National Cyber Security Centre
a part of GCHQ

10 Steps to Cyber Security

This collection is designed for security professionals and technical staff as a summary of NCSC advice for medium to large organisations. We recommend you start by reviewing your approach to risk management, along with the other nine areas of cyber security below, to ensure that technology, systems and information in your organisation are protected appropriately against the majority of cyber attacks and enable your organisation to best deliver its business objectives.

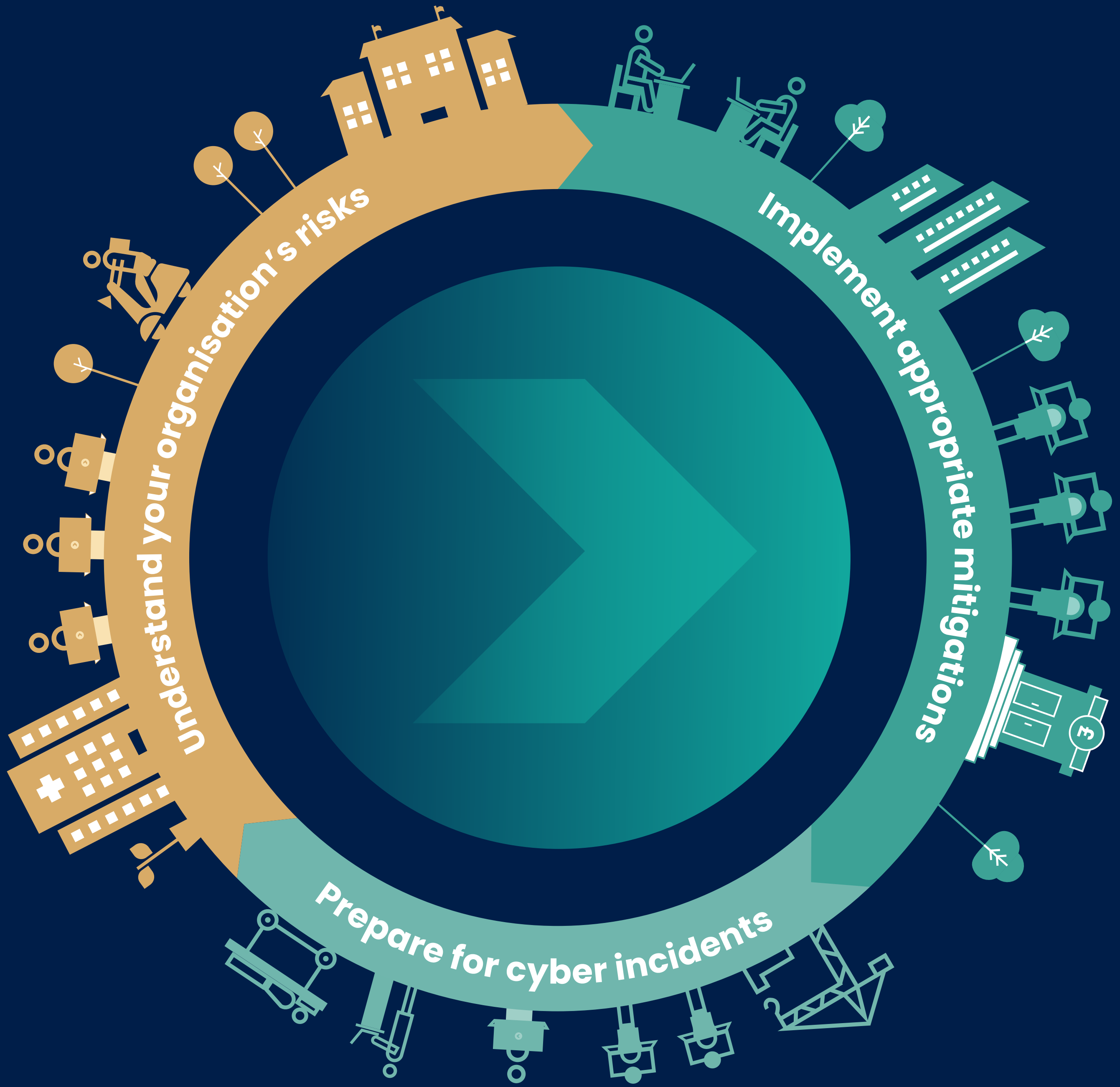
Risk management
Take a risk-based approach to securing your data and systems.

