Preventing cybercrime

How to keep fraud and cybercrime out of your business

Love business Hate fraud

Each year about four out of ten UK businesses have their computers, networks and smartphones attacked by cybercriminals.[1] The first step towards making sure this doesn't happen to you is to understand what cybercrime is and how it can hurt your business.

This guide explains how cybercrime works and the practical things you can do to keep your business safe.

What is cybercrime?

Cybercrime is crime committed online.

This can mean complicated technical attacks on computers, networks and mobile devices – such as hacking, phishing, ransomware and DDoS (distributed denial of service) – or using computers and the internet to commit traditional crimes like harassment, bullying and fraud.

Who commits cybercrime and why?

Cybercriminals can be novices, amateurs, opportunists, sophisticated professionals or even members of organised crime gangs.

They might be attacking you from the other side of the world or they might be sitting at the desk next to yours.

Money is often the motive, but not always. Governments and political groups use cyberattacks to further their objectives. Individuals may want kudos, revenge or just some fun. Whatever the motive, the damage they do is real and significant, and it can be long lasting.

Know the signs

Many cybercrimes start with a phishing email designed to exploit your natural curiosity, fear, desire to help, or sense of urgency.

Typically it will encourage you either to reveal confidential/sensitive information or to trigger malicious software (malware) by clicking on an innocent-looking attachment or link. The malware then wreaks havoc:

- locking your devices or making them unusable;
- stealing, deleting or encrypting data;
- taking control of your computers, then using them to launch attacks on other organisations;
- obtaining login details to access other systems and services;
- hijacking the computer's processor and using it to 'mine' cryptocurrency; and/or
- connecting to paid-for services (such as premium rate phone lines) which you must pay for.

It is vital to remain alert to unusual emails (and phone calls or text messages) making odd requests for sensitive information or for you to click on a link.

Be especially concerned if the message:

- is from an organisation you don't know or don't do business with;
- appears to be from a senior staff member, or a supplier, asking for a payment to be made quickly (sometimes using unorthodox payment methods like gift cards) or for sensitive information to be sent urgently;
- contains poor-quality logos/graphics or poor spelling/grammar;
- claims to be urgent or contains veiled threats;
- is from someone trying to get in touch with you using several different methods simultaneously;
- directs you to a website asking for personal/financial information or requiring you to download a special program to access the content.

Watch out for these common examples

Distributed denial-of-service (DDoS) attacks

Criminals create a network of compromised computers (which could include yours) and then use it to flood an online service with bogus traffic, causing the server to crash and preparing the way for a blackmail demand.

Hacking

Unauthorised use of, or access to, computers or networks, normally to steal information that they can sell or hold to ransom. Hackers exploit security weaknesses or bypass protections.

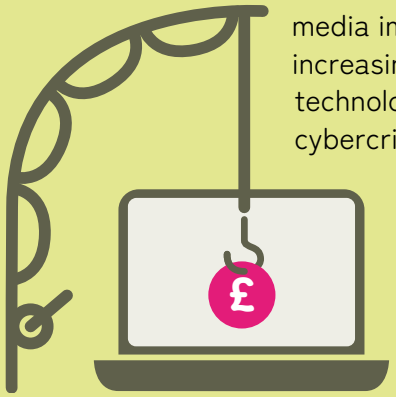
Hacking of social media and email accounts (business and personal) is common.

Phishing

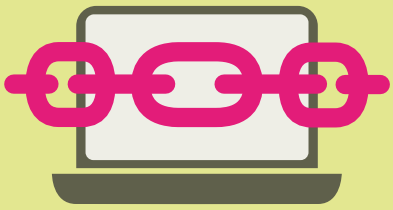
Emails, text messages or phone calls are used to trick victims into visiting a fraudulent website, downloading a virus or malware, or revealing bank details/personal information. Most hacks on business social media accounts start with phishing.

A special type of phishing targets business email systems. Criminals pretend to be a senior person (such as the finance director or chief executive) or a supplier, and trick staff into sending money or revealing confidential business information.

They also trick customers and suppliers by posing as staff members or someone else connected with the business. Email and social media impersonations increasingly use deepfake technology, changing the cybercriminal's voice and appearance to make them more convincing.



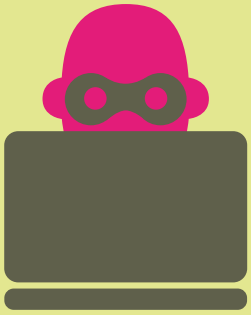
Ransomware



This kind of malware is designed to make the victim's data or computer system unusable until a ransom is paid. If the data includes sensitive personal or business information the cybercriminal may threaten to make it public if the ransom isn't paid.

