Xeretec IT Works

XERETEC IT SECURITY GUIDE FOR SMALL BUSINESSES

How to ensure the safety of your data, assets and reputation

Xeretec IT Works

IT SECURITY GUIDE FOR SMALL BUSINESSES

5 simple and affordable steps to help protect your business

CONTENTS

INTRODUCTION

IT Security can be a daunting prospect, you might be bamboozled with all the information that's out there and left wondering what to do and where to start?

With this in mind, we've created this IT security guide to help you understand the key areas you need to address, explaining everything in a language that everyone understands.

Many small businesses tend to think that it won't happen to them, their business is too small, and they would be of no interest to cyber criminals.

Contrary to this belief, there has been an increase in security threats to small business mainly because they tend to have less protection in place making them an attractive target.

THE STATS

There are more than 4 million cases annually of cyber-attacks against small businesses in the UK, and more than 50% of these come from phishing. [1]

If you're a small or medium-sized enterprise (SME) then there's around a 1 in 2 chance that you'll experience a cyber security breach. [2]

For micro firms with under ten employees, the median cost of all attacks in 2021 was just over £6,000. [3]

HOW TO IMPROVE YOUR CYBER SECURITY

Whilst cyber security is one of the top risks businesses face today, there are some simple and affordable steps you can take to significantly increase your security posture, ensuring the safety of your data, assets and reputation.

This guide takes you through each of these step, explaining why it's important, the things you need to consider and the positive results you'll see by implementing them.

SELF ASSESSMENT CHECKLIST

Finally, we have a self assessment checklist on page 10, to help you identify the areas you feel are secure and the areas that are perhaps vulnerable. By the end of it you'll have a clearer view of where your risks lie and the relevant actions you should carry out to reduce these risks.

Let's get started!

STEP 1
ENSURE YOUR DATA IS BACKED UP

Every business should back up their business-critical data to ensure it can operate in the event of physical damage or theft. In the event of a ransomware attack, with adequate backup you can easily retrieve your data and avoid paying the ransom.

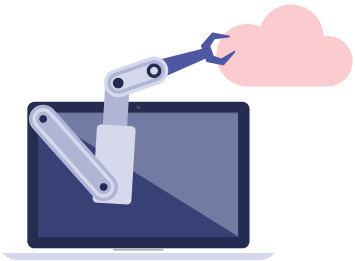
HERE ARE SOME THINGS TO CONSIDER AROUND BACKUP

KEEP BACKUP OFFSITE, CONSIDER THE CLOUD

Backups should be stored in a different location (ideally offsite) to protect the information from flood, fire, theft, or cyber-attack. Cloud storage solutions can be a cost-effective way to store your back-ups in a different location to the original copy. This will help you to recover copies more quickly if your data is lost or stolen.

IDENTIFY WHAT DATA YOU NEED TO BACKUP

This would be the information you could not function without e.g., company documents, contracts, customer information, emails and financial information.



AUTOMATED BACKUP

If you are currently relying on manual methods of backup i.e., relying on an employee to complete the backup, you really should consider an automated solution as your employee may forget or be absent from work. An automated solution mitigates this risk and ensures you have the most recent files available should a restore be required.

CHECK YOUR CLOUD APPLICATIONS

If you have moved some of your applications to the Cloud it's imperative you check to see if this information is being backed up. If we take Microsoft 365 as an example, many people think Microsoft are responsible for backing up all their information stored in Teams, SharePoint, OneDrive etc. However, they only retain your files for a short period of time and recommend you use a third-party solution for backup.

POSITIVE OUTCOMES FOR YOU

- You can retrieve your data and continue to run your business no matter what happens
- If you do experience a cyber-attack you don't need to pay the ransom, which can be extremely costly
- Peace of mind that your Cloud applications are backed up as this is often overlooked
- In line with NCSC guidance
- Be Cyber insurance ready

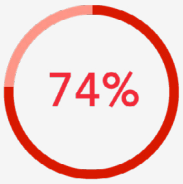
STEP 2
PROTECT AGAINST MALICIOUS EMAILS

Email is a vital part of business life, allowing companies to communicate quickly, both internally and externally.