Engagement and training
Collaboratively build security that works for people in your organisation.

Asset management
Know what data and systems you have and what business need they support.

Architecture and configuration
Design, build, maintain and manage systems securely.

Vulnerability management
Keep your systems protected throughout their lifecycle.



Understand your organisation's risks
Implement appropriate mitigations
Prepare for cyber incidents

Identity and access management
Control who and what can access your systems and data.

Data security
Protect data where it is vulnerable.

Logging and monitoring
Design your systems to be able to detect and investigate incidents.

Incident management
Plan your response to cyber incidents in advance.

Supply chain security
Collaborate with your suppliers and partners.

www.ncsc.gov.uk   @NCSC   National Cyber Security Centre   @cyberhq

CYBER SECURITY BREACHES SURVEY 2021

UK BUSINESS TRENDS

The Cyber Security Breaches Survey is an official statistic. Since 2016, it has measured how UK organisations approach cyber security, and the impact of breaches and attacks. This infographic shows the key findings for UK businesses.

1.

Despite COVID-19, cyber security remains a priority among management boards. 77% of businesses say that cyber security is a high priority for their directors or senior managers (vs. 69% in 2016).

2.

Phishing is the most commonly identified cyber attack. Among the 39% identifying any breaches or attacks, 83% had phishing attacks, 27% were impersonated and 13% had malware (including ransomware).

3.

Unprepared staff risk being caught unaware. A total of 14% of businesses train staff on cyber security and 20% have tested their staff response, for example with mock phishing exercises.

4.

Businesses are adapting to new work patterns that affect cyber security. Fewer now have firm rules preventing staff from using personal devices for work (64% vs. 69% in 2020).

5.

COVID-19 has made cyber security harder. With resources stretched, fewer businesses report having up-to-date malware protection (83%, vs. 88% in 2020) and network firewalls (78%, vs. 83% in 2020).

6.

Businesses can better prepare for future uncertainties. In total, 31% have business continuity plans that mention cyber security and 15% have done an audit of their cyber security vulnerabilities.

For the full results, visit www.gov.uk/government/statistics/cyber-security-breaches-survey-2021.

Technical note: Ipsos MORI carried out a telephone survey of 1,419 businesses (excluding sole traders, and agriculture, forestry and fishing businesses) from 12 October 2020 to 22 January 2021. This included 654 businesses that identified a breach or attack in the last 12 months. Data are weighted to represent UK businesses by size and sector.

For further cyber security guidance for your business, visit the National Cyber Security Centre website (www.ncsc.gov.uk).

This includes COVID-19 guidance covering:

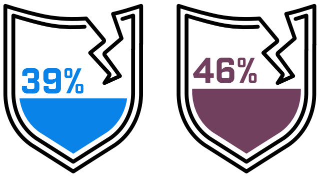
- **home working**
- **video conferencing**
- **moving your business online.**

Department for
Digital, Culture,
Media & Sport

Ipsos MORI

UK BUSINESS TRENDS

EXPERIENCE OF BREACHES OR ATTACKS



of businesses identified cyber security breaches or attacks in the last 12 months **(down from 2020)**

£8,460 is the average annual cost for businesses that lost data or assets after breaches

AMONG THE 39% IN 2021:

27% were attacked at least once a week

23% needed new measures to stop future attacks

DEALING WITH COVID-19

47% have staff using personal devices for work

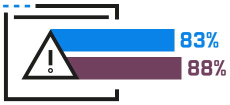
18% cover use of personal devices for work in a cyber security policy

