



# Keeping your business safe online

A guide for micro and  
small businesses



# Contents

<b>Introduction</b> .....	<b>1</b>
Foreword .....	1
Why you need to think about keeping your business secure .....	2
How to make yourself more secure .....	3
<b>Step 1: Managing Risk</b> .....	<b>5</b>
<b>Step 2: Passwords</b> .....	<b>11</b>
2.1 Two-Factor Authentication (2FA) .....	12
2.2 User privileges .....	12
<b>Step 3: Preventing Viruses</b> .....	<b>13</b>
3.1 How could I get infected with a virus? .....	13
3.2 Antivirus Software .....	15
<b>Step 4: Security Settings</b> .....	<b>17</b>
4.1 How can I keep my equipment safe? .....	17
4.2 Protect your website .....	19
4.3 Encryption .....	19
4.4 How to browse safely online .....	21
4.5 Securing your web browser .....	22
<b>Step 5: Browsing and Sharing Safely</b> .....	<b>23</b>
5.1 Can I trust public Wi-Fi? .....	23
5.2 Data transfer and file sharing .....	24
<b>Step 6: Securing Your Own Equipment</b> .....	<b>25</b>
<b>Step 7: Peripherals</b> .....	<b>27</b>
<b>Step 8: Training</b> .....	<b>29</b>
<b>Step 9: Monitoring</b> .....	<b>31</b>
<b>Step 10: Managing Security Incidents</b> .....	<b>33</b>
<b>Further Information</b> .....	<b>35</b>

# Foreword

With an ever-increasing threat to online security, it's important you put in place the basic steps to keep your business and customers safe online.

I've been working in the cyber security industry for the last 16 years, before the word 'cyber' was even used. Back when I started, the issue was split between the annoyances of teenagers writing viruses for fun and the serious stuff reserved for nation states. Since then the field has exploded, with hacking incidents often making headline news and in some instances causing businesses to collapse.

Over the years I've helped translate cyber security jargon into a language all sorts of people can understand. This booklet helps break down this complex topic into basic steps, using everyday language so that you and your business can learn to become more secure online.



**Cath Goulding,**  
Head of Information  
Security at Nominet,  
Certified Information  
Systems Security  
Professional (CISSP)

# Why you need to think about keeping your business secure

You wouldn't go on holiday and leave all your windows wide open and the front door unlocked. So why leave your business systems open and easily accessible? You need to stay secure for three main reasons:

## 1

### To protect customer and employee data

A criminal can access your business data using a range of tools – and they no longer need to be a technical mastermind. A huge market has emerged where it can cost as little as £5 to make a website inaccessible for an hour. Without protection, criminals can easily access your customer and employee records.

## 3

### To comply with the law

There are numerous laws that may apply to you and your small business. For example, if you're dealing with personal customer data in the UK, you'll have to abide by the Data Protection Act 1998<sup>1</sup>. Failure to comply with the Act could prove very expensive, leading to prosecution and a maximum fine of £500,000.

## 2

### Customer integrity

Your customers need to know that their data will be safe in your hands, and a security breach could mean they're less likely to do business with you. As if that's not enough, cyber security is also likely to form part of supplier contracts that have clauses regarding confidentiality and data protection.

<sup>1</sup> <http://www.legislation.gov.uk/ukpga/1998/29/contents>

# How to make yourself more secure

In 2015, the UK government created a useful guide called '10 Steps to Cyber Security'<sup>2</sup>. It can be a bit daunting for those new to cyber security, so we've simplified it here and used it as a basis for this booklet.

## Step 1:

### Managing Risk

Identify the areas that you need to think about, even if you're unsure what you need to do about them. Create a checklist of focus areas where a threat could be costly.

## Step 2:

### Passwords

Make sure you know what makes a secure password as it's not always what you might imagine. If you have any employees, create a password policy to ensure secure passwords are always used in your business.

## Step 3:

### Preventing Viruses

Recognise how viruses spread, install antivirus software and understand how to deal with a virus if you get one.

## Step 4:

### Security Settings

Keep your equipment, data and website safe through measures such as encryption and regularly updating software and browsers.

## Step 5:

### Browsing and Sharing Safely

Take care if you're using public Wi-Fi and ensure you're safely transferring data, which could involve choosing the right cloud provider.

## Step 6:

### Securing Your Own Equipment

Make sure that personal equipment used by you or your employees for work purposes (such as smartphones) is secure.

## Step 7:

### Peripherals

Encrypt data on portable devices like USB memory sticks to protect confidentiality and your company's systems.

## Step 8:

### Training

If you have employees make sure they understand cyber security risks and keep anyone in your business up to date with security policies. You could also share this guide with them if it's appropriate.

## Step 9:

### Monitoring

Keep a log for your important IT systems which records any unusual or suspicious activity and alerts you to it.

## Step 10:

### Managing Security Incidents

Prepare for incidents by backing up data, know what to do if an incident occurs and know how to deal with employees who may be involved.