Secure email for small business is no less important than email security for the enterprise. Many cyber criminals see email as a way into your business - a means of getting access to your network and information and smaller companies fall prey to phishing more often than the rest.

Phishing emails were the number one way in for cyber criminals with almost two-thirds (65%) of ransomware victims mentioning this method of entry (Hiscox).

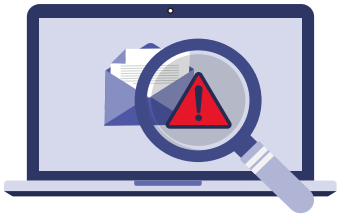
Some 74% of firms with fewer than ten employees targeted with ransomware mentioned this point of entry.



Many cyber criminals are using techniques designed specifically to bypass traditional security measures, which results in malicious emails getting through to your users and the damage can be significant.

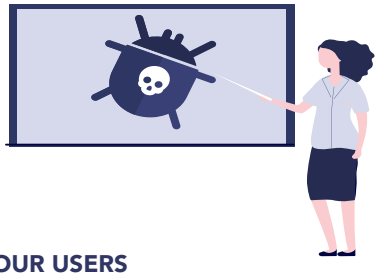
Most organisations don't have adequate protection in place to protect against these sophisticated attacks.

HERE ARE SOME THINGS TO CONSIDER AROUND EMAIL SECURITY



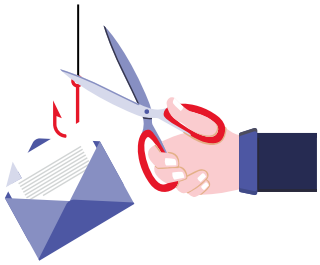
CONSIDER AN EMAIL SECURITY AUDIT

This will help you identify how secure your email actually is. Most email security solution providers will provide this service for free.



TRAIN YOUR USERS

Turn employees into an extra line of defence against phishing attacks with regular testing, education and a way to report a phishing attack.



DEPLOY AN EMAIL PROTECTION PRODUCT

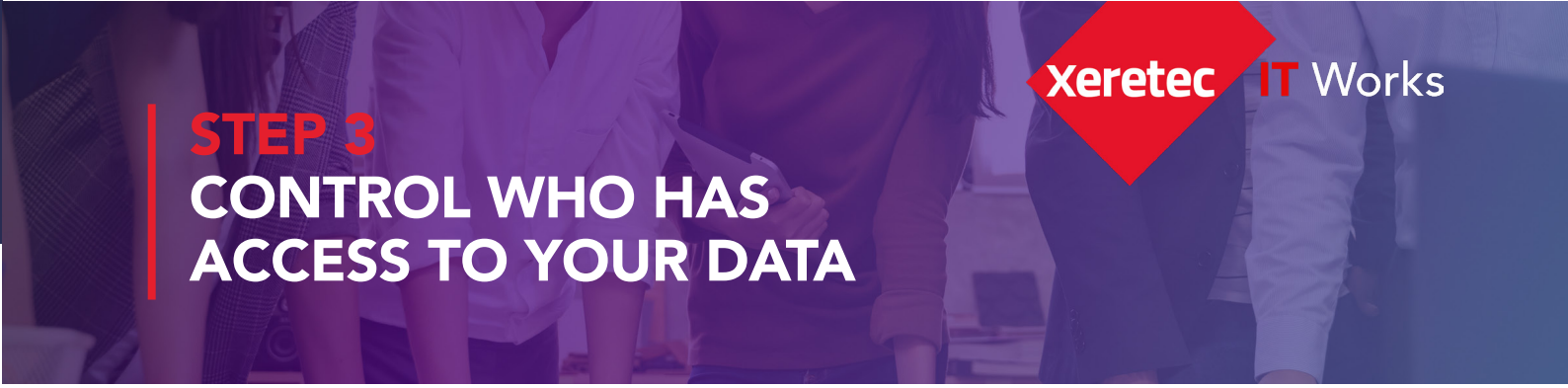
Stops advanced threats like phishing and spear-phishing by blocking malicious links and attachments in email and spotting the signs of fraud.