34% have a VPN for remote working

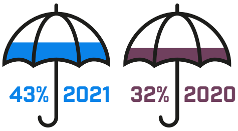
23% cover home working in a cyber security policy

MANAGING RISKS

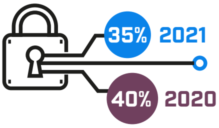
83% have up-to-date malware protection **(down from 2020)**



43% have cyber insurance cover **(up from 2020)**

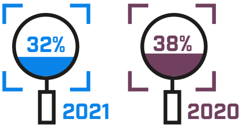


35% have used security monitoring tools **(down from 2020)**



34% have done a cyber risk assessment

32% monitor user activity **(down from 2020)**



Is **Cyber Essentials** for you?

Businesses of all shapes and sizes use Cyber Essentials to help protect their IT from attack. You could too.

No matter what your organisation does, Cyber Essentials can help to keep the devices and data you rely on safe.

We understand that not everyone has a dedicated IT department, or an in-depth knowledge of cyber security.

Cyber Essentials has been designed to be flexible, taking into account all types and sizes of organisation.

Certification will reassure current and potential customers that you take cyber security seriously. You'll also be listed in our directory of certified organisations.

CYBER ESSENTIALS

Further information

Information online that will help you secure your IT against cyber attack.

www.cyberessentials.ncsc.gov.uk

www.ncsc.gov.uk/smallbusiness

www.ncsc.gov.uk/charity

www.ncsc.gov.uk/guidance/10-steps-cyber-security

www.iasme.co.uk/cyberessentials

National Cyber Security Centre
a part of GCHQ

IASME CONSORTIUM

CYBER ESSENTIALS

Protect your organisation against the most common cyber attacks

To find out more please visit
www.cyberessentials.ncsc.gov.uk

National Cyber Security Centre
a part of GCHQ

IASME CONSORTIUM

What is **Cyber Essentials?**

Cyber Essentials is a simple and effective Government backed scheme that will help you protect your organisation against a range of the most common cyber attacks.

From the small scale startup to the established and growing business, Cyber Essentials will help you avoid the consequences of such things as:

- ✓ **Phishing attacks**
- ✓ **Malware**
- ✓ **Ransomware**
- ✓ **Password guessing**
- ✓ **Network attacks**

Our advice, in the shape of five technical controls, is easy to implement and designed to guard against these attacks.

Two levels of confidence

The NCSC works in partnership with The IASME Consortium to deliver Cyber Essentials, ensuring that the scheme continues to evolve to meet the cyber security challenges of the future.

- ✓ Cyber Essentials self-assessment is a first step towards helping you protect your business from the most common cyber attacks. The process is simple and certification costs around £300.
- ✓ Cyber Essentials Plus still has the Cyber Essentials trademark simplicity of approach, and the protections you need to put in place are the same, but for Cyber Essentials Plus a hands-on technical verification is carried out.

For more information about how to get certified visit www.cyberessentials.ncsc.gov.uk

How does **Cyber Essentials** work?

Cyber Essentials sets out five controls which you can implement immediately to strengthen your cyber defences:

