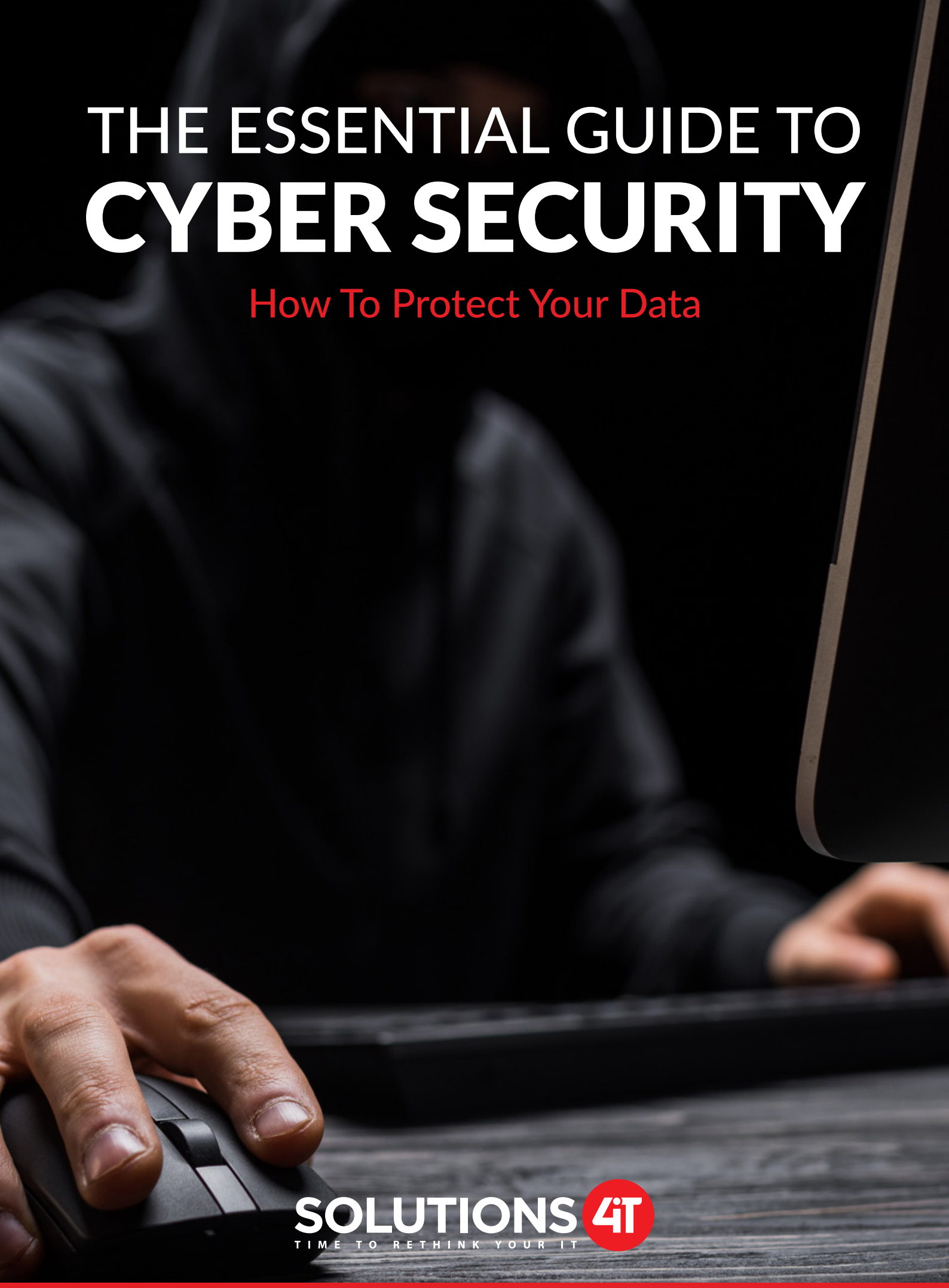


THE ESSENTIAL GUIDE TO CYBER SECURITY

How To Protect Your Data

SOLUTIONS 4IT

TIME TO RETHINK YOUR IT

www.solutions4it.co.uk | 0121 289 4477

CYBER SECURITY

In 2022

Cyber Security 2022:

What do you need to know?

The cyber threat is significant and growing at an alarming rate, yet cyber-attacks are not always sophisticated. Frequent attacks succeed simply because of an ineffective cyber strategy and the exploitation of known vulnerabilities.

