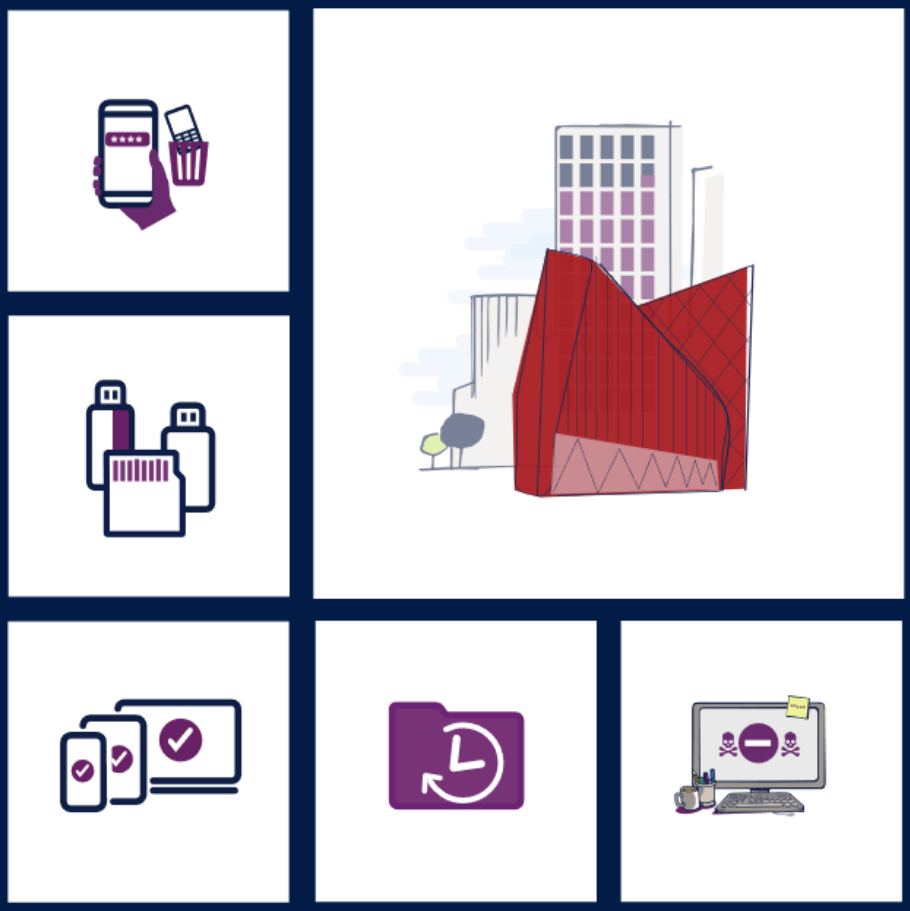
National Cyber Security Centre
a part of GCHQ

Cyber Security:
Small Business Guide



How to improve cyber security within your organisation - quickly, easily and at low cost.

Contents

Foreword

This guide has been produced to help small businesses protect themselves from the most common cyber attacks.

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. For micro / small businesses, that could result in costs of around £1,400.

Following the advice in this guide will significantly increase your protection from the most common types of cyber crime. The 5 topics covered are easy to understand and cost little to implement. This guide can't guarantee protection from all types of cyber attack, but it does show how easy it can be to protect your organisation's data, assets, and reputation.

You can find more help in the 'find out more' section at the bottom of each topic. If you need to improve your cyber security further, then you can also seek certification under the Cyber Essentials[1] scheme, which has the benefit of demonstrating to your clients (or prospective clients) that you take the protection of their data seriously. And if you're a larger business, or face a greater risk from cyber crime, then the 10 Steps to Cyber Security[2] can further help your approach to cyber security.

As we announced when the National Cyber Security Centre (NCSC) was launched[3], we want to make it easy for people to understand how to protect their information and IT against cyber attack, in the same way that everyone understands how to protect their property from other types of crime.

The NCSC is not just here to look after the IT systems of government and the UK's critical national infrastructure. Whether you run a small business, a charity, oversee the IT systems in a school, or simply want to make sure your devices at home are more secure, our mission is to make the UK the safest place for everyone to live and do business online.