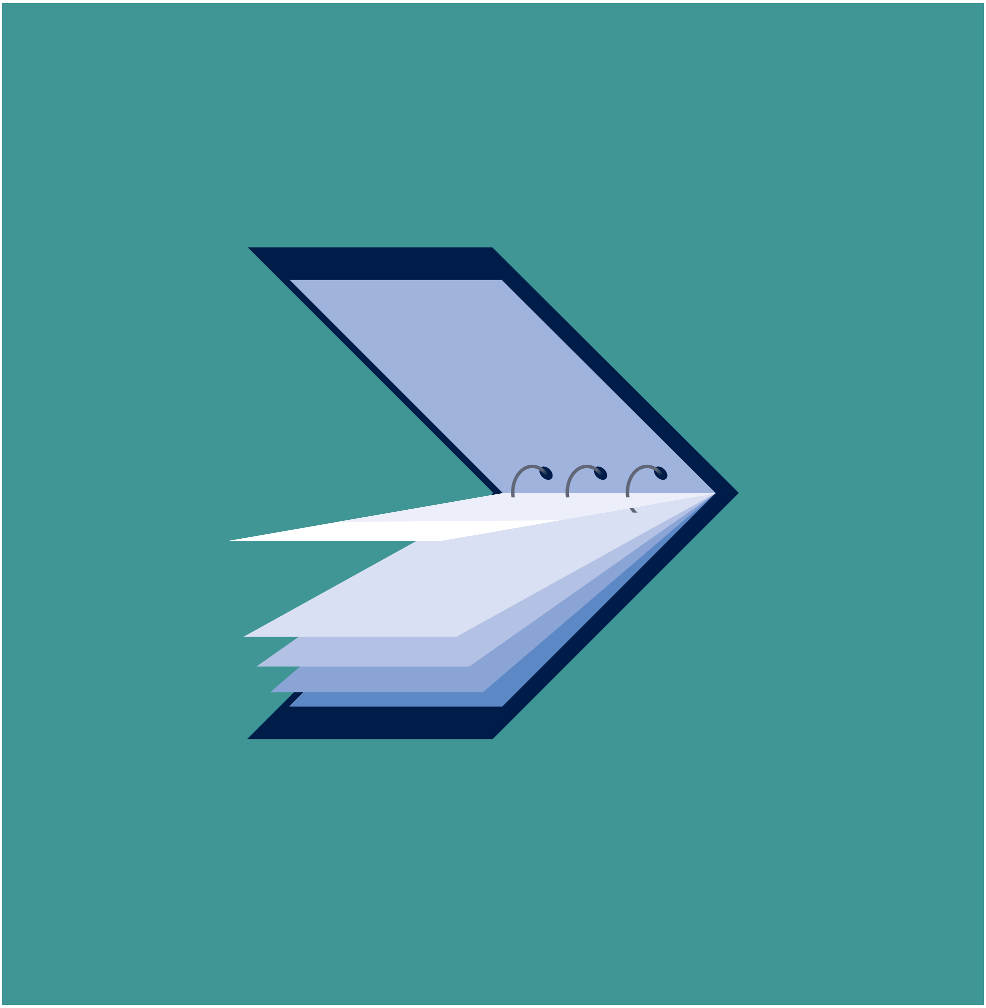
1. Use a firewall to secure your internet connection
2. Choose the most secure settings for your devices and software
3. Control who has access to your data and services
4. Protect yourself from viruses and other malware
5. Keep your devices and software up to date

National Cyber Security Centre
a part of GCHQ

Cyber Security
Small Business Guide

Small Business Guide Collection

How to improve your cyber security; affordable, practical advice for businesses



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 £900.

Following the advice in this guide will significantly increase your protection from the most common types of cybercrime. 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 cybercrime, then the 10 Steps to Cyber Security[2] can further help your approach to cyber security.

The National Cyber Security Centre want to make it easy for people to understand how to protect their information and IT against cyber attack[3], 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.

Sarah Lyons
NCSC Deputy Director
Economy & Society Engagement

[1] https://www.cyberessentials.ncsc.gov.uk/

[2] https://www.ncsc.gov.uk/collection/10-steps-to-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/guidance/mitigating-malware-and-ransomware-attacks

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/collection/cloud-security

[6] https://www.ncsc.gov.uk/collection/protecting-bulk-personal-data

[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 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/guidance/mitigating-malware-and-ransomware-attacks

[9] https://www.ncsc.gov.uk/collection/mobile-device-guidance

[10] https://www.ncsc.gov.uk/collection/mobile-device-guidance/antivirus-and-other-security-software

[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[12].

