BUSINESS
IT SUPPORT
& SERVICES

# How to Improve your Cyber Security: A Practical Guide for Small Businesses

# Introduction

**As a small business, it's important to take the necessary precautions to protect your data and deter cyber criminals. In this guide, we offer some practical, affordable tips for keeping your business safe from online threats.**

When it comes to cyberattacks, it's not a matter of if, but when.

| | | | |
|---|---|---|---|
| **19 seconds**<br>One small business in the UK is hacked every 19 seconds<br>*Source: Hiscox* | **39%**<br>of UK small businesses identified a cyber-attack in the past year<br>*Source: Gov.uk* | **£ 25,700**<br>Average basic cost of an incident, not including reputational damage and lost customers<br>*Source: Hiscox* | **60%**<br>of small businesses close within 6 months of a major cyber attack<br>*Source: National Cybersecurity Alliance* |

Smaller companies are up to three times more likely to suffer cyber attacks than larger companies. They often lack the time, resources and specialist knowledge to manage cyber threats, and that makes them an easy target for attackers who seek to exploit their vulnerabilities.

Although you can never be 100% safe from cyber criminals, there's a huge difference between being a target and a victim. For the most part, it comes down to being prepared. That's why we've put together this guide: to help you prioritise the high-impact cyber security actions to keep your business safe.

## In this guide:

**Part 1 - Backing up your data**
4 fail-safe tips for backing up your data

**Part 2 - Protecting your business from malware**
4 simple tactics to protect your business from malware attacks

**Part 3 - Keeping your mobile devices safe**
4 proactive steps to keep mobile devices safe from hackers and intruders

**Part 4 - Using passwords to protect sensitive data**
Keep your passwords strong and secure with these four best-practice tips

**Part 5 - Preventing phishing attacks**
4 tips to avoid costly phishing scams

**Your cybersecurity action plan**
A checklist of actions to protect your business.

# Know what you're up against

Cyberattacks occur in many different ways and they are multiplying daily. Here are the five biggest threats that you need to be aware of.

**Phishing:** An online scam where cyber criminals impersonate a trusted entity, like a vendor or manager, to trick you into sharing personal information or financial data. Phishing accounts for half of cyberattacks in the UK.

**Malware:** A type of software that is designed to damage, disable or steal data from your computer systems. It includes a variety of cyber threats such as viruses, worms and Trojans.

**Ransomware:** A type of malware that encrypts your files so you cannot access them until you pay a ransom. Seven out of 10 ransomware attacks target small businesses. These companies are more likely to pay a ransom as their data is often not backed up.

**Denial of service attack:** An attempt to make a machine or network unavailable to its intended users. This is usually accomplished by flooding the system with requests until it crashes.

**Password hacking:** An attempt to crack passwords in order to gain access to sensitive information. Fraudsters typically use guesswork or brute force, a cryptographic attack that tries every possible sequence to hack passwords.

## 1. Backing up your data

**4 fail-safe tips for backing up your data**

Backups are used to restore lost, damaged or compromised data after accidental deletion, system errors or a cyber attack. The more up-to-date your backups, the more quickly you can bounce back.

All businesses need a backup plan. This section outlines 4 fail-safe tips for backing up your data.

**#1: Identify which data you need to back up**
You should back up all the information that your business cannot live without, including:

- Website files
- Customer database
- Contacts
- Financial records
- Emails

If you're not sure what constitutes business-critical data, err on the side of caution and back up everything. You can always delete unnecessary files later.

**#2: Decide how you will back up your data**
There are two main types of backups: local backups and cloud-based backups. Local backups are stored on an external hard drive, USB stick or server, while cloud-based storage solutions are stored off-site. Either way, it's important that your backups are:

- Not accessible by staff, and
- Not connected to the network holding your original data. Attackers will target connected backup devices to make recovery more difficult.

When choosing a solution, you'll need to consider how much data you wish to back up and how quickly you need to be able to restore the data following any incident. A premium service that offers near real-time retrieval times may be worth the investment if your business is heavily reliant on its data.