Ciaran Martin
Chief Executive Officer, NCSC

[1] https://www.cyberaware.gov.uk/cyberessentials/get.html
[2] https://www.ncsc.gov.uk/guidance/10-steps-cyber-security
[3] https://www.ncsc.gov.uk/blog-post/what-can-ncsc-do-you

Backing up your data

Think about how much you rely on your business-critical data. Customer details, quotes, orders, and payment details. Now imagine how long you would be able to operate without them.

All businesses, regardless of size, should take regular backups of their important data, and make sure that these backups are recent and can be restored. By doing this, you're ensuring your business can still function following the impact of flood, fire, physical damage or theft. Furthermore, if you have backups of your data that you can quickly recover, you can't be blackmailed by ransomware attacks[4].

This section outlines 5 things to consider when backing up your data.

Tip 1: Identify what data you need to back up

Your first step is to identify your essential data. That is, the information that your business couldn't function without. Normally this will comprise documents, photos, emails, contacts, and calendars, most of which are kept in just a few common folders on your computer, phone or tablet or network.

Tip 2: Keep your backup separate from your computer

Whether it's on a USB stick, on a separate drive or a separate computer, access to data backups should be restricted so that they:

- are not accessible by staff
- are not permanently connected (either physically or over a local network) to the device holding the original copy

Ransomware (and other malware) can often move to attached storage automatically, which means any such backup could also be infected, leaving you with no backup to recover from. For more resilience, you should consider storing your backups in a different location, so fire or theft won't result in you losing both copies. Cloud storage solutions (see below) are a cost-effective and efficient way of achieving this.

Tip 3: Consider the cloud

You've probably already used cloud storage during your everyday work and personal life without even knowing - unless you're running your own email server, your emails are already stored 'in the cloud'.

Using cloud storage (where a service provider stores your data on their infrastructure) means your data is physically separate from your location. You'll also benefit from a high level of availability. Service providers can supply your organisation with data storage and web services without you needing to invest in expensive hardware up front. Most providers offer a limited amount of storage space for free, and larger storage capacity for minimal costs to small businesses.

[4] https://www.ncsc.gov.uk/WannaCry-guidance-for-home-users-and-small-businesses

Tip 4: Read our cloud security guidance

Not all service providers are the same, but the market is reasonably mature and most providers have good security practices built-in. By handing over significant parts of your IT services to a service provider, you'll benefit from specialist expertise that smaller organisations would perhaps struggle to justify in terms of cost. However, before contacting service providers, we encourage you to read the NCSC's Cloud Security Guidance[5]. This guidance will help you decide what to look for when evaluating their services, and what they can offer.

Tip 5: Make backing up part of your everyday business

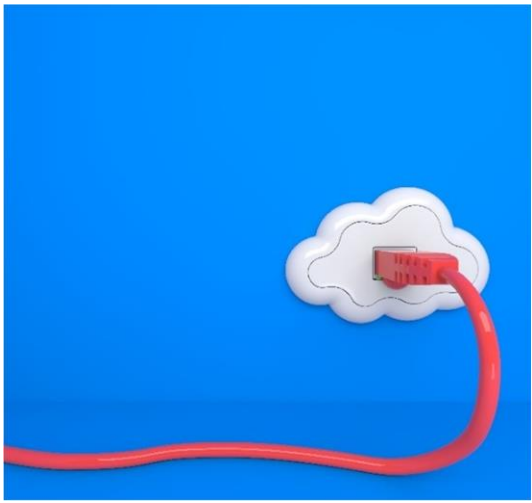
We know that backing up is not a very interesting thing to do (and there will always be more important tasks that you feel should take priority), but the majority of network or cloud storage solutions now allow you to make backups automatically. For instance, when new files of a certain type are saved to specified folders. Using automated backups not only saves time, but also ensures that you have the latest version of your files should you need them.

Many off-the-shelf backup solutions are easy to set up, and are affordable considering the business-critical protection they offer. When choosing a solution, you'll also have to consider how much data you need to back up, and how quickly you need to be able to access the data following any incident.

Find out more

For further guidance on backups, please see our Securing Bulk Data guidance[6], which discusses the importance of knowing what data is most important to you, and how to back it up reliably.