For every highly sophisticated hostile state attack such as SolarWinds, there are hundreds of low-level phishing, denial of service, and ransomware attacks. Raising cyber resilience, even if it is just the basics of ensuring good cyber security practices are implemented consistently, is the first line of defence against cyber-attacks.

During 2022 we will start to see Covid restrictions being lifted and a gradual return to the ‘new normal’ but the last two years of rapid workplace change has vastly increased the cyber risk for most organisations. The phrase ‘Cyber Pandemic’ has been used to describe this growing threat. Defining a cyber pandemic is a bit like defining a “perfect storm” only this storm is in cyberspace.

THE CYBER PANDEMIC

How has it increased security threats?

How have organisations been affected?

The increase in remotely working from home has highlighted how important technology is to enable this, unfortunately the safeguards for this are not fully in place. Cyber criminals know this and will take advantage of unprepared workforces.

Cyber-attackers see the pandemic as an opportunity to step up their criminal activities by exploiting the vulnerability of employees often through targeted coronavirus related phishing campaigns.

Criminal gangs have transitioned from other illegal activities and are now focussing and investing more in cybercrime. The Pandemic has been lucrative for these gangs, they are inventive, and their cyber-attacks will continue.

Increased financial burden and shifting priorities for organisations has resulted in less spending on cyber resilience and expertise.

CYBER STRATEGY

& Risk Management

Our Key Recommendations

1/ Review your approach to risk management and ensure that a cyber security strategy is fully integrated and prioritised when it comes to business planning and decisions.

2/ We recommend implementing a comprehensive multi-layered cyber security strategy.

3/ No method of protection is ever 100% safe, so you need to ensure that every base is covered when it comes to the security of your employees, data, and devices.

The knock-on effect of a data breach can be devastating for a company. When customers start taking their business and their money elsewhere, that can be a real body blow.

LEARN MORE ABOUT YOUR BUSINESS BECOMMING CYBER ESSENTIALS CERTIFIED

THE TOP 4

Security Threats To Your Business

Social Engineering and Email Phishing

Social engineering in cybercrime means manipulating people so they give up confidential information. The types of information these criminals are seeking can vary, but when individuals are targeted, the criminals are usually trying to trick you into giving them your passwords or bank information or access your computer to secretly install malicious software.

Phishing is a type of social engineering in which a user or users are contacted by email, telephone, or text message to lure individuals into providing sensitive data such as personally identifiable information, banking/credit card details, and passwords.

Data Breach

A data breach exposes confidential, sensitive, or protected information to an unauthorised person. The files in a data breach are viewed and/or shared without permission.

Anyone can be at risk of a data breach — from individuals to high-level enterprises and governments. More importantly, anyone can put others at risk if they are not protected.

As our computers and mobile devices get more connective features, there are more places for data to slip through. The assumption is that a data breach is caused by an outside hacker, but that's not always true.

Reasons for how data breaches happen might sometimes be traced back to intentional attacks. However, it can just as easily result from a simple oversight by individuals or flaws in a company's procedures.

Ransomware

Ransomware is a form of malware designed to encrypt all data on a computer, rendering any files and the systems that rely on them unusable. Cyber criminals then hold the data at ransom, demanding a financial reward in exchange for a decryption key that will make the data accessible again.

Ransomware incidents can severely impact business processes and leave organisations without the data they need to operate and deliver mission-critical services. The economic and reputational impacts of ransomware incidents, throughout the initial disruption and, at times, extended recovery, have also proven challenging for organisations large and small.

The best way to avoid ransomware attacks is to have the right technology in place to prevent cyber criminals infiltrating your systems in the first instance.

Malware Attacks

Malware is one of the most common threats facing business of all sizes. It encompasses a variety of cyber threats such as trojans and viruses. Malware is a varied term for malicious code that hackers create to gain access to networks, steal data, or destroy data on computers. Malware usually comes from malicious website downloads, spam emails or from connecting to other infected machines or devices.

These attacks are damaging for businesses because they can cripple devices, which requires expensive repairs or replacements to fix. They can also give attackers a back door to access data, which can put customers and employee's data at risk. Due to working from home there has been a recent increase of employees using their own devices for work, as it helps to save time and cost. This, however, increases their likelihood of suffering from a malware attack, as personal devices are much more likely to be at risk from malicious downloads.