<sup>2</sup> [www.cesg.gov.uk/guidance/10-steps-executive-summary](http://www.cesg.gov.uk/guidance/10-steps-executive-summary)

# Step 1: Managing Risk

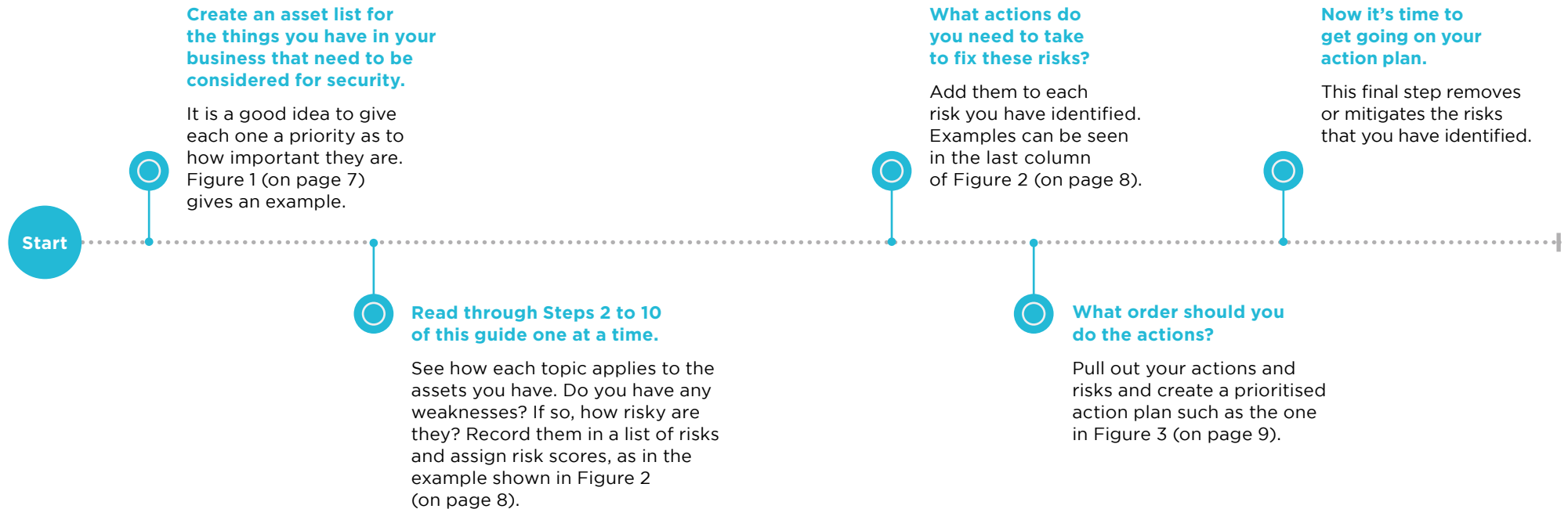
**It's important to realise that cyber security is a process rather than a goal.**

As technology evolves, so do the threats, and the steps outlined in this guide are designed to be used repeatedly. But you don't have to begin by rushing off to download software or chain your laptop to a desk. To start protecting your small business, you need to do some thinking and planning.

The following diagram gives you an overview of this and refers to three useful lists that you can compile, which we'll cover in more detail on the next three pages. You need to think about what assets you've got, what the risks are to your business and what you need to do about those risks.



## Risk Management Process



## Your assets

Get started by creating a list of your assets. It might include hardware like laptops and smartphones, or data such as customer data, financial information or your business plans. And it could also include services such as your website or emails.

Remember to give each asset a priority, as shown in the table below. You can group your assets or list them individually depending on what's appropriate for your business and it's handy to give each asset an ID number so that you can make easy references.

Figure 1: Asset list

Asset ID	Asset	Asset type	Priority High=5 Low=0
A01	Laptops	Equipment	2
A02	Business plans	Data	4
A03	Customer data	Data	5
A04	Website	Data	3

## Your risks

The next thing to do is to understand and list your risks. When you're reading this guide, think about your own business' assets so that you've got an idea of where your weaknesses are. You should also try to give a score for each risk by thinking about how easy it would be for an attacker to exploit a particular weakness and also how important the related assets are. The example given in Figure 2 uses a scale of 1-5 where

5 is the most risky. If you're unsure what risk score to give, we'd recommend using your best estimate and then increasing it, as it's better to be cautious. The final step is to record what action to take to fix the weakness, including risk IDs to make the actions easy to reference.

Figure 2 shows what a resulting list of risks might look like.

Figure 2: List of risks

Risk ID	Risk	Links to assets	Risk score High=5 Low=0	Action
R01	Laptops don't have latest versions of software	A01 A02 A03	5	Patch laptops
R02	Laptops have no passwords	A01 A02 A03	5	Add passwords to laptops
R03	Sensitive data not encrypted over email or when stored on laptop	A01 A02 A03	5	Encrypt laptops holding sensitive data  Check that emails are encrypted when in transit  Check cloud provider encrypts customer data
R04	Website doesn't have protection when it is under attack	A04	3	Perform cost benefit analysis of website protection services
R05	Backups taken monthly	A02 A03	3	Change backups to weekly
R06	No security policies	All	3	Write a security policy
R07	No security training	All	4	Deliver security training

### Your action plan

Get ready for action by pulling out the actions and risk scores from your list of risks. You'll need to prioritise the order in which you do the actions. A first step would be to order by the most risky. However, there may be

some quick wins that would be easy to address that you'd like to achieve earlier.