FREE EMAIL SECURITY AUDIT

To find out more and to arrange a free email security audit, please contact us at marketing@xeretec.co.uk

POSITIVE OUTCOMES FOR YOU

- 100% anti-virus protection and 99% anti-spam protection
- Block malicious links and attachments in email
- Large File Send provides a secure channel for emailing large files (up to 2 GB) to prevent employees from circumventing size limits on attachments by using third-party file sharing services.
- If malicious emails do get through to your users, you can be confident they are well trained and will spot and report suspicious emails In line with NSCS guidelines



Xeretec IT Works

STEP 3
CONTROL WHO HAS ACCESS TO YOUR DATA

Hackers have become very good at compromising passwords, and they have a lot of tools at their disposal.

If identity and access management procedures and controls are badly designed or implemented, they can give attackers an easy way to gain access to your systems which could appear legitimate.

It's important to create a strong password to make it hard for hackers to guess and add layers of security to make it even harder.

YOU SHOULD CONSIDER THE SECURITY OF ALL THE ASPECTS OF IDENTITY

PERMISSION ACCESS MANAGEMENT

Employees should have just enough access to software, settings, online services, and device connectivity functions for them to perform their role. Extra permissions should only be given to those who need them. By giving staff the lowest level of user rights required to perform their jobs the potential damage should they fall victim to a cyber-attack is reduced.

DEPLOY MULTI-FACTOR AUTHENTICATION (MFA)

MFA is a way of asking users for another bit of evidence in addition to their password i.e. they need to type their password plus one other piece of information to confirm their identity to access your systems. This will help stop an attacker gaining access who had managed to steal a password.

ADMIN ACCOUNTS

Check what privileges your employees have - accounts with administrative privileges should only be granted to those who need to perform administrative tasks.

POSITIVE OUTCOMES FOR YOU

- Protection against credential theft. With MFA implemented, a hacker can't access an employee's account even if they manage to crack the password.
- Layers of privileged protection in place means the risk of hackers being able to gain acess to your most valuable data is greatly reduced.
- In line with NCSC guidance.
- Be Cyber insurance ready.

STEP 4
SECURE YOUR DEVICES

Every device that is used by your employees and connected to your network, is a potential point of entry for cyber criminals. Malicious software - known as malware - is code that can harm your computers and laptops, and the data on them.

Your devices can become infected by inadvertently downloading malware that's in an attachment linked to a dubious email, or hidden on a USB drive, or even by simply visiting an unknown website.

Once it is on your computer or laptop, malware can steal your data, encrypt it so you can't access it, or even erase it completely. For this reason, it's important that you always use antivirus software, and keep it up to date to protect your data and devices. All IT equipment's software and firmware must be kept up to date.

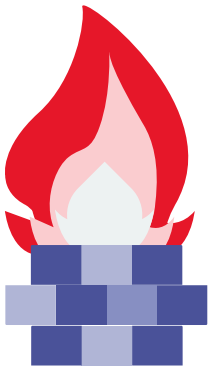
#4

"Unpatched servers were the 4th most common method of entry for cyber criminals, ending in a ransomware attack" - Hiscox

THINGS TO CONSIDER WHEN PROTECTING YOUR DEVICES

DEPLOY AN END POINT SECURITY PRODUCT

This is essential to detect, quarantine and/or delete malicious code, preventing malware from causing damage to your device. Modern antivirus products update themselves automatically, to provide protection against the latest viruses and other types of malwares.



PROTECT YOUR NETWORK WITH A FIREWALL

A firewall effectively creates a 'buffer zone' between your IT network and other, external networks. In the simplest case, this means between your computer(s) and 'the internet'. Within this buffer zone, incoming traffic can be analysed to find out whether it should be allowed onto your network or not.

KEEP YOUR DEVICES AND SOFTWARE UP TO DATE

Manufacturers and developers release regular updates which not only add new features, but also fix any security vulnerabilities that have been discovered. Applying these updates (a process known as patching) is one of the most important things you can do to improve security.

CONSIDER SAAS (SOFTWARE AS A SERVICE) APPLICATIONS

This passes responsibility for patch updates to the SaaS provider and eliminates the need for expensive manage service provider costs updating your on-premise services. This also eliminates the worry and costs associated to replacing the hardware & software that is no longer being supported by the manufacturer.

