Incoming Threats

Protect your business

Every organisation relies on the internet to some degree or another for communications, transactions, payments and data access. Unfortunately, however, the internet has also become a channel of choice for criminals to commit financial and other crimes. Your organisation must take precautions to protect itself from incoming threats.

Malware

The term malware refers to software designed and distributed to gain unauthorised access to computers and other connected devices, disrupt their normal operation, gather sensitive or confidential information or spy on the device's users.

The most common types of malware are:

- Viruses
- Spyware
- Ransomware

Virus

A virus is a file written with the intention of doing harm, or for criminal activity. Some are noticeable to the computer user, but many run in the background, unnoticed by the user. There are many types of virus. A worm, for example, can exploit security vulnerabilities to spread itself automatically to other computers through networks.
A Trojan horse (or simply 'Trojan') is a program that appears harmless but hides malicious functions.
Potentially, a virus could arrive on your device in the form of a Trojan, with the ability to replicate itself before moving on to another device (a worm) and also be

designed as a piece of spyware.

Top tip:

Ensuring that you have internet security software and that it is up to date will automatically protect you against any existing or new threats to your systems.

Follow this link for more detailed information on how to mitigate these threats.

Spyware

Spyware is a type of virus that is specifically designed to steal information about your activity on your computer or other device. Spyware writers have a number of different objectives, mainly fraudulent financial gain or identity theft. Spyware can perform a number of illicit functions, from creating pop up advertisements to stealing your bank login details by taking screen shots of the sites you visit and even logging the keys you type (known as a keylogger). Spyware may also be self-replicating. An increasingly common form of spyware is a Remote Access Trojan (RAT), via which a fraudster or other cybercriminal can take over control of infected devices remotely and use it as if he / she were the authorised user. This can include activating webcams and physically spying on users' actions.

Top tip:

Ensuring that you have internet security software and that it is up to date will automatically protect you against any existing or new threats to your systems.

Follow this link for more detailed information on how to mitigate these threats

Ransomware

Ransomware

Ransomware is an insidious form of malware which enables cybercriminals to lock down a computer or other device remotely, then charge a ransom to 'unlock' it.

Other types of malware include rootkits,

dishonest adware and scareware.

Top tip:

Ensuring that you have internet security software and that it is up to date will automatically protect you against any existing or new threats to your systems.

Follow this link for more detailed information on how to mitigate these threats

Social Engineering

Social Engineering is the route to many types of crime including fraud and identity theft. It refers to the act of manipulating or deceiving someone into certain actions including divulging personal or financial information … a kind of confidence trickery. It exploits elements of human nature such as fear of loss, being protective, wishing to be helpful, or obliging others. There is seemingly no limit to the elaborate lengths that fraudsters will go to in order to achieve their ends. Social engineering is designed to be highly convincing, with hoax approaches emulating normally trustworthy sources such as your bank, the police or a government department and often made more convincing by the presence of information already held about you or your business by the fraudster.

Types of Social Engineering include:

- Phishing
- Vishing
- Identity Theft
- Baiting

Phishing

Responding to a fraudulent email claiming to be from your company's bank or credit card provider, a government department, a membership organisation or a website you buy from, directing you to follow a link to supply confidential details – typically a password, PIN or other information

Top tip:

Never click on links in emails from unknown sources. Roll your mouse over the link to reveal its true destination, displayed on the bottom left corner of your screen. If it is different for what is displayed in the text of the link do not open it and report to your service provider.

To avoid social engineering attacks, follow this link for more detailed information

Vishing

Supplying details to a fraudster who has phoned your company claiming to be from your bank or credit card provider or the police and inventing a problem. They ask for confirmation of confidential information in order to solve the problem. This is known as vishing. They may additionally despatch a 'courier' to collect payment cards or other records, known as courier fraud.

Top tip:

If you are asked by such a caller to cut off the call and phone your bank or card provider, call the number on your bank statement or other document from your bank – or on the back of your card – but not one given to you by the caller, nor the number you were called from.

To avoid social engineering attacks, follow this link for more detailed information

Identity theft

Receiving a phone call from somebody claiming to be a legitimate support agent for your computers or software, and telling you that you have a technical issue. They sound genuine, so you or a colleague gives them your login details – which can result in fraud or identity theft. Alternatively they are granted remote access to take over your computer or network, resulting in it being infected with malware. People claiming to be from 'IT support' in your business may request your or colleagues' passwords in order to infiltrate company systems and data.

Top tip:

If you receive a phone call requesting confidential

information, verify it is authentic by asking for a full and correct spelling of the person's name and a call back number.

To avoid social engineering attacks, follow this link for more detailed information.

Baiting

Picking up and inserting into computers USB sticks, memory cards, CD-ROM/DVD-ROMs or other storage medium that has been deliberately left lying around and contains malware.

Top tip:

Do not attach external storage devices or insert CD-ROMs/DVD-ROMs into computers if their source is uncertain.

To avoid social engineering attacks, follow this link for more detailed information.

Relevant Links

- Malware
- Get Safe Online
- The National Cyber Security Centre
- Social Engineering
- Keep your business safe online
- Systems and Hardware
- Cyber Essentials
- Your online behaviour

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

Subscribe →