The Information Commissioner's Office website also has a useful introduction to cloud computing[7].



[5] https://www.ncsc.gov.uk/guidance/cloud-security-collection
[6] https://www.ncsc.gov.uk/guidance/protecting-bulk-personal-data-main
[7] https://ico.org.uk/for-the-public/online/cloud-computing/

Protecting your organisation from malware

Malicious software (also known as 'malware') is software or web content that can harm your organisation, such as the recent WannaCry outbreak[8]. The most well-known form of malware is viruses, which are self-copying programs that infect legitimate software.

This section contains 5 free and easy-to-implement tips that can help prevent malware damaging your organisation.

Tip 1: Install (and turn on) antivirus software

Antivirus software - which is often included for free within popular operating systems - should be used on **all** computers and laptops. For your office equipment, you can pretty much click 'enable', and you're instantly safer. Smartphones and tablets might require a different approach and if configured in accordance with the NCSC's EUD guidance[9], separate antivirus software[10] might not be necessary.

Tip 2: Prevent staff from downloading dodgy apps

You should only download apps for mobile phones and tablets from manufacturer-approved stores (like Google Play or Apple App Store). These apps are checked to provide a certain level of protection from malware that might cause harm. You should prevent staff from downloading third party apps from unknown vendors/sources, as these will not have been checked.

Staff accounts should only have enough access required to perform their role, with extra permissions (i.e. for administrators) only given to those who need it. When administrative accounts are created, they should only be used for that specific task, with standard user accounts used for general work.

Tip 3: Keep all your IT equipment up to date (patching)

For all your IT equipment (so tablets, smartphones, laptops and PCs), make sure that the software and firmware is always kept up to date with the latest versions from software developers, hardware suppliers and vendors. Applying these updates (a process known as patching) is one of the most important things you can do to improve security - the IT version of eating your fruit and veg. Operating systems, programmes, phones and apps should all be set to 'automatically update' wherever this is an option.

At some point, these updates will no longer be available (as the product reaches the end of its supported life), at which point you should consider replacing it with a modern alternative. For more information on applying updates, refer to the NCSC's guidance on Vulnerability Management[11].

[8] https://www.ncsc.gov.uk/WannaCry-guidance-for-home-users-and-small-businesses
[9] https://www.ncsc.gov.uk/guidance/end-user-device-security
[10] https://www.ncsc.gov.uk/blog-post/av-or-not-av
[11] https://www.ncsc.gov.uk/guidance/vulnerability-management

Tip 4: Control how USB drives (and memory cards) can be used

We all know how tempting it is to use USB drives or memory cards to transfer files between organisations and people. However, it only takes a single cavalier user to inadvertently plug-in an infected stick (such as a USB drive containing malware) to devastate the whole organisation.

When drives and cards are openly shared, it becomes hard to track what they contain, where they've been, and who has used them. You can reduce the likelihood of infection by:

- blocking access to physical ports for most users
- using antivirus tools
- only allowing approved drives and cards to be used within your organisation - and nowhere else

Make these directives part of your company policy, to prevent your organisation being exposed to unnecessary risks. You can also ask staff to transfer files using alternate means (such as by email or cloud storage), rather than via USB.

Tip 5: Switch on your firewall

Firewalls create a 'buffer zone' between your own network and external networks (such as the Internet). Most popular operating systems now include a firewall, so it may simply be a case of switching this on. For more detailed information on using firewalls, refer to the Network Security section of the NCSC's 10 Steps to Cyber Security[12].

Find out more

More detailed, technical advice on preventing malware is available from the NCSC's 10 Steps to Cyber Security[13].

For detailed information on removable media, refer to the removable media section of the NCSC's 10 Steps to Cyber Security[14].

How to protect your PC from viruses (Microsoft guide)[15].

[12] https://www.ncsc.gov.uk/guidance/10-steps-network-security
[13] https://www.ncsc.gov.uk/guidance/10-steps-malware-prevention
[14] https://www.ncsc.gov.uk/guidance/10-steps-removable-media-controls
[15] https://support.microsoft.com/en-us/help/17228/windows-protect-my-pc-from-viruses

Keeping your smartphones (and tablets) safe

Mobile technology is now an essential part of modern business, with more of our data being stored on tablets and smartphones. What's more, these devices are now as powerful as traditional computers, and because they often leave the safety of the office (and home), they need even more protection than 'desktop' equipment.