KEEPING YOUR DEVICES SECURE

It is essential to ensure that you have the right technology in place to protect your devices from the latest threats and stop cyber criminals gaining access to your data. Here are our top tips:

1/ Malware Protection

The risk of malware, viruses, ransomware, and other malicious cyber-attacks is increasing. Which is why you need effective, business-level malware protection in place.

Malware protection software will continuously scan your devices for any malicious activity. If known types of malwares are spotted, it will kill them immediately, preventing them from causing disruption to your business. Furthermore, if the malware protection discovers evidence of a new, unknown virus, it can quarantine and allow for efficient removal.

For antivirus software to be most effective, it should be managed by a team of IT specialists. They will ensure your antivirus software is reliable; with a high detection rate but without slowing down your devices. This means you and your team can continue to work as normal, whilst your antivirus software and IT partner work together to deal with any potential threats..

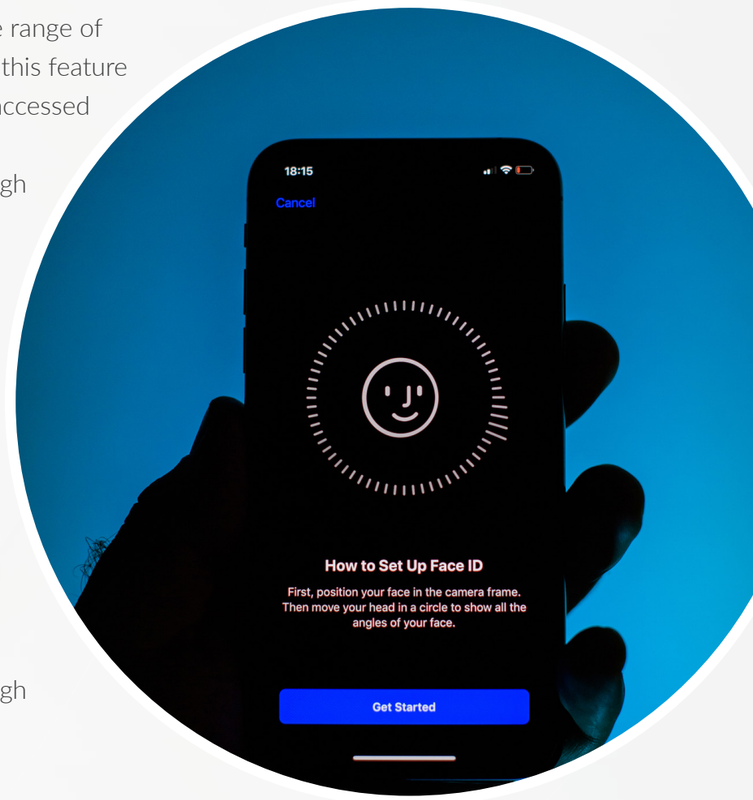
2/ Device encryption

When storing and accessing business data on laptops and mobile devices, it is essential to encrypt them. With the advent of the Covid pandemic and the introduction of remote work, the chances of the device being stolen or lost have increased dramatically.

Device encryption is the process of scrambling data into illegible code and making it indecipherable to anyone without a password or a recovery key, helping you protect your data.

Device encryption is available on a wide range of Windows and Apple Mac devices, once this feature is turned on the data can then only be accessed by people who've been authorised. This process can be centrally managed through your IT provider.
Device encryption is the process of scrambling data into illegible code and making it indecipherable to anyone without a password or a recovery key, helping you protect your data.

Device encryption is available on a wide range of Windows and Apple Mac devices, once this feature is turned on the data can then only be accessed by people who've been authorised. This process can be centrally managed through your IT provider.



3/ Mobile device policy enforcement

Lost or stolen mobile devices are the perfect opportunity for cyber criminals to compromise your data, resulting in lost files, reputational damage, breach of client confidentiality and potential fines from authorities.

An easy way to prevent this is to enforce controls on all devices that hold business data. For example, pins and passcodes can be enforced to grant employees access to their work email inbox. Not only is this easy to roll out, but it will also add a valuable layer of protection to your mobile devices, helping to protect again cyber criminals.

4/ Connect to Secure Wi-Fi

The beauty of mobile devices is that we can access the internet anywhere and everywhere we go. One of the first things we do at a restaurant or friend's house is search for Wi-Fi. While free Wi-Fi can save us on data, it's important to be wary of unsecured networks.

The use of a corporate Virtual Private Network (VPN) can help ensure that any data being transmitted by the device is secured and within the control of your organisation.