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

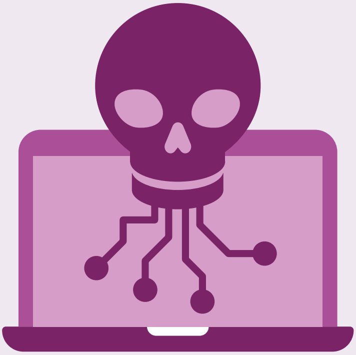
Firewalls create a 'buffer zone' between your own network and external networks (such as the Internet). Most popular operating systems now include a firewall, so it may simply be a case of switching this on. For more detailed information on using firewalls, refer to the Network Security section of the NCSC's 10 Steps to Cyber Security[13].

Find out more

More detailed, technical advice on preventing malware is available from the NCSC's 10 Steps to Cyber Security[14].

For detailed information on removable media, refer to the removable media section of the NCSC's 10 Steps to Cyber Security[15].

How to protect your PC from viruses (Microsoft guide)[16].



[12] https://www.ncsc.gov.uk/collection/mobile-device-guidance/using-peripherals-securely

[13] https://www.ncsc.gov.uk/guidance/10-steps-network-security

[14] https://www.ncsc.gov.uk/guidance/10-steps-malware-prevention

[15] https://www.ncsc.gov.uk/guidance/10-steps-removable-media-controls

[16] 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 actionable 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[17] (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[18], 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.

[17] https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0

[18] 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)[19], 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[20].

Find out more

If you're about to invest in a new device, we recommend you read our Buyer's Guide to Choosing and Using Mobile Devices[21].

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[22].

[19] https://www.ncsc.gov.uk/collection/mobile-device-guidance/virtual-private-networks

[20] https://www.ncsc.gov.uk/collection/mobile-device-guidance/using-third-party-applications

[21] https://www.ncsc.gov.uk/collection/mobile-device-guidance/choosing-devices https://www.ncsc.gov.uk/collection/mobile-device-guidance/purchasing-devices

[22] 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[23] 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)[24] with a PIN, or FileVault (on macOS)[25] 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[26] 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[27], which criminals can easily guess. The NCSC have some useful advice on how to choose a non-predictable password[28].

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.

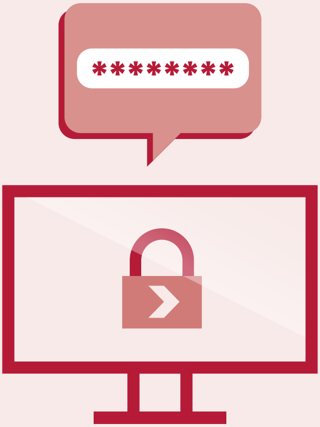
Consider using password managers[29], which are tools that can create and store passwords for you that you access via a 'master' password. Since the master password is protecting all of your other passwords, make sure it's a strong one, for example by using three random words.

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[30].



[23] https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0

[24] https://technet.microsoft.com/en-us/library/cc766295(v=ws.10).aspx

[25] https://support.apple.com/en-gb/HT204837

[26] https://www.ncsc.gov.uk/guidance/helping-end-users-manage-their-passwords

[27] https://www.teamsid.com/worst-passwords-2015/

[28] https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0

[29] https://www.ncsc.gov.uk/blog-post/what-does-ncsc-think-password-managers

[30] https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach

Avoid 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 for accessing your organisation's information[31].

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 the first steps you need to take 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[32].

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.

- 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.
- You can test how resilient your organisation is to phishing attacks by carrying out cyber security exercises. The NCSC's free Exercise in a Box tool[33] includes scenarios that include phishing.

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.

It is also important to integrate phishing guidance into your 'business as usual', so look to include messages across your company communications. This can include induction/onboarding processes, security news bulletins, communication campaigns, management training courses, prompts/banners on email, and more formal security refresher training. This will help to reinforce a culture of security mindedness.

[31] https://www.bbc.co.uk/news/uk-38332266

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

[33] https://exerciseinabox.service.ncsc.gov.uk/

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[34]. Action Fraud is the UK's national fraud and cyber crime reporting centre. If you are in Scotland contact Police Scotland on 101.

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[35] 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[36] 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.