With this is mind, here are 5 quick tips that can help keep your mobile devices (and the information stored on them) secure.

Tip 1: Switch on password protection

A suitably complex PIN or password[16] (opposed to a simple one that can be easily guessed or gleaned from your social media profiles) will prevent the average criminal from accessing your phone. Many devices now include fingerprint recognition to lock your device, without the need for a password. However, these features are not always enabled 'out of the box', so you should always check they have been switched on.

Tip 2: Make sure lost or stolen devices can be tracked, locked or wiped

Staff are more likely to have their tablets or phones stolen (or lose them) when they are away from the office or home. Fortunately, the majority of devices include free web-based tools that are invaluable should you lose your device. You can use them to:

- track the location of a device
- remotely lock access to the device (to prevent anyone else using it)
- remotely erase the data stored on the device
- retrieve a backup of data stored on the device

Setting up these tools on all your organisation's devices may seem daunting at first, but by using mobile device management software[17], you can set up your devices to a standard configuration with a single click.

Tip 3: Keep your device up to date

No matter what phones or tablets your organisation is using, it is important that they are kept up to date at all times. All manufactures (for example Windows, Android, iOS) release regular updates that contain critical security updates to keep the device protected. This process is quick, easy, and free; devices should be set to automatically update, where possible. Make sure your staff know how important these updates are, and explain how to do it, if necessary. At some point, these updates will no longer be available (as the device reaches the end of its supported life), at which point you should consider replacing it with a modern alternative.

[16] https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0
[17] https://www.ncsc.gov.uk/blog-post/ncsc-it-mdm-products-which-one-best-1

Tip 4: Keep your apps up to date

Just like the operating systems on your organisation's devices, all the applications that you have installed should also be updated regularly with patches from the software developers. These updates will not only add new features, but they will also patch any security holes that have been discovered. Make sure staff know when updates are ready, how to install them, and that it's important to do so straight away.

Tip 5: Don't connect to unknown Wi-Fi Hotspots

When you use public Wi-Fi hotspots (for example in hotels or coffee shops), there is no way to easily find out who controls the hotspot, or to prove that it belongs to who you think it does. If you connect to these hotspots, somebody else could access:

- what you're working on whilst connected
- your private login details that many apps and web services maintain whilst you're logged on

The simplest precaution is to not connect to the Internet using unknown hotspots, and instead use your mobile 3G or 4G mobile network, which will have built-in security. This means you can also use 'tethering' (where your other devices such as laptops share your 3G/4G connection), or a wireless 'dongle' provided by your mobile network. You can also use Virtual Private Networks (VPNs), a technique that encrypts your data before it is sent across the Internet. If you're using third party VPNs, you'll need the technical ability to configure it yourself, and should only use VPNs provided by reputable service providers.

Find out more

If you're about to invest in a new device, we recommend you read the Buyer's Guide to Choosing and Using Mobile Devices[18] produced by the Home Office.

For more technical information about how to ensure your staff can work safely whilst on the move or at home, please refer to the 10 Steps: Home and Mobile Working guidance[19].

[18] https://tinyurl.com/y9hgclg4
[19] https://www.ncsc.gov.uk/guidance/10-steps-home-and-mobile-working

Using passwords to protect your data

Your laptops, computers, tablets and smartphones will contain a lot of your own business-critical data, the personal information of your customers, and also details of the online accounts that you access. It is essential that this data is available to you, but not available to unauthorised users.

Passwords - when implemented correctly - are a free, easy and effective way to prevent unauthorised users accessing your devices. **This section outlines 5 things to keep in mind when using passwords**.

Tip 1 Make sure you switch on password protection

Set a screenlock password, PIN, or other authentication method (such as fingerprint or face unlock). The NCSC blog[20] has some good advice on passwords. If you're mostly using fingerprint or face unlock, you'll be entering a password less often, so consider setting up a long password that's difficult to guess.