The example below shows what your action plan could look like.

Figure 3: Action plan

Action ID	Action	Links to risks	Risk score High=5 Low=0
Action 1	Add passwords to laptops	R02	5
Action 2	Patch laptops	R01	5
Action 3	Encrypt laptops holding sensitive data	R03	5
Action 4	Check cloud provider encrypts customer data	R03	5
Action 5	Check that emails are encrypted when in transit	R03	5
Action 6	Change backups to weekly	R05	3
Action 7	Deliver security training	R06	4
Action 8	Write a security policy	R07	4

You could add target dates to your spreadsheet, allocate responsibilities to particular employees (including yourself) and keep it updated with the steps you've taken. Remember that cyber security is a process rather than a goal, so you should go through this whole cycle whenever necessary.

We'd recommended that you do it whenever there are significant changes to your business or when you hear about a particular issue (for example when all LinkedIn passwords were compromised). Otherwise, you should plan to do it on a scheduled basis, such as every 6-12 months.

Remember that cyber security is a process rather than a goal, so you should go through this whole cycle whenever necessary.



# Step 2: Passwords

A password can be the door to lots of vital and confidential business information. So make sure you don't leave that door wide open.

You'll need to set up a password for most software and online services but there are some things you should bear in mind when you do. You should also have a password policy that applies to everyone who works for your business, and the below tips can be the basis for it.

1

Your password should contain a minimum of 8 characters.

2

Avoid the most common passwords such as 'password'.

3

Don't use a number sequence (1234) or repeated numbers (1111).

4

Try to think of it as a 'passphrase' rather than a single word - 'I love green apples' is much harder to guess than a single word.

5

Use uppercase letters, symbols and numbers - for example 'I love green apples' becomes 'I10v3gr33n@ppl3s'.

6

Don't use basic personal information such as family names.

7

Don't use the same password across different accounts - otherwise if one password is breached, they are all vulnerable.

8

You wouldn't share or write down the pin number for your bank account on a Post-it® note or a whiteboard. Don't do it with your password either.

We'd also recommend you change your passwords at least every six months. And yes, it can be tricky remembering them all, so use password management services such as LastPass and 1Password. They are often free to download, offer encryption (see our encryption advice later on) and can generate random, secure passwords. Which one you choose is completely down to you.

2.1

## Two-Factor Authentication (2FA)

Two-Factor Authentication gives an additional layer of protection for your online accounts by combining something you know like a PIN or password with something you have such as a specific device that generates codes or a software token on a smartphone. The chances are you've used this type of technology for things like online banking. Google, Microsoft and many other companies also provide services which can use two-factor authentication, which you can set up by accessing the settings in your application or device.

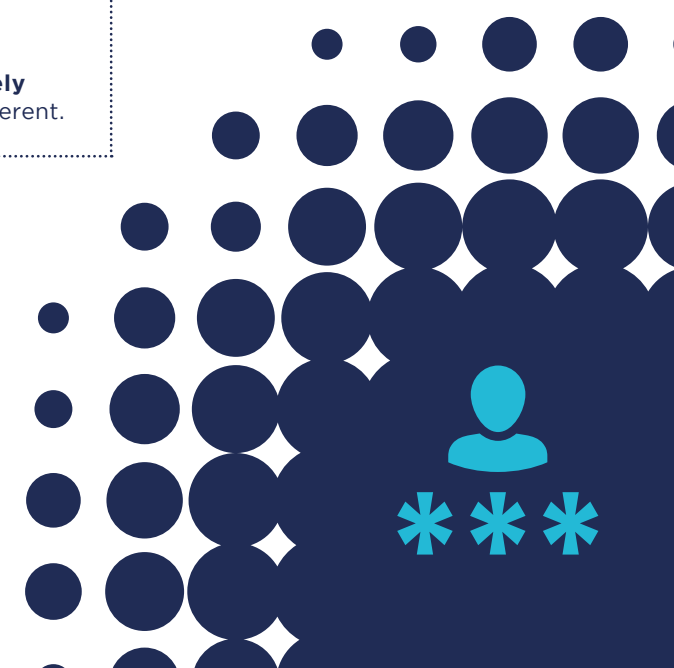
2.2

## User privileges

Who sees what within your business? It's a question you need to consider, and productivity tools such as Microsoft Office 365 or Google Apps for Business have access settings which let you structure your documents, allowing individuals to only see the ones that are relevant to them. We'd advise setting up the access rights as early as possible so that they can evolve as your business grows.

### Remember...

If you think your password has been compromised you should **change it immediately** to something completely different.