Tip: For optimum security, follow the 3-2-1 rule:

- Keep at least 3 copies
- Keep 2 copies on different media
- Keep 1 copy offsite and offline

**#3: Use cloud backup**
Cloud storage is typically more resilient for small businesses since:

- Your data is protected in the event of fire, flood or another catastrophic event at your business premises
- Malware can often move laterally across networks and infect all devices connected to it. If your backups are stored off-site, they are less likely to be infected.

There are lots of cloud storage services to choose from, including pocket-friendly options for smaller businesses with lower storage needs. For example, Microsoft's OneDrive product offers cloud storage solutions with basic plans that are free to use, and cloud storage is the default for most mobile devices.

The main disadvantage of free resources is they purge your files forever after a certain period, such as 30 or 60 days. Remember, too, that you are entrusting your data to another business outside of your control. Assess your risks as part of your overall cyber security strategy.

**#4: Automate your backups**
Automating your backups means you can schedule your operating system to backup everything at intervals, and forget about it until you need to restore your data. You'll also have peace of mind that a recent copy of your data is available that you can fall back on if needed.

Most off-the-shelf network and cloud-based backup services will offer some form of automation, and they're easy to set up. This is a good option if you don't want to have to remember to run your backups manually.

Tip: Aim to automate backups of valuable files and folders daily. This is considered a good benchmark for your most critical data.

**Summary**
Backing up your data is one of the most important things you can do to protect your business from cyberattacks. There are many different types of backups, but cloud-based backups are usually a cost-effective option for small businesses. You can usually automate the backup process, but make sure you test your backups regularly to ensure they're working as they should.

# 2. Protecting your business against malware

**4 simple tactics to protect your business from malware attacks**

For small businesses, malware is an unwelcome predator. The software itself comes in many shapes and sizes, but its end goal is always the same: to compromise your networks, servers and devices, and gain access to your business-critical data.

Here are four simple tactics you can use to protect your systems from malware.

**#1: Install antivirus software**
Antivirus software works by scanning your system for malware and quarantining or deleting any infected files. It's your first line of defence in preventing a malware infection.

If you're using a popular operating system like Microsoft, then antivirus software is included for free. Remember to enable it across all your computers, laptops and office equipment. There are also many good quality commercial antivirus products available, such as Norton and McAfee. These can be particularly useful for businesses with more complex IT systems.

Smartphones and tablets might require a separate configuration. The National Cyber Security website has straightforward guides for configuring the platforms that are commonly used in the UK today.

Antivirus software is only effective if it's up-to-date, so once you've installed a program, make sure you keep it updated. Good antivirus software should update automatically, though you may need to manually trigger an update from time to time.

**#2: Train your staff to avoid malware**
Malware can only get onto your system if someone downloads it, clicks on a malicious link or opens an infected email attachment. That's why it's important to educate your employees about the appropriate way to click and download.

Ensure you have a policy in place to help staff manage the threat. For example, you might establish the following rules:

- Don't download files or open email attachments from unknown or untrustworthy sources.
- Be careful when clicking on links, even if they're from a trusted source. Make sure the URL is correct before clicking.
- Only download apps from approved stores.
- Only use approved external storage devices, such as USB drives and cards, from within the organisation.
- Forward any suspicious emails to IT or your outsourced security team.

Training programs are available from many sources, including the National Cyber Security website. You can also find helpful staff training guides online.

**#3: Patch your applications**
If you do one thing to reduce your cyber security risk, it's the patching (or updating) of your software, applications and operating systems so they're running on the latest versions from software developers. Programmes that haven't been updated are the number one route cybercriminals use to hack businesses.

Ideally, you'll use automated updates to top up your security every day. Some companies have a manual "patch Tuesday" policy, where they manually check and install all the latest security patches on the second Tuesday of every month.

Tip: At some point, your product will reach the end of its supported life and the developer will no longer release patches for that product. When this happens, you'll need to replace it with a newer, supported version.

**#4: Switch on your firewall**
A firewall is a barrier between your network and external networks like the internet. Its role is to block incoming traffic from malicious sources, while still allowing legitimate traffic through. It can also block outgoing traffic to prevent sensitive data from leaving your network.

