Backup Systems

TOP TIPS TO PROTECT YOURSELF FROM RANSOMWARE

What is Ransomware

Ransomware is a malicious software created by cyber attackers which blocks a users access to their data until a ransom is paid. Initially aimed at individuals, cyber attackers are now targeting businesses, with more and more being attacked each day.

Every 40 seconds, a company is attacked by ransomware

Almost 3/4 of those organisations have no protection or backup

In the UK alone, £4.5m was lost to ransomware attacks

Backup Systems

1.

Backup Systems

Don’t think you’re invisible - or invincible

The first step in protecting your organisation from ransomware is acknowledging that the risk of your organisation becoming a victim of a cyber-attack exists. From small businesses with only a handful of employees to Fortune 500s or giant public sector organisations, no one is exempt.

Once organisations recognise that they may become a potential target, appropriate defensive and preventative measures can be put in place.

However, it must also be acknowledged that even with these security measures in place an attack may still slip through making quick acting recovery protocols an essential component of business continuity.

2.

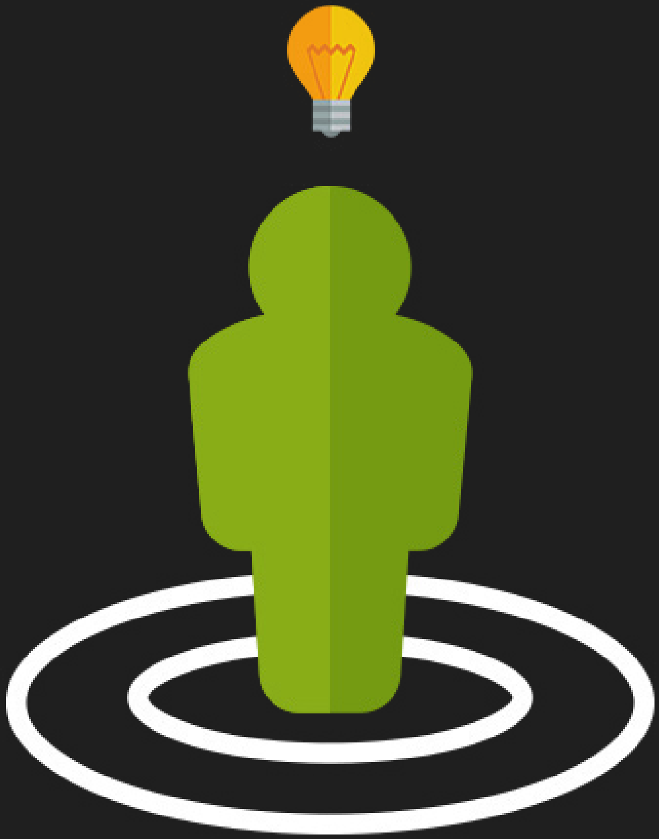
Install cyber security measures; your antivirus is your best friend

Cyber-attacks are growing in sophistication, no longer are they just underhand attacks performed for notoriety, but instead highly targeted attacks designed by highly skilled criminals whose methods are becoming increasingly more professional.

The number of these modern and advanced attacks are growing, exploiting multiple attack vectors including user behaviour, applications and systems. Organisations must continually take into consideration these vectors and ensure that the latest cyber security measures are in place and are up to date.

Backup Systems

3.



Educate your users and your staff – including your remote workforce

Many cyber security threats, such as advanced malware, can only be countered with sophisticated technology. But on a day-to-day basis, employees are typically your greatest source of vulnerability.

Making sure your IT security policy is sophisticated and comprehensive enough to cover all possible sources of attack is the first priority. Whilst alongside this, a clearly documented remediation plan is critical for disaster recovery processes.

While having these protocols in place is essential, it is also important to ensure that employees are educated in and aware of the potential risks and consequences. New employees must be trained in company policy and the existing workforce must be refreshed in any changing standards and procedures, outlined by the company IT security policy.