Having said this, password protection is not just for smartphones and tablets. Make sure that your office equipment (so laptops and PCs) all use an encryption product (such as BitLocker for Windows) using a Trusted Platform Module (TPM)[21] with a PIN, or FileVault (on macOS)[22] in order to start up. Most modern devices have encryption built in, but encryption may still need to be turned on and configured, so check you have set it up.

Tip 2: Use two factor authentication for 'important' accounts

If you're given the option to use two-factor authentication (also known as 2FA) for any of your accounts, you should do; it adds a large amount of security for not much extra effort. 2FA requires two different methods to 'prove' your identity before you can use a service, generally a password plus one other method. This could be a code that's sent to your smartphone (or a code that's generated from a bank's card reader) that you must enter in addition to your password.

Tip 3: Avoid using predictable passwords

If you are in charge of IT policies within your organisation, make sure staff are given actionable information[23] on setting passwords that is easy for them to understand.

Passwords should be easy to remember, but hard for somebody else to guess. A good rule is 'make sure that somebody who knows you well, couldn't guess your password in 20 attempts'. Staff should also avoid using the most common passwords[24], which criminals can easily guess. The NCSC have some useful advice on how to choose a non-predictable password[25].

[20] https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0
[21] https://technet.microsoft.com/en-us/library/cc766295(v=ws.10).aspx
[22] https://support.apple.com/en-gb/HT204837
[23] https://www.ncsc.gov.uk/guidance/helping-end-users-manage-their-passwords
[24] https://www.teamsid.com/worst-passwords-2015/
[25] https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0

Remember that your IT systems should **not** require staff to share accounts or passwords to get their job done. Make sure that every user has personal access to the right systems, and that the level of access given is always the lowest needed to do their job whilst minimising unnecessary exposure to systems they don't need access to.

Tip 4: Help your staff cope with 'password overload'

If you're in charge of how passwords are used in your organisation, there's a number of things you can do that will improve security. Most importantly, your staff will have dozens of non-work related passwords to remember as well, so only enforce password access to a service if you really need to. Where you do use passwords to access a service, do not enforce regular password changes. Passwords really only need to be changed when you suspect a compromise of the login credentials.

You should also provide secure storage so staff can write down passwords for important accounts (such as email and banking), and keep them safe (but not with the device itself). Staff will forget passwords, so make sure they can reset their own passwords easily.

Consider using password managers[26], which are tools that can create and store passwords for you that you access via a 'master' password. Since the master password is protecting all of your other passwords, make sure it's a strong one, for example by using three random words.

Tip 5: Change all default passwords

One of the most common mistakes is not changing the manufacturers' default passwords that smartphones, laptops, and other types of equipment are issued with. Change all default passwords before devices are distributed to staff. You should also regularly check devices (and software) specifically to detect unchanged default passwords.

Find out more

If you're in charge of setting up passwords in your organisation, please refer to our password policy guidance[27].

[26] https://www.ncsc.gov.uk/blog-post/what-does-ncsc-think-password-managers
[27] https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach

Avoiding phishing attacks

In a typical phishing attack, scammers send fake emails to thousands of people, asking for sensitive information (such as bank details), or containing links to bad websites. They might try to trick you into sending money, steal your details to sell on, or they may have political or ideological motives[28] for accessing your organisation's information.

Phishing emails are getting harder to spot, and some will still get past even the most observant users. Whatever your business, however big or small it is, you will receive phishing attacks at some point. This section contains some easy steps to help you identify the most common phishing attacks, but be aware that there is a limit to what you can expect your users to do[29].

Tip 1: Configure accounts to reduce the impact of successful attacks

You should configure your staff accounts in advance using the principle of 'least privilege'. This means giving staff the lowest level of user rights required to perform their jobs, so if they are the victim of a phishing attack, the potential damage is reduced.

To further reduce the damage that can be done by malware or loss of login details, ensure that your staff don't browse the web or check emails from an account with **Administrator** privileges. An Administrator account is a user account that allows you to make changes that will affect other users. Administrators can change security settings, install software and hardware, and access all files on the computer. So an attacker having unauthorised access to an Administrator account can be far more damaging than accessing a standard user account.