5/ Keep Your Device's Software up to date

Mobile phones, laptops and tablets all require regular operating system updates. Often these updates contain user experience upgrades but also crucially they patch the OS for any security issues.

Users tend to click through quickly or ask the device to remind them in the future, it's important to stay up to date. These updates can protect both iOS and Android devices from newly discovered threats. To check if your phone's OS is up to date, go to "about phone" or "general" and click "system updates" or "software update."

Updates can be centrally managed by your IT provider to ensure compliance with your company policies. It can even be configured to not allow any personal device that your employee owns from accessing company data unless it's up to date.

WANT TO KNOW MORE ABOUT SECURE REMOTE ACCESS?

KEEPING YOUR EMAILS PROTECTED

Here are some of our top recommendations for keeping your emails secure.

Email continues to be considered one of the main gateways for cyberattacks in businesses, organisations, and government institutions. Business email compromise and ransomware are the most dangerous attack types, and every year hackers use more deceptive methods to achieve their goals. Data theft, espionage, and the installation of backdoors are also a serious threat to government institutions and industry of all sizes.

It's therefore crucial that you have the right measures in place to protect any data used in email communication, preventing data loss, unauthorised access, or compromise.

1/ Email Filtering

Email filters are designed to identify incoming spam and malicious emails. Attackers often use emails as part of a phishing campaign, designed to get you to click on a link that downloads malicious software onto your computer or send you to a dangerous site with the intent of harvesting your username and password. Spam may contain relatively harmless content but can clutter up your inbox, consuming valuable space and making it more difficult to identify important, useful emails. Spam filters can detect spam emails. These helpful tools can recognize patterns that spam emails tend to follow.

A professionally managed email security solution will block spam and malicious emails before they reach your inbox. These emails will then be quarantined, which you can review so that if any legitimate emails have been blocked, you can release them into your main inbox. This reduces your risk of becoming a victim to cyberattack, as well as giving your employees more time to focus on important tasks.

2/ Microsoft 365 Security Audit

Email filters are designed to identify incoming spam and malicious emails. Attackers often use emails as part of a phishing campaign, designed to get you to click on a link that downloads malicious software onto your computer or send you to a dangerous site with the intent of harvesting your username and password. Spam may contain relatively harmless content but can clutter up your inbox, consuming valuable space and making it more difficult to identify important, useful emails. Spam filters can detect spam emails. These helpful tools can recognize patterns that spam emails tend to follow.

A professionally managed email security solution will block spam and malicious emails before they reach your inbox. These emails will then be quarantined, which you can review so that if any legitimate emails have been blocked, you can release them into your main inbox. This reduces your risk of becoming a victim to cyberattack, as well as giving your employees more time to focus on important tasks.

3/ Think Before You Click

Professional cyber-attacks via email are very difficult to detect, but there are a few clues for detecting fraud.

First of all, if a fraudulent email is suspected, verify whether the sender address actually matches the original domain. Consider carefully whether the sender is really an acquaintance or business partner of yours or whether the email address only resembles that of the actual person.

Check for spelling and grammar mistakes, especially if the email is supposed to come from a reputable company. An impersonal form of address in the cover letter, such as "Dear Ladies and Gentlemen," is another clue.

Be careful with links or buttons placed in emails, because as a "normal user" it is very difficult to check whether the apparent link target is correct. In case of doubt, it is safest not to click on any attached link.

4/ Email Back-Up

Email backup helps prevent data loss by enabling users to restore email content that potentially has been deleted or lost whether accidentally or through malicious intent.

Backups keep your email messages available in the event of a compromise and make tracking down lost emails much quicker.
Email providers themselves offer very limited protection against accidental data loss.

In fact, Microsoft advise all businesses to have third party back up in place. Which is why we recommend implementing an effective email backup solution.

5/ Two Factor Authentication (2FA)

With Two Factor Authentication (2FA), you add an extra layer of security to your account in case your password is stolen. After you set up 2FA, you'll sign into your account in two steps using: Something you know, like your password. Something you have, like your phone.

Typically, a code will be sent to your phone through text message which then needs to be entered when prompted for. Microsoft also have an Authenticator App which can be installed on your phone and will prompt you to approve a sign in on your account.

If a scammer has somehow managed to get your password, they will not be able to access your email, since they will not have your mobile device to approve the sign in.

6/ Vulnerability Scanning

Vulnerability scanning is the process of identifying security weaknesses and flaws on devices and software running on them.