A final word

Don't leave the responsibility for cyber security with a single person. Every member of the team (including board members) needs enough knowledge to understand how cyber security impacts on their area of focus.

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

[35] https://www.actionfraud.police.uk/sign-up-for-action-fraud-alert

[36] https://www.ncsc.gov.uk/cisp

National Cyber Security Centre
a part of GCHQ

Cyber Security

Small Business Guide

This advice has been produced to help small businesses protect themselves from the most common cyber attacks. The 5 topics covered are easy to understand and cost little to implement. Read our quick tips below, or find out more at **www.ncsc.gov.uk/smallbusiness**

Backing up your data

Take regular backups of your important data, and test they can be restored. This will reduce the inconvenience of any data loss from theft, fire, other physical damage, or ransomware.

- **Identify what needs to be backed up**. Normally this will comprise documents, photos, emails, contacts, and calendars, kept in a few common folders. Make baking up part of your everyday business.
- **Ensure the device containing your backup is not permanently connected** to the device holding the original copy, neither physically nor over a local network.
- **Consider backing up to the cloud.** This means your data is stored in a seperate location (away from your offices/devices), and you'll also be able to access it quickly, from anywhere.

Keeping your smartphones (and tablets) safe

Smartphones and tablets (which are used outside the safety of the office and home) need even more protection than 'desktop' equipment.

- **Switch on PIN/password protection/fingerprint recognition** for mobile devices.
- Configure devices so that when lost or stolen they can be **tracked, remotely wiped or remotely locked**.
- Keep your **devices** (and all **installed apps**) **up to date**, using the **'automatically update'** option if available.
- When sending sensitie data, don't connect to public Wi-Fi hotspots - **use 3G or 4G connections** (including tethering and wireless dongles) or **use VPNs**.
- **Replace devices that are no longer supported by manufacturers** with up-to-date alternatives.

Preventing malware damage

You can protect your organisation from the damage caused by 'malware' (malicious software, including viruses) by adopting some simple and low-cost techniques.

- **Use antivirus** software on all computers and laptops. **Only install approved software** on tablets and smartphones, and prevent users from downloading third party apps from unknown sources.
- **Patch all software and firmware** by promptly applying the latest software updates provided by manufacturers and vendors. Use the '**automatically update**' option where available.
- **Control access to removable media** such as SD cards and USB sticks. Consider disabling ports, or limiting access to sanctioned media. Encourage staff to transfer files via email or cloud storage instead.
- **Switch on your firewall** (included with most operating systems) to create a buffer zone between your network and Internet.

Avoiding phishing attacks

In phishing attacks, scammers send fake emails asking for sensitive information (such as bank details), or containing links to bad websites.

- Ensure staff **don't browse the web or check emails** from an account with **Administrator privileges**. This will reduce the impact of successful phishing attacks.
- **Scan for malware** and **change passwords** as soon as possible if you suspect a successful attack has occured. **Don't punish staff** if they get caught out (it discourages people from reporting in the future).
- Check for obvious signs of phishing, like **poor spelling and grammar**, or **low quality versions** of recognisable logos. Does the sender's email address look legitimate, or is it trying to mimic someone you know?

Using passwords to protect your data

Passwords - when implemented correctly - are a free, easy and effective way to prevent unauthorised people from accessing your devices and data.

- Make sure all laptps, Macs and PCs **use encryption products** that require a password to boot. Switch on **password/PIN protection** or **fingerprint recognition** for mobile devices.
- **Use two factor authentication (2FA)** for important websites like banking and email, if you're given the option.
- **Avoid using predictable passwords** (such as family and pet names). Avoid the most common passwords that criminals can guess (like passw0rd).
- **If you forget your password** (or you think someone else knows it), tell your IT department as soon as you can.
- **Change** the manufacturers' default passwords that devices are issued with, before they are distributed to staff.
- **Provide secure storage** so staff can write down passwords and keep them safe (but not with their device). Ensure staff can reset their own passwords, easily.
- **Consider using a password manager**, 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.

