



Protect what matters to you and your business

As an Aviva Cyber insurance customer, you have access to a range of useful resources, available at no extra cost, to help you manage the risks to your business. We've outlined some that you might find particularly useful below but there is much more available at our [Aviva Risk Management Solutions website](#). You'll also find information on our range of [Specialist Partners](#) who can provide a variety of solutions to help you.

Protect what matters to you and your business

Here to help

As an Aviva Cyber customer, if you think you may have suffered a cyber incident, you can call our 24/7 Incident Response helpline on **0800 051 4473*** where our team of experts can help you fix the issue and advise you on any action you may need to take.



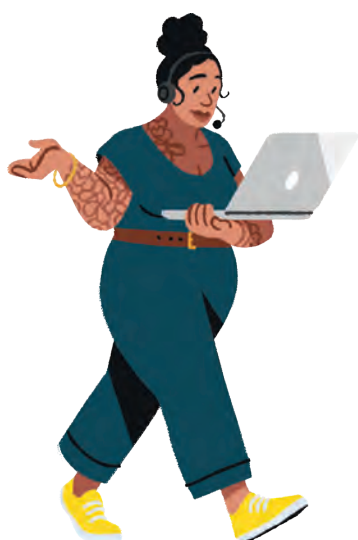
Managing your exposure to common cyber risks

If you get an email from a supplier saying they've changed their bank details and asking you to pay their latest invoice to their new account, what would you do? Sometimes this could be a genuine request but this can also be a tactic used by cyber criminals to trick you into paying money to them instead.

This process, known as **social engineering**, involves a cyber criminal posing as a person or organisation you know and trust and manipulating you to take action. This could include sending them payments or sensitive information, clicking on a link or opening an email attachment that's infected with malware. It's a common method of cyber crime but being aware of the signs can help you spot a social engineering attempt and stop it before it becomes a problem. This [helpful document](#) outlines the types of social engineering and some guidance on how to minimise the chances of falling victim to an attack.



The use of **ransomware** is another technique deployed by cyber criminals. Ransomware is malicious software (malware) that infiltrates a network, system, or computer and prevents access to certain elements until a ransom is paid to the attackers. This type of attack can be high profile and is often reported in the news but it's not just large organisations who are targets - any business with a weakness in their systems can be exploited. [In this document](#) you'll find more information on ransomware and some of the steps you can take to help protect your business including backing up your data regularly, introducing Multi-Factor Authentication (MFA) for network access and updating your software.



Ensuring your staff are trained on what to look out for is a really important factor in protecting your business. We work with [Bob's Business](#), one of our Specialist Partners, who provide cyber security awareness training for businesses of all sizes. Find out more about the [preferential rates available to Aviva customers](#).

Cyber hygiene

You may also wish to consider undertaking the **Cyber Essentials accreditation**¹ which is a UK Government-backed scheme designed to help businesses defend themselves against cyber attacks. It includes guidance on putting fundamental controls in place and support on managing third party risks. If you become accredited you will receive a certificate to provide assurance to your business partners, suppliers and customers that you have basic cyber hygiene in place. If you're interested in learning more about Cyber Essentials or want to know how to get certified, you can visit the [National Cyber Security Centre \(NCSC\) website](#).

Things you need to do

This is a summary of the actions you must take in relation to our cyber insurance cover to make sure you are protected and that your policy cover operates fully. They are also steps that can help you with your cyber hygiene.

- Any default or manufacturers' passwords or access codes must be changed and kept secure.
- Data must be backed up no less frequently than every 7 days. You must check the backup routine is working, and backups must be stored securely and separately from the original data or programs.
- All personal data and other sensitive, protected or confidential data must be stored and disposed of in a secure manner.
- Updates to software must be carried out within 14 days of an update being released, where the product vendor describes the issue as 'critical' or 'high risk', or the update addresses a vulnerability with a Common Vulnerability Scoring System (CVSS) v3 score of 7 or above.
- Computer equipment connected to the internet or an external network must be protected against unauthorised access by an active firewall.
- Computer equipment and any personal devices used for accessing your computer systems must have effective and up to date software protecting against virus and malicious code that's updated at least once a month.
- On receiving a cyber extortion demand you must immediately notify and comply with the requirements of our Claims Service Provider. You will also need to report the crime to Action Fraud, the UK's national fraud cybercrime reporting centre.
- You, your partners, directors and employees must be trained in the dangers of social engineering fraud and how to spot these attempts and you must keep a record of such training.
- You must have a documented policy in place, which states that details of any new payee requests or amended payment instructions are always checked verbally by using details held on file or a published website and do not solely rely on the new instruction. This policy must be accepted by all Partners, directors and Employees, with such acceptance recorded.



¹ [Cyber Essentials scheme process and evaluation, gov.uk, 2023](#)

Contains public sector information licensed under the Open Government Licence v3.0.

Protect your business

You also have access to some additional **services** that can help your business run smoothly.

Counselling Service Helpline: 0117 934 0105*

This is a confidential service available to your staff to help deal with personal issues such as bereavement, divorce, the threat of violence in the workplace and bullying at work. The helpline can also support your staff should they suffer stress or trauma following a cyber incident.

Legal and Tax Helpline: 0845 300 1899*

Call this helpline anytime, day or night, for advice on legal or tax matters in the United Kingdom. Given in confidence, the advice is available at no extra charge - you pay for just the cost of the call.

Aviva Businesslaw – <https://avivabusinesslaw.farill.io/>

This is a complimentary website, provided by Aviva, offering many tools and resources to help you manage your business effectively.



This service includes:

- unlimited access to legal advice via the legal advice helpline
- a range of regularly updated business and legal guides, document builders, interactive checklists and videos that can help you with the day-to-day running of your business, as well as helping you to manage your exposure to legal risk
- easy to use templates to build legal documents including employee contracts, health and safety policies, dismissal letters
- topics ranging from data protection branding, crowdfunding, financial and tax planning, to marketing strategy to help build and grow your business
- email alerts on changes in law, legislation and regulation

To register:

1. Visit <https://avivabusinesslaw.farill.io/>
2. Enter the voucher code **DASBAVI100** into the **‘First time using Aviva Businesslaw?’** box
3. Click **‘Validate Voucher’**
4. Fill out your details and create a password
5. Validate your email address by pressing the link in the confirmation email that you receive.

This document contains general information and guidance. It is not intended to be specific advice and should not be relied on as such. It may not cover every risk, exposure or hazard that may arise and we recommend that you obtain specific advice relevant to your circumstances. We accept no responsibility or liability in respect of any person who may rely upon this document.

*The cost of calls to 01/02/03 prefixed numbers are charged at national call rates (charges may vary dependent on your network provider) and are usually included in inclusive minute plans from landlines and mobiles. Calls to 0800 numbers from UK landlines and mobiles are free. For our joint protection telephone calls may be recorded and/or monitored.