

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.



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.

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!



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

Published December 2022. © Fraud Advisory Panel and Barclays 2022. Fraud Advisory Panel and Barclays will not be liable for any reliance you place on the information in this material. You should seek independent advice.

 This work is licenced under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International Licence.

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**.