POSITIVE OUTCOMES FOR YOU

- Endpoint encryption ensuring all data transmitted from a device via the web is encoded
- This prevents users allowing access or installation of malware onto their device.
- Be Cyber Essentials and Cyber Insurance ready.
- In line with NCSC guidance.

Xeretec IT Works

STEP 5
MONITOR YOUR SYSTEMS

As cyber threats are becoming more sophisticated, real-time monitoring and security analysis is needed for fast detection and remediation.

However, the ability to monitor all vulnerabilities, identifying and responding to threats and meeting compliance requirements across the business has become increasingly difficult with remote working, limited budgets, no in-house cyber security specialist or monitoring tools.

CONSIDER AN OUT-SOURCED CYBER SECURITY TEAM

An out-sourced virtual cyber security team can offer the following services:

- A Cyber Audit to understand your current cyber security posture
- 24/7 monitoring and alerting of your organisations infrastructure, detecting threats, intrusion attempts, system anomalies, poorly configured applications, and unauthorised user actions
- Monthly vulnerability reporting to identify any potential configuration issues
- Tailored security awareness programmes and phishing simulations to test employees
- Dark Web Monitoring to keep track of personal information found on this section of the internet

POSITIVE OUTCOMES FOR YOU

A cyber audit allows you to understand where your risks are and the out-sourced team can put a tailored package together to reduce these risks.

A cost effective way of ensuring that your systems are being monitored without having to invest in monitoring tools or in-house security specialists.

SELF ASSESSMENT CHECKLIST

	YES	NO	UNSURE	ACTIONS
Have you recently reviewed what data you need to back up?				Conduct a review to identify the information your business could not function without.
Are your backup's stored off site?				Consider a Cloud storage solution.
Do you use manual backup methods e.g. relying on an employee?				Consider an automated backup solution.
Have you moved some of your applications to the Cloud e.g. M365 or Google G Suite? Do you have additional backup for these?				Implement a Cloud-to-Cloud Back-up Solution.
Have you reviewed your email security?				Conduct an email security audit, most companies will offer this for free.
Do you regularly train your users to help them spot and report suspicious emails?				Look for a product which offers email security training.
Have you implemented any additional email security protection to protect against advanced threats?				Deploy an email protection product to provide extra layers of defence.
Do you limit access to certain area's of the business depending on employee role?				Review all staff roles and limit their access, only allowing them permission to the area's they need to complete their job.
Do you ask staff to provide a password and extra information when logging into the system to confirm they are who they say they are?				Deploy Multi-factor Authentication so that staff identify themselves in 2 or more ways.
Do you currently have anything in place to detect, quarantine and delete malicious code?				Deploy an endpoint security product.
? Not sure what to say here				Protect your Internet with a Firewall.
Do you regularly apply updates to devices and software (Patching)?				Ensure all devices have the latest software installed.
Are some of your applications hosted on-premise?				Consider moving to Cloud based applications (SaaS) as all responsibility for Patching then lies with them.
Do you carry out Cyber Security Vulnerability testing?				Consider a out-sourced cyber security audit to help you understand your vulnerabilities.

SUMMARY

Hopefully this guide has provided you with some practical advice to how to improve your cyber security. It is impossible to guarantee total security but by implementing the right measures to protect against these ever-evolving threats you will certainly reduce the risk of falling victim to a cyber-attack.

We understand that small companies do not have the luxury of large budgets for a dedicated in-house cyber security expert and this is where we can help.

Our team of local experts can help you identify where your vulnerabilities are and recommend simple, affordable solutions to boost your security. We work with a range of market leading security vendors and can recommend the right solution for your business.

Should you have any questions or need advice, please get in touch.

WANT TO LEARN MORE?
GET IN TOUCH

Tel: 0800 074 8136
Email: info@xeretec.co.uk

SOURCES

1. Ponemon Institute
2. https://www.thexyz.com/blog/microsoft-office-365-usage-statistics/
1 Federation of Small Businesses National Chair Mike Cherry
2 NCSC
3. Hiscox Cyber Readiness Report 2021 1.