# Step 3: Preventing Viruses

Computer viruses aren't a new thing. It was back in 1983 that the term "virus" was originally coined, along with the notion of them "infecting" systems and programs. Since then, viruses have become much more sophisticated and widespread, so here's how to avoid them like the plague.

Some viruses are attached to emails and need you to actually do something to activate them, while others run on their own, looking for specific systems or programs to infect.

The good news is that there are a number of ways to minimise the threat of a virus, such as using antivirus software.

## 3.1 How could I get infected with a virus?

Here are a few examples of ways you could become infected with a virus:

- If you open attachments on suspicious emails.
- If you click on links within suspicious emails or visit untrusted websites.
- If you download files (usually free) from untrusted sources.
- If you click/accept pop-ups when you're using the internet.
- If you access pirated content online.
- If you have USB memory sticks from third parties and connect them to your machine.

### Top tip...

Read customer reviews of antivirus software to help assess what's good (and what's not) when it comes to dealing with viruses.

Most viruses are caused by a human interaction, which is usually accidental or happens because of a lack of understanding. And if you're using a Mac operating system, don't believe the myth that Macs don't get viruses. **They do!**

There are a number of ways to minimise the threat of a virus.



## Definitions

### Virus:

A virus (also known as malware) is capable of copying itself and having a negative impact on your business, such as corrupting your computers or destroying your data.

### Pop up:

Small windows that literally 'pop up' while you're browsing the internet.

### Operating System:

The most important program on a computer, as every other program runs off it. Every general-purpose computer must have some sort of operating system installed to perform even the most basic of tasks. An example of a common operating system is Windows.

### Spam:

Sometimes referred to as 'junk mail' this usually takes the form of advertising emails sent out from a company or organisation to an email list.

### Firewall:

A barrier that only allows approved applications to communicate.

### 3.2

#### Antivirus Software

You'll be pleased to know that there are some simple steps you can take to protect yourself and your business. Some of these steps involve software, while others are based on common sense.

## 1

#### Install trusted antivirus software

Think of this as your essential front line of defence. Try to choose an antivirus product from a trusted vendor such as McAfee, Norton or Windows Security Essentials.

## 2

#### Ensure this software is up to date and is always active

Make sure you accept any automatic updates.

## 3

#### Ensure a firewall is active

A firewall is a barrier that stops viruses accessing your computers and systems. There's a Windows Firewall on machines running Windows and an Application Firewall for Apple Macs, which you can find under the respective operating system's security settings in the control panel.

## 4

#### Don't open any suspicious emails or links online

If the content or address on an email seems unusual, don't take any chances. Avoid the temptation to click links within these emails or follow any of their instructions.

## 5

#### Avoid free software unless it's from a guaranteed trusted source

There's a whole host of free or cheap software available online but very often when it appears too good to be true, it usually is.

## 6

#### Block all spam emails

Nearly all web-based (Gmail, Hotmail, Yahoo) or computer based email (Outlook, Thunderbird) contain a spam filter for unwanted spam emails. If a spam email does sneak through into your inbox, simply click the 'Spam' or 'Junk' button to get rid of it. These emails will now be sorted into a dedicated folder and deleted automatically.

## 7

#### Complete a full scan of your machine on a regular basis

All major antivirus software will perform scheduled quick-scans on your machine but you should still try to do a full scan regularly.

#### Remember...

If you do get a virus, you might start thinking it's the beginning of the end. **But don't panic** – and focus instead on the steps you need to take to get rid of it.

#### Don't ignore it

Do a full scan with your antivirus software. Identify the virus and follow the instructions on-screen for removal.

#### Remove the threat

Make sure the virus is removed and there are no further problems. Run through a quick health check of your machine to see if it's running correctly and that any issues have been resolved.

#### Reconnect and update

Reconnect your machine and 'Check for Updates' on your antivirus software. If any are available, download and install them right away.

If this clears the virus, breathe a sigh of relief. If it doesn't, you can restore your computer by essentially rolling it back to a time before the virus was present (see step 10 for more on this). Although this should solve the problem, it does mean you'll lose any files you've updated since your last back up. If this isn't an option, contact an IT specialist to help save your files and reinstall your operating system and other software.

#### Know the signs...

When you've got a virus, there are some tell-tale signs that all is not well with your computer:

- Machine runs slowly or behaves strangely.
- Email bounces back, or you receive "read" receipts for emails you haven't sent.
- Antivirus or firewall protection suddenly turns off without your approval.
- Strange pop-ups or extra toolbars appear.
- Web browser takes you straight to an unknown site on start up.

# Step 4: Security Settings

When it comes to your security settings, the key thing is to make sure all your software is up to date. It doesn't matter if you're using a Mac or Windows computer – when you're prompted to update your software you should do it straightaway, as the update will often contain improved security settings.

It's also really important to think about how you protect your business equipment. You might have insured your equipment but what about the data that's on it? Ensure you've got a robust plan in place so you can retrieve any data from affected devices.

Think about what would happen if someone stole the equipment or if it was damaged by flooding, fire or simply spilling a cup of coffee on it.