Use two factor authentication (2FA) on your important accounts such as email. This means that even if an attacker knows your passwords, they still won't be able to access that account.

Tip 2: Think about how you operate

Consider ways that someone might target your organisation, and make sure your staff all understand normal ways of working (especially regarding interaction with other organisations), so that they're better equipped to spot requests that are out of the ordinary. Common tricks include sending an invoice for a service that you haven't used, so when the attachment is opened, malware is automatically installed (without your knowledge) on your computer.

Another is to trick staff into transferring money or information by sending emails that look authentic. Think about your usual practices and how you can help make these tricks less likely to succeed. For example:

- Do staff know what to do with unusual requests, and where to get help?
- Ask yourself whether someone impersonating an important individual (a customer or manager) via email should be challenged (or have their identity verified another way) before action is taken.

[28] http://www.bbc.co.uk/news/uk-38332266

[29] https://www.ncsc.gov.uk/blog-post/im-gonna-stop-you-little-phishie

- Do you understand your regular business relationships? Scammers will often send phishing emails from large organisations (such as banks) in the hope that some of the email recipients will have a connection to that company. If you get an email from an organisation you don't do business with, treat it with suspicion.
- Think about how you can encourage and support your staff to question suspicious or just unusual requests, even if they appear to be from important individuals. Having the confidence to ask 'is this genuine?' can be the difference between staying safe, or a costly mishap.

Tip 3: Check for the obvious signs of phishing

Expecting your staff to identify and delete all phishing emails is an impossible request and would have a massive detrimental effect on business productivity. However, many phishing emails still fit the mould of a traditional attack, so look for the following warning signs:

- Many phishing scams originate overseas and often the spelling, grammar and punctuation are poor. Others will try and create official looking emails by including logos and graphics. Is the design (and quality) what would you'd expect from a large organisation?
- Is it addressed to you by name, or does it refer to 'valued customer', or 'friend', or 'colleague'? This can be a sign that the sender does not actually know you, and that it is part of a phishing scam.
- Does the email contain a veiled threat that asks you to act urgently? Be suspicious of words like 'send these details within 24 hours' or 'you have been a victim of crime, click here immediately'.
- Look out for emails that appear to come from a high-ranking person within your organisation, requesting a payment is made to a particular bank account. Look at the sender's name. Does it sound legitimate, or is it trying to mimic someone you know?
- If it sounds too good to be true, it probably is. It's most unlikely that someone will want to give you money, or give you access to some secret part of the Internet.

Tip 4: Report all attacks

Make sure that your staff are encouraged to ask for help if they think that they might have been a victim of phishing, especially if they've not raised it before. It's important to take steps to scan for malware and change passwords as soon as possible if you suspect a successful attack has occurred.

Do not punish staff if they get caught out. It discourages people from reporting in future, and can make them so fearful that they spend excessive time and energy scrutinising every email they receive. Both these things cause more harm to your business in the long run.

If you believe that your organisation has been the victim of online fraud, scams or extortion, you should report this through the Action Fraud website[30]. Action Fraud is the UK's national fraud and cyber crime reporting centre. If you are in Scotland contact Police Scotland on 101.

