11 scary signs your business has been hacked

If you spot just one, you could protect your business from a potential catastrophe

ACU IT Solutions

Managing the technology powering your business

www.acu-it.co.uk 0141 255 1617

Being hacked is scary. It has the potential to destroy your business and everything you've worked towards.

And it's no longer about if' you're going to be attacked, it's when.

That's because the rise in cyber crime figures is alarming

You may have heard about the WannaCry ransomware attack that hit the NHS back in 2017. It brought many NHS trusts to a standstill and left the country with a £92 million IT bill.

Those kind of huge headline hacks make business owners and managers believe their organisation is too small to be targeted.

But the reality today is that all businesses are being targeted, all the time. Hackers use automated software to look for vulnerabilities everywhere. And when they find them, they will exploit them to either cause damage, or demand cash to release data.

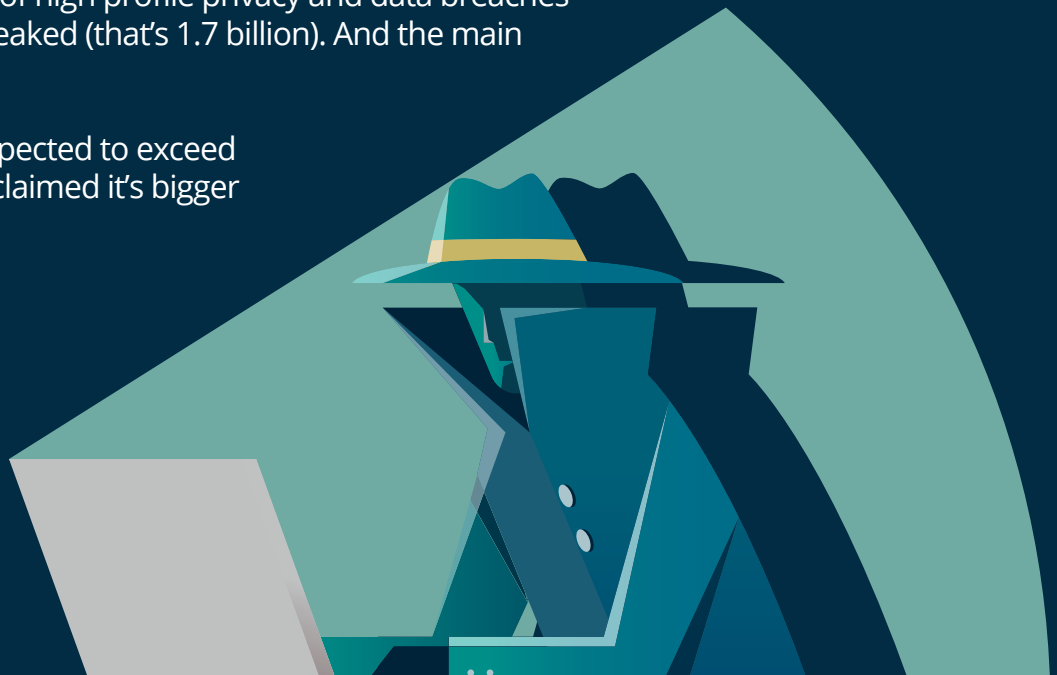
No one is exempt from this type of attack – not even your business – and it's happening more and more because hackers love ransomware attacks. The threat has become so dangerously high, that it's estimated that in 2019, attacks like this will cost organisations and businesses £9 billion in damages.

That's just ransomware attacks. What about data breaches? Data breaches could destroy the trust you have with your client as well as be a GDPR nightmare. There has been a string of high profile privacy and data breaches recently. In January alone, exactly 1,769,185,063 user records were leaked (that's 1.7 billion). And the main cause of data breaches is malicious or criminal attacks.

Finally but not exhaustively, the global cost of cyber crime itself is expected to exceed $2 trillion in 2019. The threat is so high; Investor Warren Buffet has claimed it's bigger than treats from nuclear weapons.

These facts are terrifying. But what does it mean to your business?

As you're reading this, think about if your business is prepared for a potential attack – small or large. And if your data was leaked, your systems rendered useless and money stolen, how this would affect the business you have worked so hard to build?