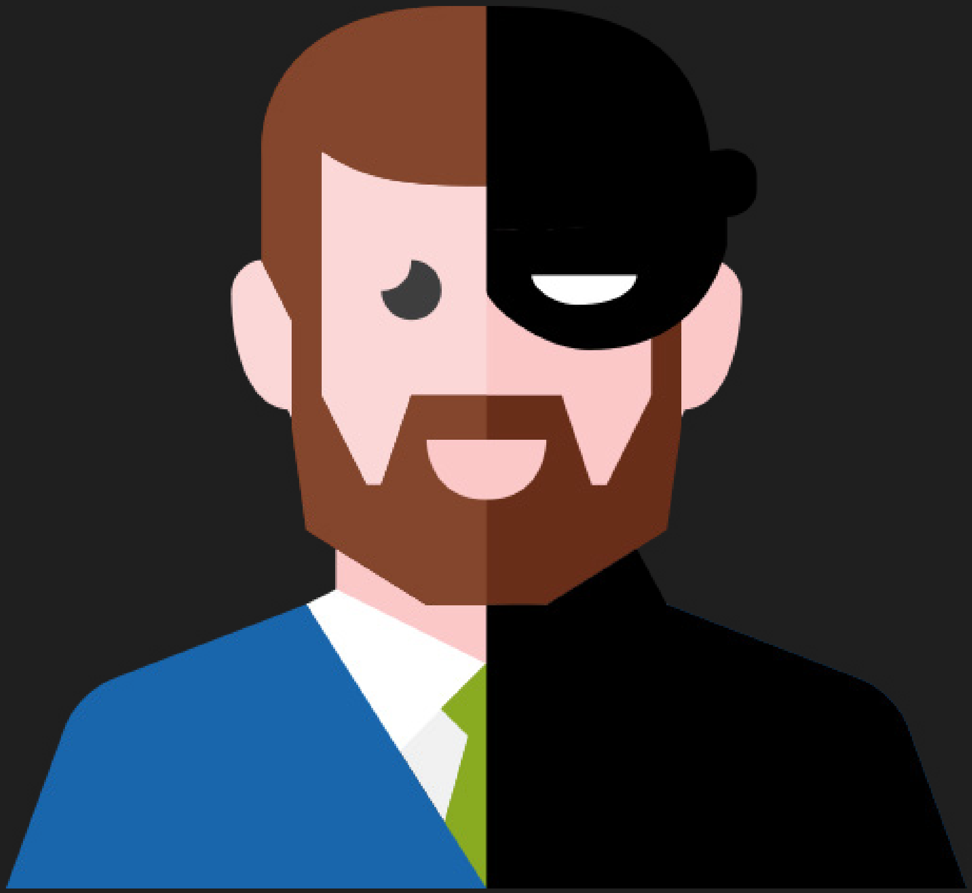
4.

Beware of phishing

For ransomware to succeed, hackers must download malicious software onto your organisation's network. Once your systems have been breached, the attack is launched and your files encrypted.

