Cyber Security

Jargon Buster

www.sharp.co.uk

SHARP

Be Original.

Complex security terms, simplified

Cybercrime can take on many different forms for businesses that stay connected digitally. Understanding what an attack looks like, how it can materialise, and the implications it can have on your business should not be underestimated.

But for many small and medium-sized enterprises (SMEs), without internal technical expertise, understanding the cyber security jargon and it's meaning can be the first hurdle to overcome.

To provide a better understanding, we've broken down some of these for you.

Network security

The steely padlock that protects your information

Similar to how you lock up your most valuable goods in a safe, or chain your bike to a wall, network security protects your business' sensitive information. Essential on any business network, your security protection should include an intrusion detection system (IDS), which is designed to keep an eye out for and identify potential threats, suspicious activity, and unauthorised access attempts on digitally connected devices, such as laptops and printers.

Data breach

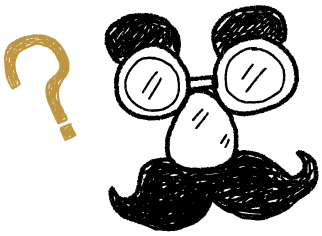
Kind of like someone pinching your wallet on the train

You might not always know it's happened until it's already in the wrong hands. A data breach is where sensitive information, whether it belongs to the company or a client, is stolen by bad actors (cybercriminals). This can occur without the business knowing or giving authorisation. A data breach can ultimately lead to a loss of trust from customers or users, damaged brand reputation and even costly fines.

Phishing, smishing and vishing

Basically: a hacker disguised as your boss, client, best friend or favourite clothes shop

These types of attacks may not always be obvious to the eye, but they are common. In fact, around 90% of cyberattacks begin with phishing (email), while the rate of smishing (SMS) and vishing (voice call) attacks is also rising. We've all seen those shifty looking emails pop up in our junk folder. Phishing, smishing and vishing are cyberattacks that trick users into clicking on emails, scanning QR codes, responding to messages, or answering calls that they think are legitimate. If the attack proves successful, employees will then unknowingly be duped into providing sensitive information like their network password.



Malware

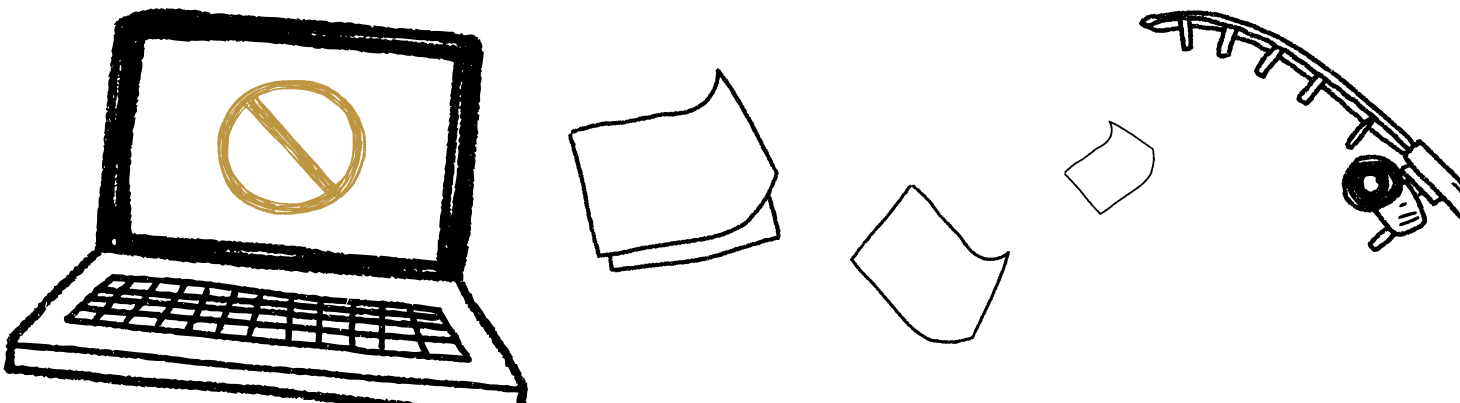
The evil kind of software, made only with bad intentions

'Malware' is short for malicious software. This is software designed by cybercriminals to cause harm to your business' network systems – and stop you from being able to use them. As a result of opening a phishing email, clicking on a suspicious link, or going to a website that has already been compromised, malware can infiltrate your system. Once it's done so, information stored on your network can be exposed to hackers, leading to an escalated attack.

Ransomware

Your data held hostage

A form of malware, ransomware is used by cybercriminals to withhold access to critical business information by encrypting it (scrambling it into code). Every type of digitally connected business owns data, from financial records to the test results of patients and confidential legal documents. Having access to it is crucial for the running of a business. However, once ransomware has infiltrated your network, your business can lose this access. To get it back, ransoms (costly fees) often need to be paid to the hacker perpetrating the attack.



End-point security

Essentially, making sure all your devices are just as secure as your desktop

Your digital defence doesn't start and end with your desktop. End-point security refers to the process of ensuring all of your 'endpoints'; from tablets to smartphones and other internet-connected devices (like your office printer), have shared protection. These should be centrally managed and monitored to guarantee there is a realistic view of your cybersecurity posture.

Encryption

Imagine all your data, jumbled up in a scrabble bag

How do you stop somebody reading a secret message? You mix up the words, letters, and numbers. This is essentially what encryption does. It encodes 'plain text' – your sensitive data – into 'cyphertext', which makes it unreadable to anyone without a 'decryption key', i.e. the passcode you use to access a secured wireless network. In a business, encryption should be applied to all devices, like your phone and laptop, so the content held on each can't be read if the device is lost or stolen.

Patch management

Think: updating your phone to the latest operating system

We've likely all encountered those software updates on our phones: 'update now to Windows 10', or 'install iOS 9,999'. However, these updates are a crucial security measure. Patch management is the process of applying updates to software, drivers, and firmware to protect vulnerabilities on the network. This involves compliance monitoring, managing the applications your business uses, and ensuring your systems are operating to their full potential.

Incident response

Your plan of action for fending off an attack

What's the first port of call when your business is compromised by a cyberattack? An incident response (IR) is the systematic approach taken by organisations that want to plan how to respond to and manage cybersecurity incidents effectively. Not having a solid IR approach in place for when a threat surfaces, can prevent your business from fighting it off – and is critical for maintaining the integrity, confidentiality, and availability of sensitive business data.

Stay secure and keep evolving

Though complex, understanding cybersecurity jargon is important for every digitally-connected business today.

Unfortunately, jargon evolves and grows as threats do. That's why engaging external technical expertise helps you take action and evolve in line with threats. Sharp offers complete security solutions and services for all organisations.

Discover more on the Sharp Security Hub.

Explore the hub