Financial transactions you don't recognise

#1

There's lots of ways hackers can steal your hard earned money and it all starts by getting your personal data. This can be via a malware or phishing scam, ransomware, or by hacking into your online and social media accounts.

It's happening all the time, because to hackers it's easy cash.

Unfortunately, there's no way to make your computer completely impenetrable to a cyber attack of this kind. Which means hackers will keep on finding ways to steal money from you, your business and potentially your clients. Even large organisations with full time cyber security teams cannot 100% guarantee they can stop this from happening.

But if you make it really difficult for hackers to break into your computer by following standard security steps, you'll decrease the risk of them accessing your various banking and billing systems.

They include:

- Using long robust passwords, generated by a random password generator
- Keeping track of complicated passwords with a password manager
- Using multi factor authentication – such as a text message with a code to confirm it's you trying to login
- Verifying new payment details over the phone; not just relying on details sent by email

One other aspect to consider is social engineering. Sophisticated hackers will break into email and sit in the background, watching what's happening and waiting for an opportunity.

Such as sending an email that appears to be from you when you're on holiday, asking for an urgent payment to be made. You'd be surprised how many staff fall for this one.

Keep a daily eye on your banking and if you notice any unexplained transactions, it could be a red flag that you've been hacked.

#2

Your phone or computer really slows down

Hacking your computer or phone to send out malware for instance, takes a lot of processing power and energy. This can cause your devices to slow right down.

We're not talking about a gradual decrease in speed and device efficiency, because that happens naturally over time. We're talking about significant drops in performance that happen suddenly - either to the device itself or your internet connection.

If you do experience this, it's possible that it's been caused by a hack.

Malware is a type of software that is intentionally designed to cause damage to your computers, server, clients or computer network.

Once hackers have been able to infect your systems with malware, like a virus, it will also attack the security systems that are currently in place. This is in order for it and other threats to create more chaos.

If you notice your security software / antivirus programme stops performing like it's supposed to; keeps being disabled or disappears all together – it's possible that malware is to blame.

Pay close attention to how your security software is performing, as this is your system's first line of defence and any differences could indicate a potential hack.

Security software that has stopped working

#3

#4

Software and browser add-ons you haven't asked for

If your systems get infected with malware, it's likely that other threats will start attacking you because your defences have been weakened.

Other threats initially caused by malware can sometimes take the form of new software on your devices, including add-ons and browser extensions.

While they look innocent to the untrained eye (potentially many members of your team) some will be busily working away causing lots of undetected damage.

That's why you need to be diligent and keep a look out for software that you haven't downloaded, as this could mean you have been hacked.

The easiest way to check your systems for threats of this kind is by using Task Manager for Windows and Activity Monitor for macOS. Both of these will show you what's running.

Just make sure you know what you're doing before you start deleting software... lots of critical components have strange names, but computers can't work without them.

Pop up frenzy

These days, your systems are pretty good job at managing and filtering pop-ups. But even the most advanced security systems can sometimes get infected with malware – which could mean a very authentic looking, yet random pop-up could appear while you or your team is working away.

Hackers aren't stupid. They want to make pop-ups look as real as possible, so it's the randomness you need to look out for. The randomness of the pop-up indicates that it's probably been caused by malware and that you've potentially been hacked.

If the pop-up is not related to your search or website, don't click on it. And make sure your systems are thoroughly checked for malware.

#5

#6

Your system settings have been changed

Similarly to unwanted software add-ons and browser extensions, hackers could deploy malware that changes your computer settings, allowing the infection to cause more and more damage.

Often, this could cause your usual default search engine browser to change. This is a classic example but luckily these days, browsers have become clued up to that trick and prevent malware from doing it.

Other examples include requests to change your systems settings or give particular software more advanced permissions.

If you haven't asked for it, it's likely that a hacker is asking for it – so it's important that you and your team don't confirm random requests, just because your computer prompts you to.

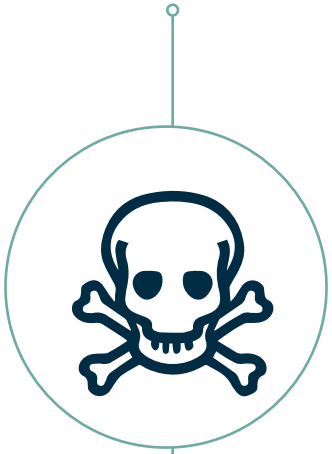
If you or your team do notice integral changes to their settings, or additional programmes, it's possible that you have been hacked and the necessary steps need to be taken.