## 4.1 How can I keep my equipment safe?

Here are some common-sense tips for keeping your equipment – and the data stored on it – safe.



### Computers (Desktop machines and laptops)

- Make a note of all serial/asset numbers for any computer equipment and keep them safe.
- Consider securing computers to desks with a locking cable and lock laptops away after use.
- Keep your laptop with you whenever possible (and don't be tempted to leave it in the car while you go elsewhere).
- Set up separate computer accounts if a machine has multiple users.
- Ensure all employees use secure passwords and lock screens when away from their equipment.
- Assign specific assets to named individuals so you know who has what equipment.
- Never store passwords on a work machine, particularly a laptop.
- Consider disabling USB ports on work machines to prevent malicious use such as copying confidential company files.
- Run regular backups of data.



### Portable Devices (Phones, tablets, USB memory sticks, external hard drives and CD/DVD's)

- Set up remote locking of mobile devices by using Android Device Manager for Android phones, Find My iPhone for Apple phones and Find My Phone for Windows Phones.
- Make a note of IMEI serial numbers on mobile devices (to get this, type \*#06# into your phone dialler).
- Encrypt all business information data.
- Set up user accounts where necessary and restrict access to apps/information accordingly.
- As a minimum, all mobile devices should be password protected. Phones should have SIM locks and should be set to lock automatically after the device goes into sleep mode.
- Check sync settings to make sure unwanted/sensitive information isn't being backed up or unnecessarily copied onto the device.
- Limit use of public, unsecured Wi-Fi and don't send sensitive data across them.
- Ensure Bluetooth is disabled when in public and that the device is not 'discoverable'.
- Lock away any portable media devices and discs that contain confidential or sensitive business information, just like you'd do with hard copies.

## Definitions

**IMEI:**  
International Mobile Equipment Identity – a unique number given to every mobile phone

**Wi-Fi:**  
The common standard of wireless communication between computers or devices

## Remember...

- It's not just the device that's valuable, the stored data is too.
- Know where your equipment is at all times.
- Communicate security policies to any employees and regularly review them.

#### 4.2 Protect your website

Your website and emails are also assets of your business and they're not immune to scams, which include your website being 'hijacked' and visitors being directed to a fraudulent site. The same problem could also affect your email and cause your messages to be sent elsewhere. You'll need to contact your domain name provider immediately if you suspect this is happening. Meanwhile there are a few preventative steps you can take to stop these scams or to minimise their effects:

- Only use reputable domain name providers and hosting companies.
- Check what security protection they're offering.
- Make sure your contact details are up to date.
- Report issues back to them quickly.
- Ensure you're on a trusted domain name that operates under UK law and offers UK support, such as .co.uk or .uk.

#### 4.3 Encryption

Encryption is the process of protecting documents in such a way that only authorised parties can access them. When you've got vital business information, encryption will not only help to protect it but may also support any legislation requirements you have and give your customers confidence that you're a secure business. Encryption might sound a bit scary, but it doesn't have to be costly or difficult to implement. It can be applied to email, file sharing, removable media devices (USB memory sticks, hard drives) and even your computer.

Exactly what you choose to encrypt is up to you but below are some of the main areas to consider:



Email

There are three main ways you can approach email encryption:

**Microsoft Outlook:**  
Controlled from the security settings within the email.

**Apple Mac:**  
Acquire a security certificate and link this to your Apple Mail. For more information visit <https://support.apple.com>.

**PGP (Pretty Good Privacy) Email:**  
Free/low-cost software which has become the de-facto standard for email encryption.



File sharing

When you're sharing information, you don't want it to fall into the wrong hands – and encryption goes a long way to ensuring it won't. It can be done directly or through the use of cloud based services, which depends on whether you're looking to send one file to someone or are looking to set up a more collaborative working environment, such as when building your website with a web design agency.

Some options are:

**Secure File Transfer Protocol (SFTP):**  
Often protected with a password, this is a common file encryption system for businesses.

**Cloud Storage:**  
Examples are Google Drive, Dropbox, Box and OneDrive, which offer varying levels of encryption.



Your website

If your business sells goods or services online, you need to know about SSL (Secure Socket Layer) Encryption, which ensures the privacy of the data transferred when people buy from you. You can tell if a website is running SSL by looking for the 'https' prefix at the beginning of the website address, usually accompanied by a small padlock next to the address bar or at the bottom of the browser.

It's highly recommended that you use some form of SSL encryption if you're in the business of e-commerce, and you can do it by purchasing a certificate from your provider and setting it up on your website.

### Definition

**Hosting:**  
The service that provides the location where your website is stored and maintained.

### Remember..

To encrypt removable media, such as USB memory sticks – **see Step 7 for more** on how to do this.



#### 4.4 How to browse safely online

You don't go through life believing absolutely everything you hear. And when it comes to the internet, you can't always place your trust in what you see. When browsing online, you could be exposed to various threats, including viruses – and the key is to use your common sense.

If something doesn't look right, don't trust it. This could be anything from an unusual link within an email to a malicious website.