Other cybercrimes

Other types of cybercrime include identity fraud, cyber espionage, illegal gambling and the selling of illegal items.



FRAUD ADVISORY PANEL

Sponsored by BARCLAYS

MOORE Kingston Smith

Thanks to Edward Nkune and Paras Shah from Moore Kingston Smith for kindly writing this guide.

Love business. Hate fraud.

This practical guide highlights some of the potential cybercrime risks to your business. But business fraud comes in many other guises. It makes good business sense to find out more.

Go to lovebusiness-hatefraud.org.uk or follow the campaign on Twitter and LinkedIn.

[1] Department for Digital, Culture, Media & Sport (2022). 'Cyber Security Breaches Survey 2022'.

Preventing cybercrime

How to keep fraud and cybercrime out of your business

A checklist

Ask yourself...

- What information do we store electronically? (For example accounting, customer, IP, development plans.) How valuable is it to us? Who has access to it? Where is it stored?
- Am I confident that our 'cyber perimeter' (firewalls, antivirus software etc) is secure and nothing threatening is sitting on our network?
- Are we making regular data back-ups? Are they stored offline, disconnected from the main network and the internet?
- Do we have a clear idea what we will do if our systems are compromised? Is everyone familiar with the plan?

Do...

- Use strong passwords (such as three random words) and two-step verification wherever possible – especially for email and social media. (A password management tool can help.)
- Keep antivirus software up to date and make sure your firewall is switched on.
- Back up data regularly. (There are often automatic settings for this.) Make sure the back-up device is not permanently connected to the main data source.
- Keep all software and apps up to date on all devices. Allow staff to download apps only from manufacturer-approved stores.
- Train your staff in cyber security. They are your first line of defence and will often know where the key vulnerabilities lie.
- Check every important email request independently by another method – a phone call (using a number held on file and known to be genuine), by logging into your online account, by post or (where practical) in person.
- Take control of your digital footprint, including social media accounts. Check privacy settings regularly. Disclose information only when you really need to.
- Encourage staff to report all suspicious emails.
- Create a cyber response plan and make sure it works by practising it regularly.
- Consider working towards certification under the government's Cyber Essentials scheme, and suggesting to your suppliers that they do the same.
- Consider the need for cyber insurance.

Don't...

- Assume that small businesses aren't worth targeting. It is more a question of 'when' not 'if'.
- Rely on a single means of defence. Use a combination of several different controls.
- Share passwords, reuse passwords across different accounts, or use the same password for work and personal accounts.
- Pay a ransom immediately. The police say there's no guarantee you will get your data back. It may also leave you open to future attacks.

Protecting your business

A few simple steps will make your business safer.

Have a cyber response plan

Use 'walk throughs' and dry runs to practise what will need to be done and who will need to do it in the event of a cyber attack. The National Cyber Security Centre's Exercise in a box (free online) can help you test and practise in safety.

If you are an SME it's unlikely you'll have all the skills you need in-house. Consider finding expert help: IT specialists to help with the technical aspects; legal advisers for your obligations to customers, clients and employees; and specialist investigators to build a picture of how and why the incident unfolded.

It takes time to find experts you can rely on. Start looking now.

Action Fraud – the UK's national reporting centre for fraud and cybercrime – can also provide advice and support if you are suffering a live cyber attack.

Keep antivirus and system security up to date

A lot of cybercrime can be prevented simply by keeping antivirus software up to date and applying security patches as soon as they become available. Don't click the ignore button!

Make staff aware of cyber threats

Get everyone involved. Make sure staff, contractors, suppliers and other stakeholders are made aware of the threats to your business and their own responsibility for improving cyber security.

Train new staff well and provide regular refreshers for everyone else, starting with the common methods used by cybercriminals.

Consider penetration testing

This is a safe and controlled way to find security vulnerabilities by simulating the technical and social engineering (phishing) methods used by criminals.

Listen to the NCSC

Follow the National Cyber Security Centre's (NCSC) good practice advice (including its small business guide and cyber action plan) and you will significantly improve the cyber resilience of your business.

FRAUD ADVISORY PANEL

Sponsored by BARCLAYS

MOORE Kingston Smith

Thanks to Edward Nkune and Paras Shah from Moore Kingston Smith for kindly writing this guide.

Love business. Hate fraud.

This practical guide highlights some of the potential cybercrime risks to your business. But business fraud comes in many other guises. It makes good business sense to find out more.

Go to lovebusiness-hatefraud.org.uk or follow the campaign on Twitter and LinkedIn.