Most operating systems now include a basic firewall, so it's just a case of turning it on. However, firewalls are not a one-size-fits-all solution. You may need additional firewall protection if you have a lot of users, you manage a lot of sensitive data, or you have a lot of remote and mobile employees.

External IT services like Point of Sale systems are a bit like opening a backdoor malware. Make sure your POS system is behind a firewall with separate credentials and password to keep it safe from attack.

**Summary**
Antivirus software is your first line of defence against malware. Install it on all of your systems and keep it up to date. Humans are the weak link in your security, so educate your employees about security threats and have a policy in place to help them avoid malware. Patch your systems regularly and switch on your firewall for additional protection.

# 3. Keeping your mobile devices safe

**4 proactive steps to keep mobile devices safe from hackers and intruders**

Most businesses use a mix of laptops, smartphones and tablets. These devices may be issued by the company or owned personally by employees but, either way, are likely to contain a lot of sensitive data. Keeping all your mobile devices secure is critical to protecting your information and minimising the risk of losing money.

Since they travel with staff, mobile devices need as much or greater protection than your desktop computers. The following four tips can help keep your mobile devices safe from cyber attack.

**#1: Use password protection**
The simplest and most effective way to protect your mobile devices is to use password protection. All mobile devices should have a complex password that's difficult to guess. Ideally, passwords should be 12 characters long and include a mix of upper- and lower-case letters, numbers and symbols.

Staff should have different passwords for each of your devices and accounts. That way, if one of their passwords is compromised, the others will still be safe.

**#2: Use mobile device management software**
Today's smart devices come with a suite of tools to help protect your data if the device is lost or stolen, including tools that:

- Automatically lock devices after periods of inactivity
- Track the location of a device
- Remotely lock the device to prevent anyone else using it
- Remotely wipe the data stored on the device
- Remotely retrieve a backup of data stored on the device

Setting up these features is usually quick and easy, so there's no excuse not to use them. Mobile device management (MDM) software makes it even easier by enabling you to configure and patch the security settings on all the devices in your fleet simultaneously from a central application.

Some MDM solutions also help you track data usage, so you can manage costs while keeping an eye out for unusual activity.

**#3: Keep your devices and apps up to date**
When it comes to security updates, mobile devices should be treated the same way as desktop computers. Make sure that staff know how to install security updates and the automatic feature is turned on for all devices.

**#4: Protect your data when using public wi-fi**
Using public wi-fi is convenient, but it's also one of the easiest ways for hackers to get access to your devices and data. Educate staff to be especially cautious when connecting to wi-fi in places like airports and coffee shops and avoid logging into any sensitive accounts or websites while they're connected.

The best way to protect your business is to not connect to unknown public wi-fi hotspots at all. Instead, have your staff use a 4G or 5G connection with in-built security. You can also use tethering (which turns your mobile device into a personal hotspot) to create a secure connection for other devices and wireless dongles (which connect devices to the internet via a USB port).

Avoid using any file-sharing services, as these can be exploited by hackers.

**Summary**
Mobile devices are an essential part of business but they also come with unique security risks. Make sure the security features of your devices are up to date and staff are using strong and effective passwords. Mobile device management software can make it easier to manage the security of your fleet of devices at the same time. Instead of using public wi-fi, choose alternative methods to connect to the internet. With these steps, you can help keep your mobile data safe from cybercrime.

# 4. Using passwords to protect sensitive data

**Keep your passwords strong and secure with these four best-practice tips**

Passwords, when used correctly, are an extremely effective way to protect data and IT systems from unauthorised access. We've compiled 4 best practices to help you protect your passwords, information and identity online.

**#1: Choose non-predictable passwords**
Hackers have access to programs that guess trillions of different password combinations, so the more complex your password, the better. Strong passwords:

- Are long (at least 12 characters)
- Contain a mix of uppercase and lowercase letters, numbers and symbols
- Are not based on easy-to-guess information such as the names of children or pets that can be easily guessed by someone looking at your social media profiles
- Stay clear of dictionary words; even random words such as "superman" or "sunshine" are easily cracked
- Make sure your staff are following best practices when setting screen lock and access passwords.