There are three things you should always avoid if you're unsure about any online content:

# 1

#### Do not open any suspicious emails or links online

If the content or address on an email seems unusual, then delete it. Do not be tempted to click links within these emails or follow any of their instructions. Spam emails can appear to be from legitimate organisations so beware of these and never click an attachment on emails like this. It could very well contain a virus or another type of malicious software. If you are not sure, contact the apparent sender of the email to verify they did in fact send it.

# 2

#### If you're ever in any doubt, don't fill in forms that request personal or financial information

You may be used to buying things online from reputable outlets but there are plenty of other websites that aren't so reliable. Seek advice if you or an employee is uncertain.

# 3

#### Avoid downloading untrusted software

You should also be aware of websites taking your cookie information. Cookies are text files that store information about you on a website, such as your username. Their aim is to provide a more convenient website experience – and most are completely safe. However, some cookies will basically spy on you, tracking your online activity, capturing your personal information and browsing habits so that advertisements or malicious sites can be pushed to you.

It's now a legal requirement for all UK websites to ask for your permission before using cookies and your browser can be configured to minimise their risk. We'd also advise you check your privacy settings on applications such as social media and webmail.

#### 4.5 Securing your web browser

Your internet browser is your window to the internet. Whichever one you choose to use, you should make sure that you always have the latest version of it installed. A few other things you can do to make sure your browser is secure are:

- Activate the pop-up blocker.
- Adjust security settings to control active content.
- Routinely delete any unused cookies.
- Always close your browser.

You should set your security settings high enough to protect you effectively without having a negative impact on the way a website actually functions.

## Definitions

### Cookie:

A message given from a web server to your web browser. This can include personal information and it helps a website recognise you.

### Domain Name:

Just as a street address allows people to physically find the location of your business, a domain name is the unique way to identify where you can be found on the internet. An example would be:  
**www.theukdomain.uk**

### SSL (Secure Sockets Layer):

A way of transmitting private information via the internet. This is often used for confidential information such as payment details and user information.

The key is to use your common sense. If something doesn't look right, **don't trust it.**



# Step 5: Browsing and Sharing Safely

As part of a small business, you'll often find yourself working from multiple locations, either at home, in a shared office or in a public place such as a coffee shop. Here are some tips on how to stay secure, including when you're working remotely.

## 5.1 Can I trust public Wi-Fi?

Public Wi-Fi is invaluable for small businesses, especially when it's free. But the key here is that it's public – and there will be other users who could intercept what you're doing. Be pragmatic – it's an invaluable tool but make sure you're taking the necessary steps to protect your business. For example, if you're accessing or sending any personal or confidential information, make sure it's encrypted.

And if your browser ever complains about a certificate, or flags an issue with a secure site – STOP immediately and go no further. That is one indication that someone is impersonating the website, and our technology can only do so much to help us if we ignore its warnings.

### Remember..

These days, browsers are very good at warning us when something is suspicious – **so pay attention when they do.**

## 5.2 Data transfer and file sharing

You'll deal with a wide variety of contacts at your business such as employees, customers, business partners, lawyers and accountants. And from time to time, you'll need to transfer data to them. If the data is small enough, you can send it via encrypted email but if the file is large your email provider may not be able to send it and you'll need to find a different way of sharing it securely.

You can also use cloud services to host your files, which are cheap and convenient because information saved in the cloud doesn't sit on your machine and can be accessed over the internet. Take a look at Dropbox, Google or Microsoft OneDrive, which are all good examples.

If you're accessing or sending any personal or confidential information, make sure it's encrypted.

# Step 6: Securing Your Own Equipment

You may well use your own, personal equipment (such as a smartphone) to carry out work. If that's the case, you need to make sure all of your company files are protected. We recommend the following steps when you or your employees are using your own devices:

1

## Only allow the use of personal devices running official operating systems

These operating systems are Windows, Android and Apple iOS and include modified versions from phone manufacturers (such as HTC Sense and Samsung TouchWiz).

2

## Ensure all devices are protected with a passcode or biometrics if available (fingerprint/iris scanner)

A simple passcode is fine and acts as a barrier to someone simply picking up a device and rummaging through it. You should also regularly back up your contacts in case your phone is hacked or stolen.

3

## Ensure all devices have a dedicated mobile antivirus package installed

It isn't just computers that can be affected by viruses. Many mobile phone operating systems have security features built-in but there are also free antivirus applications available on the official app stores (Google Play, iTunes, Windows Store).

4

## Change all passwords and permissions when an employee leaves

You wouldn't want an employee to keep a key to the office if they left the business and you don't want them being able to access your systems either. So any services used by an employee that provide access to confidential information should have their passwords changed to prevent access after the employee leaves the company. Many cloud services also allow you to de-authorise a specific device.

5

## Enable remote wiping and search tools

If the device supports remote wipe, enable it. Both Android and iPhone now do this out of the box. Don't forget to also change email passwords if any of your devices are lost, as well as installing an app to locate the device.

Don't forget to also change email passwords if any of your devices are lost.

### Definition

#### App:

Short for 'application' and commonly used to refer to mobile-based applications.