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

@NCSC

National Cyber Security Centre

@cyberhq

Information correct at the time of publication - October 2020

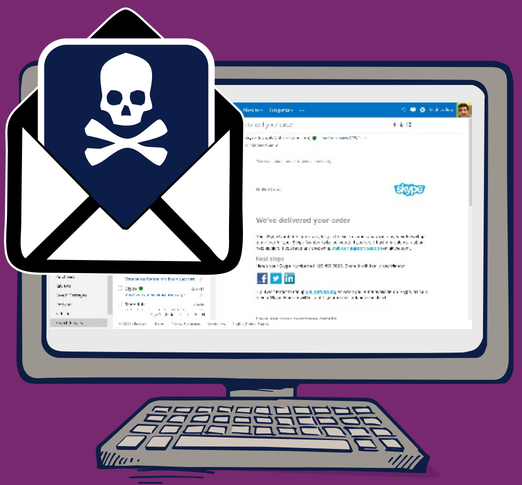
Designed and created by Agent Marketing Ltd.
agentmarketing.co.uk

National Cyber Security Centre

Phishing attacks

Dealing with suspicious emails

Phishing emails try to convince users to click on links to dodgy websites or attachments, or to give sensitive information away (such as bank details). This advice includes tips about how to spot the most obvious signs of phishing, and what to do if you think you've clicked a bad link. For more information, please visit **www.ncsc.gov.uk/phishing** .



What is phishing?

Phishing is when criminals attempt to trick people into doing 'the wrong thing', such as clicking a link to a dodgy website.

Phishing can be conducted via a text message, social media, or by phone, but the term 'phishing' is mainly used to describe attacks that arrive by email.

Criminals send phishing emails to **millions of people**, asking for sensitive information (like bank details), or containing links to bad websites. Some phishing emails may contain viruses disguised as harmless attachments, which are activated when opened.

Make yourself a harder target

Information from your website or social media accounts leaves a 'digital footprint' that can be exploited by criminals. You can make yourself less likely to be phished by doing the following:

Criminals use publicly available information about you to make their phishing emails appear convincing. Review your privacy settings, and think about what you post.

Be aware what your friends, family and colleagues say about you online, as this can also reveal information that can be used to target you.

If you have received an email which you're not quite sure about, forward it to the NCSC's suspicious Email Reporting Service (SERS): report@phishing.gov.uk

What to do if you've already clicked ?

The most important thing to do is not to panic. There are number of practical steps you can take:

Open your antivirus (AV) software, and run a full scan. Follow any instructions given.

If you've been tricked into providing your password, you should change your passwords on all your other accounts.

If you have lost money, you need to report it as a crime to Action Fraud. You can do this by visiting www.actionfraud.police.uk.

Tell tale signs of phishing

Spotting a phishing email is becoming increasingly difficult, and even the most careful user can be tricked. Here are some tell tale signs that could indicate a phishing attempt.

Is the email 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.

Others will try and create official-looking emails by including logos and graphics. Is the design (and quality) what you'd expect?

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 at the sender's name and email address. Does it sound legitimate, or is it trying to mimic someone you know?

Your bank (or any other official source) should never ask you to supply personal information in an email. If you need to check, call them directly.

If it sounds too good to be true, it probably is. It's most unlikely that someone will offer you designer trainers for £10, or codes to access films for free.

National Cyber Security Centre

Ransomware

Prevention & recovery

Following this advice can reduce the likelihood of you becoming a victim of ransomware. Ransomware makes your data or computers unusable and asks you to make a payment to release it. If your computer is already infected with ransomware, we've included some useful recovery steps below. For more information, please refer to **www.ncsc.gov.uk/ransomware** .

What is ransomware?

Ransomware is malicious software that prevents you from accessing your computer (or data that is stored on your computer).

If your computer is infected with ransomware, the computer itself may become **locked**, or the data on it might be **stolen**, **deleted** or **encrypted**.

Normally you're asked to make a payment (the ransom), in order to 'unlock' your computer (or to access your data).