[30] http://www.actionfraud.police.uk/report_fraud

Tip 5: Keep up to date with attackers

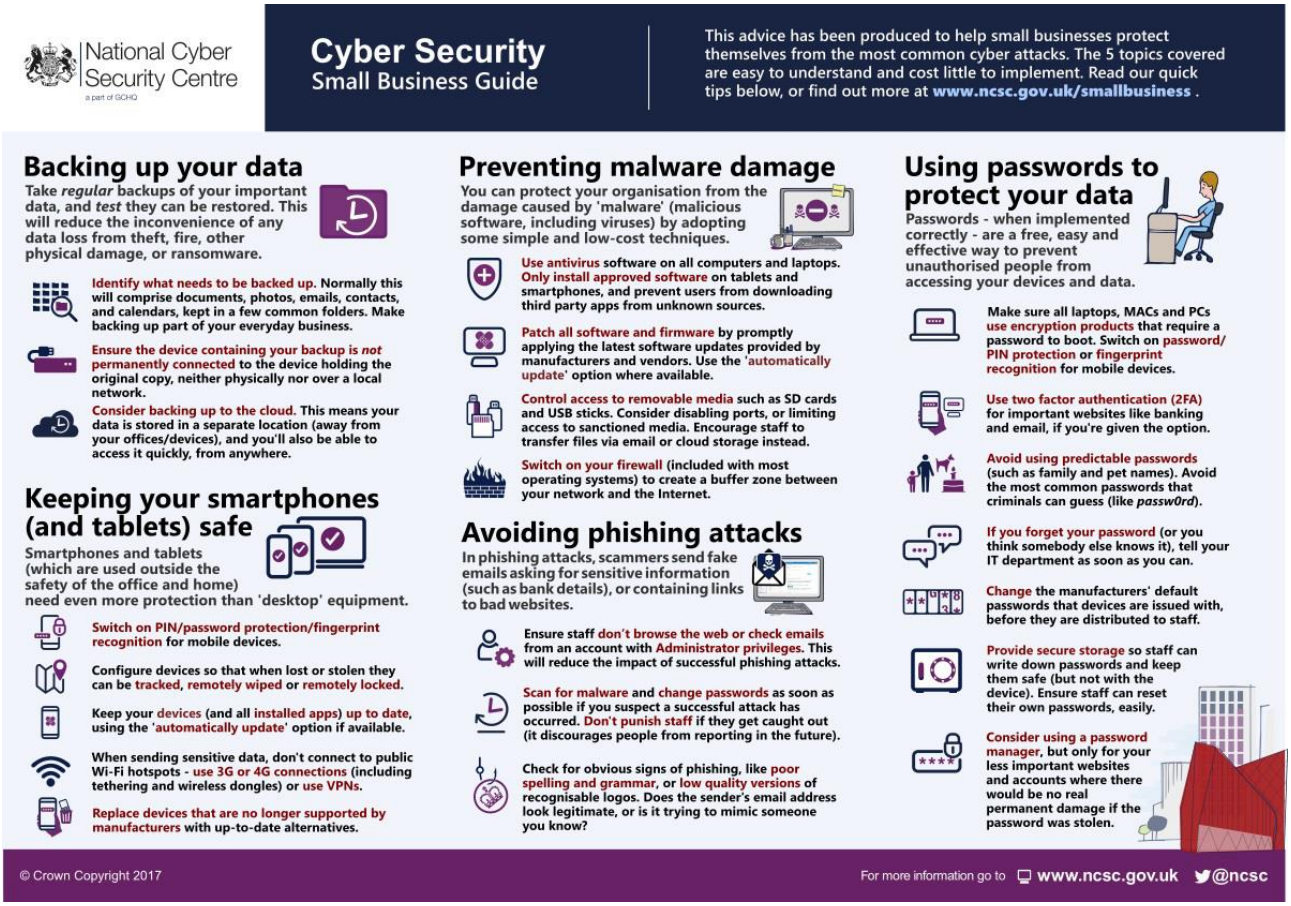
Attackers are always trying different methods of attack, even when tools like automatic email protection have prevented previous attempts. So it's worth keeping on top of the techniques used by attackers, to try and stay one step ahead. Consider signing up for the free Action Fraud Alert service[31] to receive direct, verified, accurate information about scams and fraud in your area by email, recorded voice and text message.

Monitor the advice from your local Police Service, and Regional & Organised Crime Unit (ROCU), who will put out warnings of specific cyber crime activity in your area. Join CiSP[32] which provides a forum for cyber security discussion from beginner through to expert level. It's also a platform where organisations can share intelligence gathered from their own computer networks.

[31] http://www.actionfraud.police.uk/signup
[32] https://www.ncsc.gov.uk/cisp

Infographic summary

The following infographic summarises the tips provided in this guidance. You can download a high-quality PDF version of this at the NCSC website at www.ncsc.gov.uk/smallbusiness.



National Cyber Security Centre
a part of GCHQ

Cyber Security:
Small Business Guide

Organisations can carry out the following actions in accordance with the guidance contained in the Small Business Guide.

