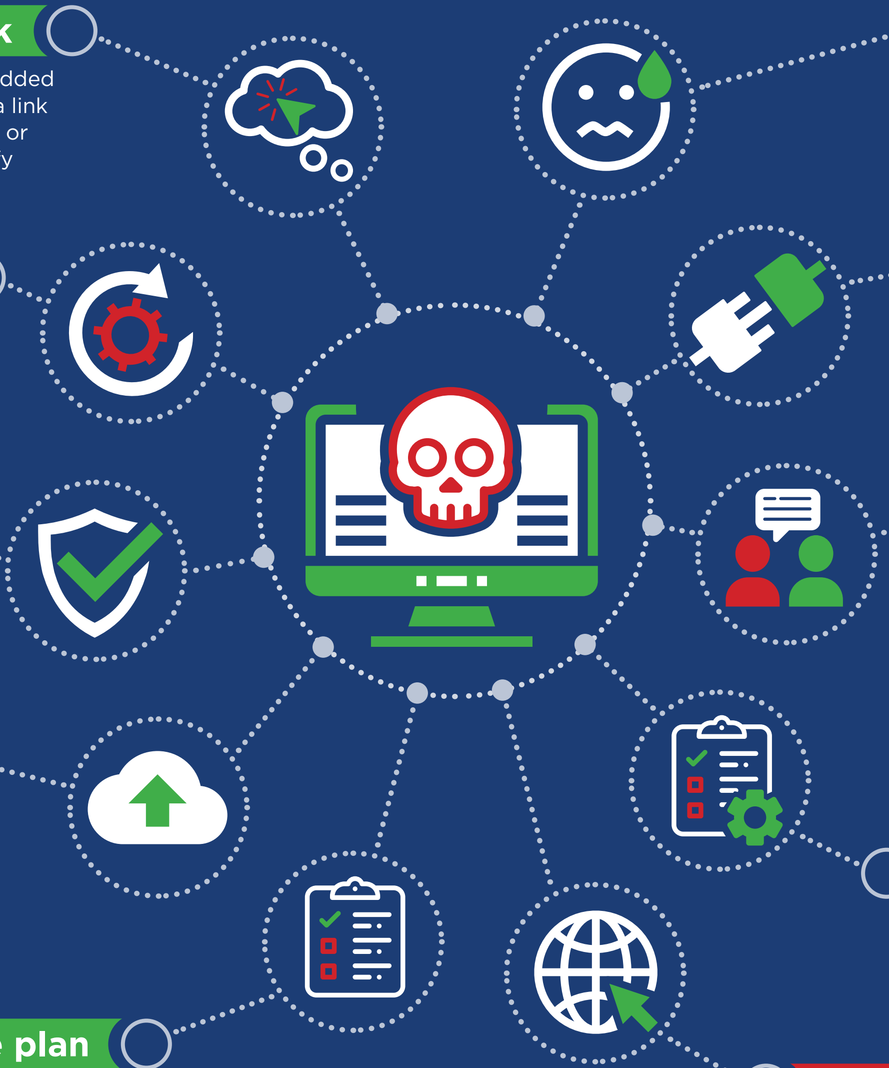
MANAGING A BREACH – RANSOMWARE

PDSC
POLICE DIGITAL SECURITY CENTRE

Here are five tips from the Police Digital Security Centre (PDSC) on **HOW TO PROTECT YOU AND YOUR ORGANISATION** from a potential ransomware attack.

If you and your organisation **ARE EXPERIENCING A RANSOMWARE ATTACK,** here are five things you can do that may limit its impact.



Think before you click

Cyber criminals may use phishing emails, which are embedded with a ransomware virus, to manipulate you into clicking a link or opening an attachment and gain access to your device or system. Avoid opening any suspicious emails, always verify unsolicited emails and block all incoming phishing emails.

Software updates

Ensure that you always have the latest software updates installed on all your devices and apps. These security upgrades are essential in protecting your device from viruses and reducing the risk of being targeted by a ransomware attack. Therefore, set all your devices to receive and install updates automatically.

Install Anti-virus

Install and activate anti-virus software on all your devices, preferably set it to update automatically. This will help you to run a complete scan of your system and check for any malware infections.

Back up

A ransomware attack aims at locking you out of your devices or network and keeping your files hostage. The ransom note will usually require you to pay an amount for them released back to you. To safeguard your most important personal data and information, back them up to an external hard drive or cloud-based storage system to avoid any losses in an event of an attack.

Develop an incident response plan

Preparation is key. Having an incident response plan in place will help minimise the damage caused by a ransomware attack. There are five crucial elements needed for a plan: Identify, Protect, Detect, Respond and Recover. This will allow you to set out plans for disaster recovery, ensuring business continuity, crisis management and technical capabilities.

Don't panic!

Maintaining a clear head will help you identify what the issues are and allow you to take appropriate actions to help avoid the virus from spreading further.

Disconnect the infected device

Once you have identified the infected device(s), you should disconnect them immediately from all network connections, whether wired, wireless or mobile phone based. This will help to stop the spread of the virus to other devices.

Notify your staff

As an employee or employer, it is important to notify the rest of your staff of the breach immediately, including your IT department. It is important to encourage reporting from your staff and to not punish them if a breach occurs. This way everyone in your organisation is informed quickly and can help prevent the spread of the ransomware by following the incident response plan accordingly.

Activate incident response plan

If you have one in place, this should be activated immediately, as a well planned and executed incidence response plan can help minimise the damage of the attack.

Report it

Anyone experiencing a ransomware attack should contact Action Fraud immediately at www.actionfraud.police.uk. They have a 24/7 live cyber reporting hotline specifically for businesses.