Your online behaviour

Equip yourself

Every organisation needs to equip itself with information and advice on managing online behaviour, information and cyber security in a world where we have become completely dependent on data and the internet.

Staff Policies

Virtually every organisation enables staff to access the Internet in order to carry out their day-to-day work. As with going online at home, the convenience and efficiency is balanced by a degree of risk, which must be minimised. The same goes for accessing the organisation's information systems.

Good technical security and staff training can reduce the incidence of issues, but effective staff policies are also essential because they make it very clear what is acceptable… and what is not.

Top tip:

You should consider seeking professional advice in drafting staff policies and changes to employee contracts. It is also worth obtaining advice about how to introduce new policies to staff and combine them with a training programme.

Follow this link for further information.

Supply chain

As your organisation grows and starts to work with more customers, suppliers and partners, you become a link in one or more complex supply chains. Being a desirable, trustworthy supplier or customer now extends far beyond delivering good products or services, providing great customer care and paying on time. Today's way of conducting business means that you must observe good practice (and in many cases, compliance) when it comes to cyber and information security because vulnerabilities put not only your own organisation at risk… but also that of the others up and down the supply chain.

Top tip:

It is essential that every organisation in your supply chain has secure systems and practices, can demonstrate this to the others in the chain, and also has confidence in the others in the chain.

Follow this link for more detailed information on keeping your supply chain secure

Backups

The information held on your computer systems and devices is probably irreplaceable. If it is lost or corrupted as a result of theft, being criminally compromised, physical damage or technical failure, your organisation faces potential multiple risks. These include business interruption (in the case of customer and supplier records, accounts files, emails and software programs), loss of revenue, loss of reputation, non-compliance with data regulations and negligence litigation. You and/or other people in the organisation could also be held individually responsible.

Top tip:

Correctly and regularly backing up your data will help to safeguard against the above eventualities.

Following this link for detailed information on the risks to your business and the types of backups available to you.

Staff training & behaviour

Educating your workforce is the main line of defence against online threats and breaches in information security. The best internet security software is of little use if employees do not know how to spot a phishing email, and the most robust firewall ineffective without proper password control.

Effective training is one of the best methods of ensuring online safety and defending against intrusion by cyber criminals because simple human error – ignorance, omission or relapsing back into bad habits – is one of the most common causes of a security breach. Employees need to be enabled to acquire security knowledge by using their own reason, intuition and perception in order to demonstrate the correct behaviours.

Top tip:

Get employees into the habit of asking themselves the following questions as second nature and knowing the correct answers:

1. What corporate data do I have access to?
2. What are the consequences of a breach to the organisation / to me?
3. What are the risks?
4. What controls do we have in place?

Follow this link for detailed information on objectives, approach, induction training and general security.

Mobile devices

Every organisation relies heavily on mobile devices – smartphones and increasingly tablets – to maintain efficient communication, both with customers and suppliers, and connection with the business itself. This applies as much to data usage as it does to voice as effectively, today's mobile devices provide similar functionality to computers.

However, the many benefits of mobile working are countered by a number of specific risks – many arising from this substantial functionality.

The risks of using mobile devices in your business can in turn lead to other issues such as various types of fraud, identity theft, data theft, compromised employee security, loss of reputation, non-compliance with data regulations and even blackmail or being held to ransom (either corporate or individual).

Top tip:

Ensure mobile users are responsible for their behaviour and actions and include the use of mobile devices on company business in the company handbook.

Follow this link for advice and detailed information on using mobile devices for your business

Social media

Many of the risks associated with social networking / social media arise from having such a large and, in many cases, unknown group of people with whom you are interacting, and an effectively un-moderated forum.

Your organisation and its employees can avoid the risks and use social networking/social media safely by following a few sensible guidelines in the link below.

Top tip:

Ensure you have effective and updated internet security software and firewall running before you go online. Ensure your staff are on guard against phishing, vishing, and other social engineering activity aimed as getting social media passwords.

Follow this link for more detailed information on how to avoid the risks and for best practice guidelines when using social media for your business.

Data loss

Preventing your data from loss or falling into the wrong hands should be a key part of your IT strategy. The consequences of such events can include breaches of confidentiality, non-compliance penalties, espionage, financial losses (to your business, employees and customers) and compromised reputation.

Top tip:

Control who has access to your data by setting access levels.

Follow this link for information on the risks and how to protect your data.

Fraud

Businesses and other organisations can be affected by many types of fraud, and it is essential to ensure that you are aware of the risks in your particular organisation, and how to identify and prevent it.

Top tip:

Reconcile bank statements and company credit card statements meticulously and regularly.

Follow this link to understand the risks and how to protect your organisation from fraud.

Downloading and file sharing

Downloading is a commonplace and very convenient way to obtain and update software as well as documents, pdfs, video, photos, and other files. Downloading is different from streaming, which is where video, music or sound is sent over the internet for you to watch or listen to in real time, rather than being able to be saved on your computer to use later.

Top tip:

Ensure effective and updated internet security software and firewall are installed and running before any downloading takes place. Follow this link to for information on the risks of downloading and how to safely download and file share.

Relevant Links

- Supply Chain
- Backups
- Staff Training
- Mobile Devices
- Social Networking / Social Media
- Data Loss Prevention
- Fraud
- Downloading & File Sharing
- Get Safe Online
- The National Cyber Security Centre
- Keep your business safe online
- Systems and Hardware
- Incoming Threats

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

Subscribe →