Okay, so wild might be an over exaggeration. But if you do notice that your phone or computer has a mind of its own, it's possible that hackers are controlling your device via a backdoor app.

Although attacks like this are rare, it still happens. If you see random mouse movements, key presses, programme launches or your display waking up when you haven't touched it, this could indicate that the hackers are hard at work.

If you suspect that you have been hacked in this way, immediately disconnect your internet and server connection, restart your computer and scan it for potential threats using the appropriate malware and security software.

Your phone or computer goes wild



#7

#8

Involuntary shut downs and restarts

If this has happened just once or twice, it doesn't necessarily mean you're being hacked. So don't worry. But if it continues to happen, it's certainly worth investigating.

Much like hackers controlling your device via a backdoor app, your phone or computer shutting down and restarting again could mean that an unauthorised app has taken control.

A great way to see what is running on your computer is by checking Task Manager for Windows or Activity Monitor for MacOS. Or check your phone by going to settings and seeing a full list of your downloaded apps.

If anything looks suspicious, take controlled steps to safely remove it from your device and complete a thorough malware and anti-virus scan.

Like we've said before, malware loves to cause continual damage. It will try and get its mitts into anything it can, including your mailboxes. That way it can try to infect all of your contacts. Argh!

If you do spot any messages that you can't remember sending, be suspicious and complete a precautionary anti-virus and malware scan of your device and emails.

Also, best practice is to check your sent messages on a regular basis for any evidence that hackers have accessed your account and are sending messages.

This can sometimes be unmanageable. But fortunately, many contacts are quite aware of dodgy emails and will notify you if they receive anything that looks spammy – allowing you to take the necessary steps to remove any harmful software. And protect your mailboxes, devices and servers from similar threats in the future.

#9

You've noticed messages that you didn't send

#10

Online activity that doesn't belong to you

Another telltale sign that you're being hacked is online activity that doesn't belong to you. This could be anything from joining random Facebook groups; random Twitter followings; and emails from companies you've "subscribed to", but in reality you haven't.

Unless you're on top of checking your activity on a regular basis (and let's face it, who has time for that), hackers are free for the few days it takes us to notice to spread their havoc.

If you do notice on business systems, your Facebook account's activity log, or your Netflix's recent watched feed for instance, that there is activity that doesn't belong to you, take action immediately. Change your passwords and follow the necessary steps to remove any malware that has helped the hacker to access your accounts.

Unless you think you've genuinely forgotten your username or password, it's possible that if you can't access your accounts, hackers have got in, changed your login details and have locked you out.

They are now able to continue hacking you for a longer amount of time without your intervention, as you can't access the account. However, most online accounts, such as emails are pretty clued up to help you gain access to accounts that rightfully belong to you.

They know what computers you usually use, where you are in the world and offer other recovery links like mobile numbers and emails. So, don't worry if you have been locked out of your accounts due to being hacked, as you're sure to be back in control soon. Just take action with great speed... the longer someone has access to your accounts, the greater the damage they can do.

You can't access your accounts

#11

So, what do you do if you think you've been hacked?

Being hacked tells you that there is weakness in your business's line of defence. If the first attack hasn't damaged your business then you're very lucky. So be sure to strengthen your security so that you're not vulnerable to future, potentially more damaging attacks.

You should:

- Regularly change your passwords
- Ensure your passwords are different for every single account
- Regularly scan your devices using antivirus and malware software
- Ensure your team are trained on the various techniques hackers use to threaten your business. And the signs that have been outlined within this guide that could indicate you're being attacked

This is what you should do if you notice any of the 11 signs included within this guide

You should contact us immediately.

We will then be able to tell you what steps need to be taken to remove the threat, repair any damage that has been caused and safeguard your business in the future.

We're not just an emergency recovery service. Most of our clients use us to proactively monitor and protect them, so they just don't need to think about this kind of thing.

We'd love to do the same for your business.

ACU IT Solutions
Managing the technology powering your business

www.acu-it.co.uk 0141 255 1617