Jersey Business

Keep your business safe online

Tips to safeguard your business

Running a business is challenging enough without having to deal with the outcome of fraud and other online and data security issues.

With most businesses and their customers communicating, transacting, accessing services and managing their finances online, we tend to take the internet for granted, and it is hard to imagine a world without it.

Unfortunately, however, things go wrong online, with an increasing number of businesses of all sizes and descriptions being affected by fraud, identity theft, reputational damage and other negative outcomes. The consequences can vary from inconvenience through financial losses to, in the worst cases, business failure.

As a business owner or operator, there are technical precautions you must take to safeguard the organisation, but most problems can also be avoided by making sure that simple rules are followed and that security becomes second nature to everyone in the business.

Top 10 expert tips

1. Run regular online safety and information security awareness sessions for all employees. Get staff to question and challenge things that seem irregular.
2. Ensure that only those who need it can gain physical access to computers and servers.
3. Enforce strict access to company, employee and customer data.

4. Perform regular backups to a reputable service, preferably one that is in the cloud and easily accessible when you need it.
5. Introduce and reinforce rules about mobile devices, including keeping them safe, use of public internet and secured home access, and the use of employees' own smartphones and tablets in the business.
6. Make sure you and all staff can spot the signs of a social engineering email or phone call designed to gain confidential information and know how to avoid the company being defrauded in this way.
7. Have a software policy firmly in place including usage, updates, licences and what to do with redundant programs and apps.
8. When disposing of redundant computers, servers and mobile devices, ensure all data is thoroughly erased (not just deleted) to ensure it doesn't fall into the wrong hands.
9. Set guidelines about employees' social media use to help ensure that the reputation of the business is not compromised.
10. If your business enables access to its systems by others in the supply chain, take steps to ensure that they have robust technology and processes in place.

You can find more information on these and our other tips at www.gov.je/besafeonline

Golden rules for you and your colleagues

1. Choose, use and protect passwords carefully, and use a different one for every account.
2. Ensure that reputable internet security software or an app is loaded, kept updated and switched on.
3. Never reveal too much personal or financial information… you never know who might see it, or use it and you can never be sure who's asking.
4. Don't click on links or open attachments if the source isn't 100% known and trustworthy.
5. Take your time and think twice, because everything may not be as it seems. You should also consider gaining certification to the government's Cyber Essentials scheme which defines a basic cyber security standard and provides confidence in your

business’s ability to measure and reduce basic risks.

Qualifications

You should also consider gaining certification to the Cyber Essentials scheme which defines a basic cyber security standard and provides confidence in your business’s ability to measure and reduce basic risks.

For more information, visit www.gov.je

Download Keeping your business safe online

Relevant Links

- 10 steps to cyber security
- Systems that support your business
- GDPR - What will it mean for your business?
- Systems and Hardware
- Incoming Threats
- Your online behaviour
- Data Protection for SMEs
- Get Safe Online
- The National Cyber Security Centre

Keep up-to-date with business information, news and events
sign up for the Jersey Business newsletter.

Subscribe →