## Step 7: Peripherals

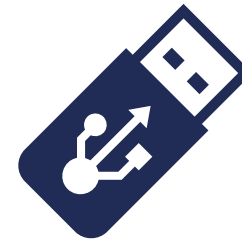
If you need USB memory sticks or portable hard drives to store work-related information, it's worth considering how these devices are used. They've got their uses but also their drawbacks, particularly as they can pick up viruses and bring them into your business.

You should consider encrypting any data on removable media and there are a number of ways to do this. Some will provide their own encryption, or you can use specific encryption software (PGP and VeraCrypt are a couple of examples).

For extra convenience, you can also use the built-in encryption provided by other software.

Microsoft Office 2007 and onwards provides good encryption as a built-in function for all documents types (Word, Excel etc) if required. The popular compression utility WinZip also provides strong encryption.

This can't guarantee 100% security but will help ensure the confidentiality of your data, and the integrity of your company's systems.



You should consider encrypting any data on removable media.





# Step 8: Training

## How to start security training

If your business has employees, making sure they're trained and up to date with security policies is vital. After all, it's no good being confident about your own cyber security knowledge if one of your employees isn't sure what they're meant to be doing.

Before you start your security training, you need to think about what's going to be included. Good security training should cover all the bases, outlining risks but also setting down clear codes of practice which means that when an incident does occur, your team will be educated and ready to deal with it quickly. It's an approach that will minimise disruption to your business, so here's what you might want to include as part of the training:

### Identify the Threats

Make sure you've identified and listed all potential cyber threats to your company. Your employees need to be able to spot them too.

### Outline the Risks

Identify the main risk areas for you and your business. And don't just acknowledge their existence - you need to know where and why you're particularly vulnerable.

### Explain the Consequences

Ensure your whole team understands the consequences for the business and its employees should a security incident occur.

### Establish the Controls

Explain what you've done and what procedures are in place to protect against cyber threats. Include information on why the procedures were chosen and the threat they're designed to tackle.

### Explain Staff Roles

How do these controls affect your staff and what are their responsibilities under these new measures? Build this into their job roles.

### Cover all legal Issues

There are legal criteria that might apply to your business, like data protection, confidentiality of information and software piracy and it's vital that all employees are aware of how important these regulations are and how they need to comply with them.


Security training shouldn't just be a tick-box exercise and we'd recommend you carry out reminder courses and provide regular communication to employees about the latest threats and guidance.

## Step 9: Monitoring

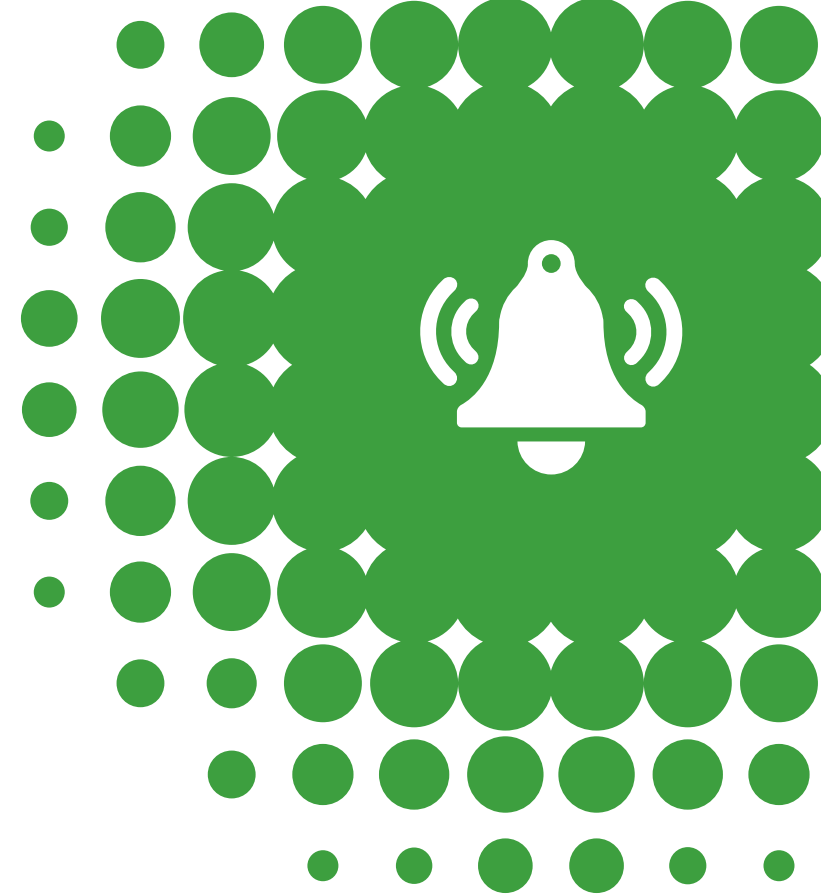
You should regularly check your logs to make sure the systems that are important to you are performing how they should be. Security software can detect and record suspicious activity, while operating systems usually log a variety of information.

