

Your Essential Guide to Cyber Security



Your Essential Guide to Cyber Security



Introduction

The best way to prevent a cyber security incident is to invest in robust Cyber Security. Similar to the way you would invest in a strong door, windows, alarm and CCTV for your physical office.

Data is one of the most valuable assets of any business and every business needs to take data security seriously and protect data from unauthorised access, theft, or loss.

Technology is the first line of defence, and IT experts are best placed to know the current and emerging threats and how to protect against them. The world of technology evolves quickly, and it would be difficult for a business owner to keep track of all the emerging cyber threats.

For that reason it is advisable to get expert advice and use a Managed Service Provider (MSP) to oversee your IT security, but here is a run down on best practice and what to consider when assessing your risk.

Only 31% of UK businesses have done a cyber security risk assessment in the last 12 months

How to optimise your data security

Keep updated

All systems and PCs must be kept up to date. Software updates are often released specifically to address a security flaw that has been found. Not updating a device or system

Your Essential Guide to Cyber Security

can leave it wide open to attack. It is best practice to set devices to automatically update where possible (such as phones and computers). Other devices should be manually updated whenever a software update is released.

A report to show which devices have been updated is a useful document for businesses to have to hand when reviewing security.

Check your firewall

A good firewall monitors and protects network traffic, providing the very first line of defence for your systems to make sure that none of the traffic that accesses the network is malicious or harmful. It is therefore important that the firewall is set up correctly and maintained to make sure it still meets your requirements. Has your firewall been effectively blocking malicious activity? Does it have the latest update?



Enhance your email protection

Most business will have Anti-Spam but there are now more stringent measures that can be implemented to provide a suite of protections for data coming into your inbox. These include email filtering, impersonation protection, and domain fraud protection.

Anti-spam is still important but business should consider adding in more protection based on advice and risk.

Endpoint protection

Modern endpoint protection is vital for keeping your devices and data safe from cyber threats. Traditional anti-virus software can't cope with the complex and changing attacks that target your endpoints. Modern endpoint protection offers comprehensive and proactive security that uses artificial intelligence, behavioural analysis, and cloud-based threat

Your Essential Guide to Cyber Security

intelligence. It can spot and stop malware, ransomware, phishing, zero-day exploits, and other advanced threats that can harm your business.

Manage access and passwords

Setting up who has access, access policies and password management is a key protection to get in place for any business.

51% of people use the same passwords for both work and personal accounts

Remembering complex passwords no longer needs to be restricted by an individual's brain power! Password managers can generate a suitable password (that follows your policy) and store it in a safe and secure way.

An MSP can advise on the best practice for access management and password policies, as well as giving your team access to training on passwords and other security threats.

Enable multi-factor authentication

Enabling multi-Factor Authentication will provide an extra layer of security to your login process. When you log into an account you are sometimes asked to verify with a code that it is really you that is logging in. This is MFA.

There are many different types of MFA methods but the most popular include entering a one-time text code to your mobile or using your fingerprint or facial recognition to prove that it is you. An MSP can guide you through setting this up and advise on the best option for your team.

Take regular backups

Taking regular data backups, including offsite backups, are a vital way to protect company data. A backup means valuable company data can be restored to the level of data that was present at the last backup.

Therefore, a regular backup is vital, but backup monitoring and backup tests are just as key and check everything is working if the backup is required.

Reduce human error

There are many options now for putting in place regular training and phishing simulations to increase and test the knowledge of your team. Phishing emails are becoming more advanced all the time so it is important that training refreshes and updates knowledge of the methods used on a regular basis.

Your Essential Guide to Cyber Security

Consistent security awareness training was proven to reduce employee phishing susceptibility from 60% all the way down to 10% within the first 12 months

Get certified

Businesses can show cyber security in their organisation by completing Cyber Essentials certification.

This is an annual assessment of your business against a minimum baseline standard, backed by government, and includes cyber liability insurance for businesses in the UK with a turnover of less than £20 million.

Monitor and test your network

An MSP can scan and monitor a network to detect threats to your system swiftly, enabling it to be isolated and dealt with immediately.

They will also be on hand to resolve any issues and can run vulnerability tests to identify any gaps in your security defences.



Let us help you get secure!

Data security is vital for any business that wants to succeed in today's digital age. However, it can be challenging to achieve and maintain. TechWyse can help you boost your data security so you can enjoy peace of mind, knowing your data is safe and secure.

If you want to learn more about how TechWyse can help you with your data security drop us a line today and we'll be happy to assist you.

t: 03332 400 660

e: info@techwyse.co.uk

Your Essential Guide to Cyber Security

References

Databasix

<https://www.dbxuk.com/statistics/data-breach-statistics>

Keepnet Labs

<https://keepnetlabs.com/reports>



**If you have more questions about
cyber security, or need some IT
advice, give us a call or send us an
email.**

**03332 400 660
info@techwyse.co.uk**