Implementing these actions will significantly reduce the chance of you becoming a victim of cyber crime. To find out more, please visit **ncsc.gov.uk/smallbusiness**

Find out more

For further information, or to contact us, please visit:
www.ncsc.gov.uk

@ncsc

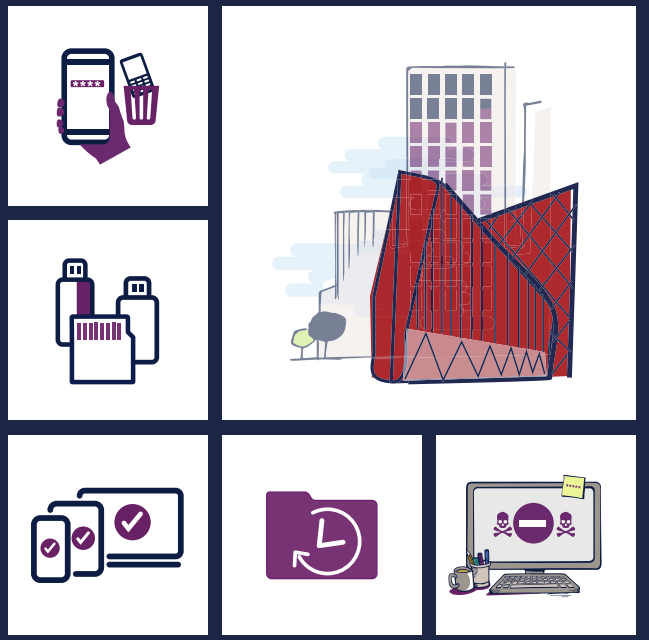
Information correct at time of publication – February 2018

National Cyber Security Centre
a part of GCHQ

National Cyber Security Centre
a part of GCHQ

Cyber Security:

Small Business Guide Actions



How to improve cyber security within your organisation – quickly, easily and at low cost.

Policy actions

These actions should be carried out by staff responsible for determining the overall cyber security policy.

- ☐ Identify and record essential data for regular backups.
- ☐ Create a password policy.
- ☐ Decide what access controls your users need so they can access only the information and systems required for their job role.
- ☐ Decide what staff need access to USB drives
- ☐ Sign up to threat alerts and read cyber local advice e.g. briefing sheets/threat reports from www.actionfraud.police.uk/signup.
- ☐ Create an inventory of approved USB drives and their issued owners, and review whether the ownership is necessary periodically.

Technical actions

These actions should be carried out by technical staff responsible for the setup and configuration of devices, networks and software.

- ☐ Switch on your Firewall.
- ☐ Install and turn on Anti-virus software.
- ☐ Block access to physical ports for staff who do not need them.
- ☐ Consider making a password manager available to your staff to secure their passwords. Review the star ratings before choosing one from an app store.
- ☐ Ensure data is being backed up to a backup platform e.g. portable hard drive and/or the cloud.
- ☐ Set automated back-up periods relevant to the needs of the business.
- ☐ Switch on password protection for all available devices. Change default passwords on all internet-enabled devices as per password policy.
- ☐ Install and turn on tracking applications for all available devices e.g. Find my iPhone.
- ☐ Enable two-factor authentication for all important accounts (eg email).
- ☐ Apply restrictions to prevent users downloading 3rd party apps.
- ☐ Install the latest software updates on all devices and switch on automatic updates with periodic checks.
- ☐ Ensure all applications on devices are up to date and automatic updates have been set to download as soon as they are released. Schedule regular manual checks on updates.
- ☐ Set up encryption on all office equipment. Use products such as Bitlocker for Windows using a Trusted Platform Module (TPM) with a PIN, or FileVault (on mac OS).

Training and awareness actions

These actions should be carried out by staff responsible for implementing staff training and awareness.

- ☐ Provide secure physical storage (eg a locked cupboard) for your staff to write down and store passwords.
- ☐ Create a Cyber Security training plan that you can use for all staff.
- ☐ Include details of your ‘Password’ policy explaining how to create a non-predictable.
- ☐ Include how to spot the obvious signs of phishing.
- ☐ Include details of your reporting process if staff suspect phishing.
- ☐ Include details on how your business operates and how they deal with requests via email.
- ☐ Include details of Wi-Fi hotspot vulnerabilities and how to use alternative options (eg VPN/ Mobile network).