By using a vulnerability scanner to identify the points of weakness in your systems, you can reduce the attack surface that criminals might exploit, focusing your security efforts on the areas that are most likely to be targeted.

EMPLOYEE TRAINING & BEST PRACTICES

Considerations to apply to your business and continued professional development plans.

The human factor is often the weakest link in an organisation's security. So, it's crucial your staff are trained to recognise potential threats quickly and deal with them effectively.

It's also important that procedures are put in place regarding all end user's passwords and data access to further prevent valuable personal or financial data from being stolen. Here are some of our top recommendations for keeping your employees secure.

1/ Cyber Security Awareness Training

Cyber security staff awareness training is an effective way to educate employees and ensure proper procedures are followed. It reduces risk and keeps your organisation's data safe against cyber-attacks.

Training typically consists of training videos and multiple-choice questions that show employees how to differentiate between something that's malicious and something that's legitimate.

Email phishing campaigns are also a great way to test their ability to identify potential threats in a real-life situation. Those who do click on potentially harmful links in spoof emails will be enrolled into compulsory extra training to ensure their knowledge is refreshed.

Regular group training events and incorporating the procedures and company policies into the company handbook are also great ways to build a culture of security within your business.

2/ Dark Web Monitoring

The term "dark web" sounds ominous, and there's a reason for that. The dark web is a part of the internet and made up of hidden sites that you can't find through conventional web browsers. It is often used for illegal activities including sharing compromised usernames and passwords.
Dark web monitoring is the process of searching for, and tracking, your organisation's information on the dark web. If any information is found, you will be alerted.

If you store any personal information online, it's possible it has made its way to the dark web. Hackers and identity thieves launch cyber-attacks and phishing scams to try to access your sensitive information. You've probably heard about breaches of large companies on the news. When these breaches occur, the hackers gain access to your information and try to resell it on the dark web.

3/ Password Managers

We all know that we need to use complex, varied passwords to protect against cyber-attack. But the truth is that many employees continue to reuse simple passwords across multiple sites because they're easier to remember.

A password manager enables your employees to store, share and access login details in an encrypted vault. This simplifies the process of using complex passwords, encouraging employees to do so. Additionally, effective password managers will also offer the option to automatically generate passwords, ensuring that all new passwords meet security standards.

4/ Policy Management

Having a centralised place for all of your company's security policies is an effective way to ensure your staff know what to do if they encounter something suspicious or are unsure of something.

We recommend storing and amending documents in one centralised location, making it easy to find, send and revise different policies. This allows for easily tracking which users have viewed the documents and often incorporates electronic signing.

TOP 5 CYBER SECURITY TIPS

1/ Keep Your Software Up to Date

One of the most important cyber security tips to mitigate ransomware is patching outdated software, both operating system, and applications. This helps remove critical vulnerabilities that hackers use to access your devices. Here are a few quick tips to get you started:

Turn on automatic system updates for your device
Make sure your desktop web browser uses automatic security updates
Regularly audit by using a vulnerability scanner

2/ Use Anti-Malware Protection & Firewall

Anti-Malware protection software can stop many attacks in their tracks by blocking malware and other malicious viruses from entering your device and compromising your data.

Using a firewall is also important when defending your data against malicious attacks. A firewall helps screen out hackers, viruses, and other malicious activity that occurs over the Internet and determines what traffic is allowed to enter your device.

3/ Multi-layered Cyber Security Strategy

Only having a firewall and anti-virus software doesn't provide enough resistance against increasingly sophisticated cyber-attacks.

A multi-layered security approach means having several different levels of security to protect your data and systems. This means that each security level has a backup in case of a breach, and the strengths of the layers taken as a whole help to cover any flaws in individual components.

4/ Robust Cyber Security Policy

Ensure you have a robust cyber security policy outlining potential risks and the technology and procedures in place to mitigate these risks. Ensure that this is reviewed and amended regularly in line with business and industry updates. A third-party assessment of this policy and others would also be beneficial.

5/ Managed Security Partner

A managed security service provider (MSSP) provides outsourced monitoring and management of security devices and systems. Common services include managed firewall, intrusion detection, virtual private network, vulnerability scanning and anti-viral services. Ensure they have the right certifications and credentials to be able to offer you the very best cyber security solutions available

RAISE AWARENESS IN YOUR BUSINESS WITH OUR CYBER SECURITY TRAINING


SOLUTIONS 4IT
TIME TO RETHINK YOUR IT