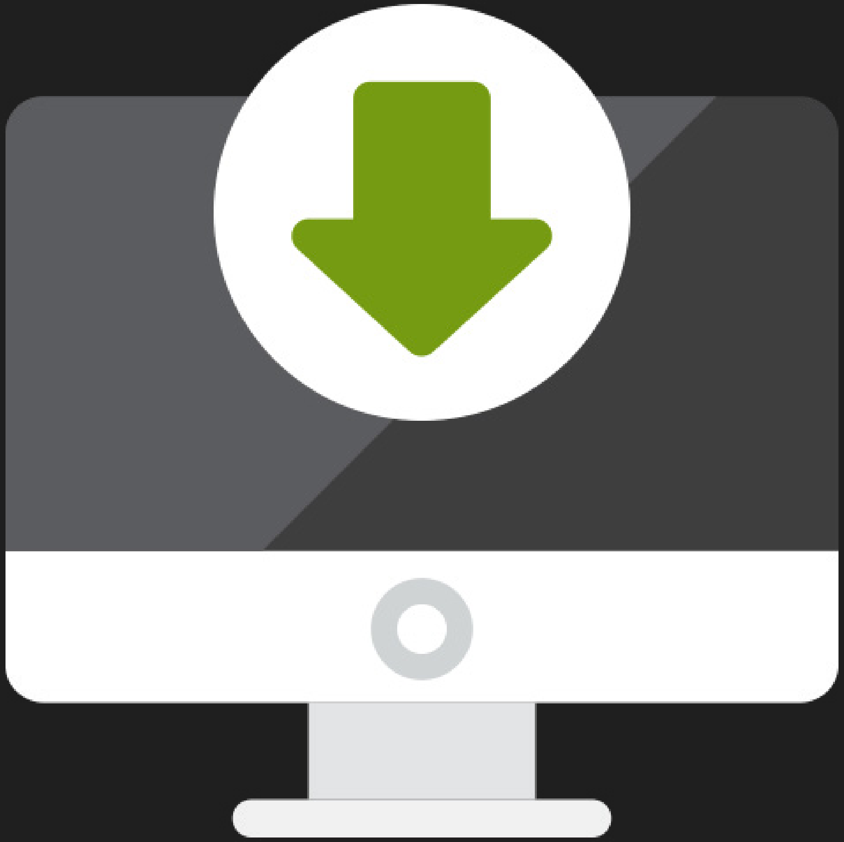
Phishing emails are one of the most common ways for software to be introduced into your network while other commonly reported ways include malicious adverts on websites and questionable apps and programs.

Employees should be educated in security best practices and to follow an established protocol when opening unsolicited emails or visiting websites they are unfamiliar with. Procedures should also be established for reporting suspected network breaches along with first response protocols.



Backup Systems

5.



Keep up to date with your system updates

The Wannacry ransomware attack which infected hundreds of thousands of devices in countries all-round the globe highlighted the vulnerabilities of a system not running up to date software and patches.

The criminals behind the WannaCry attack took advantage of the Windows exploit known as EternalBlue. This exploit allowed the hackers to gain remote access to their victim's devices and install the encryptor, holding their data to ransom and disrupting critical systems.

The Microsoft security update patch, MS17-010, which addressed this vulnerability, had been available for over a month before the WannaCry attack; reinforcing the importance of keeping systems updated.

Backup Systems

Detect concealed threats

Threats and vulnerabilities could be everywhere; email inboxes filled with malicious attachments just waiting to release a malware out into your network. Making sure your infrastructure is scanned regularly to both detect and remove any latent or concealed threats is essential in maintaining a clean system.

6.

Backup Systems

7.

Develop an emergency protocol

Your organisation should develop an emergency protocol to ensure quick action is taken when a breach is first discovered. This will ensure that organisational down time is drastically minimised with proper procedures being actioned before your organisation is attacked and not during. These emergency plans should be regularly tested and reviewed to ensure they are effective, robust, and that all employees have the experience to efficiently react.

The protocol should take into consideration steps such as switching to backup servers, isolating your network, and going offline. It is also recommended that an emergency response team is put in place which consists of individuals from multiple departments, for instance IT, HR, Legal and Intellectual Property.

8.

Outsource your Backup Solution

If the recent cyber security hacks highlighted anything, it was that every organisation needs a data backup strategy against ransomware - and a good one! A simple, reliable backup system lets you recover from many attacks within minutes or hours, at a very low cost. When data is corrupted, encrypted, or stolen by malware, simply restore from backup and get back to business. You cannot predict when your system may be comprised, so do not risk it- back up your organisational data.

Keeping in mind that it is extremely unlikely that we have seen the last of these global cyber attacks, it is not enough for organisations to just go on the defence: they must be arming themselves with the essential data backup solutions to take a proactive approach that anticipates cyber attacks.

Backup Systems