You might be surprised to learn that many devices come with pre-set, default passwords. These are usually easy to guess (like "admin" or "password"), which makes them a security risk. If you're using any devices with default passwords, you should change them to something more secure as soon as possible.

You should also regularly check devices to detect unchanged default passwords.

81% of data breaches are due to weak passwords – Verizon's 2021 Data Breach Investigations Report

**#2: Use password alternatives**
PINs and other authentication methods such as fingerprint or face unlock are tied to a device and are thus considered safer than passwords. PIN protection, for example, typically allows a maximum number of login attempts before shutting down. And it's impossible to brute-force a fingerprint.

Password alternatives can facilitate a quicker, more usable experience. However, they're only as good as the people using them. Don't use National Insurance numbers, phone numbers, addresses, or other personally identifiable information as PIN codes. If someone gains access to this information, it will be among the first things they use to try to get into your account.

**#3: Use two-step verification for sensitive accounts**
Having one strong password is great; having two is better. Two-Factor Authentication (2FA), also known as two-step verification (2SV) requires you to prove your identity in two ways before you access a service, generally with a password plus a code that is sent to your phone. This makes it much harder for hackers to gain access to your account, as they would need both your password and your phone.

Many online services, including Microsoft Office, offer 2FA as an option. You should enable it for all accounts that support it.

**#4: Use password managers to reduce password fatigue**
A password manager or password 'vault' is a software program that helps you store passwords securely for all your online accounts. It can also auto-generate highly secure passwords. Password managers work by encrypting your passwords and locking them behind a master password. This means you only have to remember one master password to unlock the entire password vault.

Many password managers offer additional features, like two-factor authentication, time-saving password autofill and the secure synchronisation of passwords across multiple operating systems. So if your employees are using Windows at work and Mac at home, they will be able to quickly access their passwords regardless of which platform they're on.

There are many free options available. Opt for a cloud-based system and you can access your password manager anywhere, from any device.

**Summary**
Passwords and PINS are an effective way to control access to your data, the devices you store it on, and the online services you use. Create strong passwords in line with best practices, reset them regularly, and use 2FA on your important accounts. You can also use a standalone password manager to help you create and store strong passwords in a secure vault.

# 5. Preventing phishing attacks

**4 tips to avoid costly phishing scams**

Phishing is a scam that involves hackers sending fake emails or texts in an attempt to trick you into doing the wrong thing, like sharing your login credentials or bank details. Hackers can also create fake websites that look identical to the real thing. When you enter your details on these fake sites, hackers can use them to gain access to your accounts.

While that sounds straightforward, for your staff, phishing scams can be difficult to spot. This section contains some tips to help you recognise and avoid phishing attacks.

**#1: Train staff on the obvious signs of phishing**
The best defence against phishing is a good cyber security policy and training for your employees to help them recognise a genuine email from a fake one. Things to look for include:

- Slight misspellings in the domain name (for example, “amaz0n” instead of “amazon”)
- Misspelt words in the email (this is done to bypass your spam filter)
- Receiving an invoice for a service that you haven’t used, which instals malware when the attachment is opened
- Emails with unusual phrasing
- Requests for information that purport to come from a trusted source like a customer or manager
- Great offers or rewards

Train staff to spot the red flags and have the confidence to ask, “is this genuine?” The earlier they learn about the latest attack methods through regular security awareness training, the more likely you are to avoid a potential attack.

**#2: Implement a ‘need to know’ policy**
The less access users have, the safer your data will be from compromise. As such, accounts should be configured according to the ‘principle of least privilege,’ so that employees have the access they need to do their job, and no more. For example, if an employee doesn’t need access to financial or HR information, they shouldn’t have it. This reduces the chances of a hacker being able to do serious damage if they gain access to an employee’s account.

To further reduce the damage, make sure that your employees don’t browse the web or check emails from an account with Administrator privileges. Administrators can make changes to system settings, install programs and access all files on the computer. If a hacker gains access to an Administrator account, they can cause serious damage.

Tip: Use classifications like public, restricted and confidential and limit access depending on the level.