For example, you can look at reports and events in your antivirus software, the logs in your firewall or the security logs in your “event viewer” in Windows. You can also look at logs for your file shares or email accounts to check who is accessing them and what they are looking at.

Your logs can alert you to any suspicious activity and it's recommended that you record the details of any such activity or particular security incidents.



Security software  
can detect and record  
suspicious activity.



You can look at logs for your  
file shares or email accounts to  
check who is accessing them.

# Step 10: Managing Security Incidents

If an incident does occur, you might have to 'roll back' your software to clear the infection, so it's essential that you run regular backups. They protect your data from accidental loss and help meet your legal obligations under the Data Protection Act.

'Backups' is a term you've probably heard before. It simply means copying your information over to another location so that you have a backup copy of it. But it really is a crucial step in securing your business information, as it helps to safeguard against human error, theft, damage and can improve your recovery from cyber-attack.

You can choose whether you backup to physical media or cloud storage and we've summarised these options here. Note that there may be a charge from the service provider for storing your files in the cloud.

Either backup all of the files on your computers or, if you're looking to minimise external hosting costs, you might want to pick only specific files (for example your documents but not your photos and videos).

You can do backups hourly, daily, weekly, or whenever suits your needs. For example, your business might only trade during the day, so you could schedule your backups to run at night. Both Apple's Time Machine for Macs and Windows Backup for PC's can be scheduled to run whenever you like, so you don't have to worry about it and can restore from any previous backup.

## Physical Media:

Information stored on CD/DVD's, USB memory sticks or external hard drives

- Recovery can be faster than cloud-based solutions.
- Data should be stored off-site, never in the same physical location as your equipment.
- You need to consider how much data you'll be backing up as you'll need physical media with enough memory.

If you choose to backup to physical media, make sure this data is encrypted. Some software packages and USB memory sticks may do this automatically.

## Cloud Storage:

Information stored online. You might have to pay for this service depending on how much data you want to store.

- Information automatically backed up by cloud storage software.
- The backup is not stored on-site so reduces risk.
- Data is encrypted.
- All information can easily be recovered from the cloud where your data is stored.

## Dealing with employee cyber security breaches

Employees can do any number of things to cause cyber security breaches and some of them may be criminal acts (e.g. uploading or downloading obscene material, or "hacking" which can be an offence under the Computer Misuse Act, 1990). Some of these acts could also cause damage to third parties (e.g. if confidential information about that person is leaked or personal data is compromised).

You'll obviously hope this doesn't happen but, if it does, there are some legal steps you may need to take. One thing that will definitely help is having a clear policy which employees have to sign up to (whether through an employee handbook or in their contract) and which governs their use of the internet.

Any such policy should include the following points:

- Company computers should never be used to access, download or send offensive and illegal material.
- Opening attachments which have not been checked for viruses is prohibited.
- A list of employee duties in relation to confidentiality and protection of personal data.

When security breaches occur, having a policy in place helps to a) take disciplinary action against the employee and b) helps defend yourself against the activity, as it's possible for employers to be liable for the actions of their employees.



## Definition

### Backup:

A copy of system files or information, which can be recovered later if needed.

### Hosting:

The service that provides the location where your website is stored and maintained.

# Further information

Thank you for reading this guide, which we hope has been a useful starting point to keeping your business safe online. To help you further, we've listed a few recommended websites that can give you more information on cyber security.

**Cyber Street Wise:**

[www.cyberstreetwise.com](http://www.cyberstreetwise.com)

**Get Safe Online:**

[www.getsafeonline.org](http://www.getsafeonline.org)

**Stay Safe Online:**

[www.staysafeonline.org](http://www.staysafeonline.org)

**Action Fraud:**

[www.actionfraud.police.uk](http://www.actionfraud.police.uk)

**Communications-Electronics Security Group (CESG):**

[www.ncsc.gov.uk](http://www.ncsc.gov.uk)

**Future Learn:**

[www.futurelearn.com](http://www.futurelearn.com)

**National Archives:**

[www.nationalarchives.gov.uk/sme](http://www.nationalarchives.gov.uk/sme)

**Safer Internet:**

[www.saferinternet.org.uk](http://www.saferinternet.org.uk)

**ISO 27001:**

[www.iso.org/iso/iso27001](http://www.iso.org/iso/iso27001)

[www.iso27001security.com](http://www.iso27001security.com)



### **The shorter domain for everyone.**

For businesses and individuals. Starting your digital journey or taking your business to the next level. Get on board with your own .uk.

Confident. Entrepreneurial. Distinctive.



### **The original domain for British business.**

One of the most established and popular domains in the world. The .co.uk is a great choice for business and enterprise in the UK.

Established. Commercial. Trusted.



### **For your cause.**

Ideal for charities, fundraising, social causes.

Dependable. Safe. Responsible.



### **When it's all about you.**

Whether you are writing a personal blog, promoting your own portfolio or showcasing your hobbies and talents, this domain is the place to build your own unique online presence.

Personal. Special. Exclusive.

The No.1 British domain name

**theukdomain.uk**