedcom.net w www.sedcom.net