**#3: Proactively manage your publicly available information**
Every business and all its employees have a digital footprint of information that’s publicly available on the web. Hackers use this information to make their phishing messages more convincing. For example, a hacker could email pretending to be from a trusted source, like your ISP or web hosting company, and try to trick you into sharing sensitive information.

While it’s not realistic to remove all traces of yourself from the internet, you must help staff be proactive and shape their digital footprint into something that you and your organisation are happy with. Are you:

- Reviewing what personal and work-related data is available online and deleting parts that say too much?
- Asking staff to review their passwords and change default privacy settings on devices, apps and social media sites?
- Thinking carefully about what you share and how it will be protected?

**#4: Report all phishing attacks**
If you receive a phishing email or text, do not respond to it. Delete the message immediately. If an employee accidentally clicked on a link in the message, run a full virus scan and change passwords on all your accounts as soon as you can.

Remember to be kind to your employees – phishing scams get more sophisticated every day and everyone makes mistakes. The important thing is that you encourage staff to report suspicious activity and have a system in place for spotting issues and improving your defences.

If you believe your business has been the victim of a phishing scam or fraud, report it to Action Fraud, the UK's national fraud and cybercrime reporting centre. Action Fraud has the power to investigate phishing attacks and they can also provide you with advice on how to protect yourself in the future.

**Summary**
Phishing emails try to convince users to click on fake or infected links and websites, or to give away sensitive information such as bank details. Offence is the best form of defence against phishing, so train staff to spot the signs and make yourself a harder target by limiting the information that appears online. If someone clicks a suspicious link, don't panic. Respond immediately with a full virus scan and password-change protocol to limit the damage.

# Stay alert to cyber threats

**When your business is at stake, you need to be vigilant to the risk of cyber attacks. Implementing the actions outlined in this guide will significantly reduce the chance of you becoming a victim of cybercrime.**

For round-the-clock monitoring and support, consider working with a Managed Service Provider.
MSPs are IT experts who will:

- Identify your weak spots
- Proactively manage your systems
- Encrypt and backup sensitive data
- Block the threats
- Update your security in real time and
- Provide you with the latest cyber security intelligence so your small business can be just as robustly protected as your larger counterparts.

CNS IT goes beyond basic support to provide your business with stability, security, and resilience against cyber threats. Visit cns-it.co.uk to discover more and book a free audit.

# Your Cybersecurity Action Plan

**The following actions can help small businesses reduce the risk of becoming a victim of cybercrime.**
**To find out how we can help visit www.cns-it.co.uk**

**PROTECT**
Offence is the best defence

- Identify business-critical data for backups
- Create automated backups and store them in secure, preferably offsite, locations
- Store sensitive data in encrypted format
- Install firewalls to protect against attacks
- Update antivirus software and scan systems for malware
- Restrict access to sensitive data to authorised users only
- Enable two-factor authentication whenever possible
- Use secure communications protocols
- Use a Virtual Private Network (VPN)
- Use a token or password manager to manage your passwords
- Install a tracking device on all mobile devices
- Restrict employee access to certain websites/apps
- Establish access controls so employees can access only the information and systems required for their job role

**TRAIN**
Human error accounts for 90% of cyber incidents

- Train staff on cybersecurity risks
- Create a policy on strong passwords
- Have a clear reporting process if staff suspect phishing
- Train staff on wi-fi hotspot vulnerabilities and using alternative options (e.g VPN/mobile network)
- Test your policies with simulated exercises

**DETECT**
Threats are constantly changing, so review the landscape frequently.

- Regularly scan your network for vulnerabilities
- Patch applications as soon as updates are released
- Keep a register of incidents to help you track and fix problems
- Allocate a responsible owner
- Contact CNS-IT to stay on top of the latest cyber threats

**CNS IT provide managed IT solutions and support to small and medium sized organisations across North Wales, Cheshire and Wirral.**

CNS IT Ltd is a limited company registered in England

BUSINESS IT SUPPORT & SERVICES

**IT Managed Services. Managed Better**


**Get in touch**

E: hello@cns-it.co.uk

W: www.cns-it.co.uk

**OFFICE**

10 Telford Court
Chester Gates, Dunkirk,
Chester, CH1 6LT
T: 01244 851 866