Systems and Hardware

Securing your systems

How can businesses ensure IT security and find reliable support when needed?

When running your business you must establish and maintain the appropriate levels of safety to safeguard IT systems, devices, business and employees against issues relating to online and information security. You also require support for your actual technology, computers and servers, mobile devices, infrastructure, software and middleware. It is vital to know where to obtain such advice, as well as having a dependable source of help if something does go wrong. You should find and engage a trustworthy IT support supplier who has been recommended by someone you trust, and who can demonstrate a sound capability in providing security advice and problem resolution.

IT Support

Choosing the right IT support partner is important and some research is required prior to making your decision so ask colleagues, suppliers, trade organisations and other companies who they use. You should also carry out an online search for ‘IT Support’ in your area.

In the context of cyber and information security support, if you can find a provider who also holds the relevant qualifications and industry body memberships, you could use that provider for both your IT and cyber/information security support requirements.

Tip tip:

When selecting an IT supplier get evidence that they have the relevant experience and can help as your business grows and your needs change.

Click here for more detailed information

Passwords

Passwords are the most common way for your organisation and the people in it to prove identity when carrying out company business. The use of strong passwords and their secrecy is therefore vital in order to protect the organisation's and individuals' security and identity.

Top tip:

The generation and use of passwords can be a complex so having a Password protocol and control should be a key part of your organisation's cyber and information security strategy.

Click here for more detailed information.

Upgrades

Systems

When new versions of operating systems are launched, such as Microsoft Windows, Apple OS X / iOS or Android, they are generally accompanied by improved usability, additional features and an enhanced user experience. However, cybercriminals quickly find vulnerable areas in the new operating system and continue to do so for the lifetime of the version. To counter this, the software companies release regular updates –such as security updates or critical updates which protect against malware and security exploits.

Software

As is the case with operating systems, cybercriminals quickly find vulnerable areas in other software and continue to do so for the lifetime of the version. This is more commonplace in mainstream packages used generically across many types of organisation, than

specialist, industry-specific programs.

To counter this, software manufacturers release regular updates such as security updates or critical updates, which protect against malware and security exploits. Other types of updates correct errors that enhance the software's functionality, and are not necessarily security related.

Top tip:

You will generally receive a notification from the software manufacturer in the form of an alert on your screen, that updates are available. You will normally be given the choice of whether to download and install the update immediately or later. Our recommendation is to download and install as soon as possible.

Follow this link for more detailed information on protecting your devices and systems and software updates.

Website protection

Whether your business operates an eCommerce or marketing website, it is essential to protect it against attacks from hackers as well as technical failure. The consequences of not doing so include loss of service, reduced revenue and damaged reputation.

Top tip:

If you are hosting your own website ensure that your hardware and software are secure by using strong protected passwords, an effective firewall is in place and monitor log files to spot any attempts at intrusion.

Follow this link for more detailed information.

Disposal

Your computers, tablets and smartphones are used to store and communicate data which – if in the wrong hands – could be used to compromise the safety and security of your organisation and its employees. This data could be stored on the device itself, or accessible in the

form of internet bookmarks, remote network access, or via email and social networking contacts.

It is vital, of course, to safeguard this data whilst devices are in use, but equally important to ensure that computers, tablets and smartphones do not remain vulnerable at the end of their life. This is done by disposing of them correctly. Even data which you may think has been safely deleted can be retrieved with relative ease by both dedicated criminals and skilled opportunists.

Top tip:

If a device is at the end of it's life it should be dismantled and disposed of properly. Contact your IT support supplier who can help with the disposal.

Follow this link for more detailed information.

Relevant Links

- Get Safe Online
- The National Cyber Security Centre
- Systems that support your business
- Keep your business safe online
- Your online behaviour

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

Subscribe →