However, even if you pay the ransom, there is no guarantee that you will get access to your computer, or your files. This is one of the reasons why it's important to **always have a recent backup** of your most important files and data.

Don't be blackmailed - keep a backup!

If you have a recent backup of your most important files, then you can't be blackmailed.

Make regular backups of your most important files (such as photos and documents), and check that you know how to restore the files from the backup. If you're unsure how to do this, you can search online.

Make sure the device containing your backup (such as an external hard drive or a USB stick) is not permanently connected to your computer.

Turn on auto-backup so that data on your smartphone is automatically copied to the cloud. This means you'll be able to recover your data quickly by signing back into your account from another device.

Protecting your data and devices

The following steps will reduce the likelihood of your devices being infected with ransomware.

Keep your operating system and apps up to date. Apply software updates promptly to help keep your device secure. This includes protection from ransomware and other types of virus. Set updates to happen automatically, so you don't forget.

Make sure your antivirus product is turned on and up to date. Windows and macOS have built in malware protection tools which are suitable for this purpose.

Avoid downloading dodgy apps. Only use official app stores (like Google Play or the Apple App Store), which provide protection from viruses.

What to do if you are infected

If your computer has been infected by ransomware (or any type of malware), you should:

Open your antivirus (AV) software, and run a full scan. Follow any instructions given. If your AV can't clean your device, you'll need to perform a 'clean re-install', which will remove all your personal files, apps and settings. If you're unsure how to do this, you can search online using another device, or ask family and friends.

Restore your backed-up data that you have kept on a separate device (such as USB stick, external hard drive) or cloud storage. Do not copy any data from the infected computer.

If you receive a phone call offering help to clean up your computer, hang up immediately (this is a common scam).

AF

Anyone who thinks they may have been subject to a ransomware attack should contact Action Fraud (www.actionfraud.police.uk). Organisations should call 0300 123 2040. In Scotland, contact the police by dialing 101.

Should I pay the ransom?

Law enforcement do not encourage, endorse, nor condone the payment of ransom demands. If you do pay the ransom:

- **there is no guarantee that you will get access to your data or computer**
- **your computer will still be infected**
- **you will be paying criminal groups**
- **you're more likely to be targeted in the future**

If you have paid any extortion demands you should report this to your local police force.

www.ncsc.gov.uk @NCSC National Cyber Security Centre @cyberhq

Work Safe at Home

Be safer with strong passwords. Many people don’t practice the same strong password habits on their personal home devices as they do at the office. Add a strong password and two-factor authentication to your Wi-Fi and the router, plus any other personal devices.

Know what needs to be protected. Jot down a list of everything you don’t want falling into the wrong hands and determine a security arrangement for each. Paper notebooks and folders. Company phone. Company computer. Portable hard drives. USBs. Contact lists. Customer lists. You probably have more than you think.

Using public Wi-Fi. Not recommended. Everybody should know the danger by now, yet 81% of recent survey respondents said they still use public Wi-Fi. If you are going to use the unsecured public network at your local coffee shop or library, think twice about exposing your company’s private information this way.

Ramp up your security awareness. While browsing the web and checking your email, be on the lookout for a tidal wave of malicious sites and emails designed to play off your COVID-19 related anxiety.

Guard your login credentials. When working remotely — especially in public spaces — take care to guard your login credentials. If they are seen or shared accidentally, you’ve made tracking down illegal access very hard for the security team.

Be a VIP with a VPN. Many companies have a VPN (virtual private network) as part of online protection packages for remote and traveling staff. For those not in the know, a VPN provides a secure, encrypted connection that tunnels data directly to its destination. If your company doesn’t have one, talk to your boss.

Be smart and ratchet up your security outlook. Keep your family and friends from using your work computer. Install an antivirus program in your home system. Get a copy of your company’s security policy and follow it. Lock up or shred confidential documents — don’t throw them in your home recycling bin. Don’t leave your laptop, documents or other devices in your car. Keep track of your smartphone.