National Cyber Security Centre
a part of GCHQ

CIOB

Cyber security for construction businesses

Cyber security guidance for small-to-medium businesses working in the construction industry and the wider supply chain

Foreword

Sarah Lyons
NCSC Deputy Director Economy & Society Resilience

The National Cyber Security Centre (NCSC) is delighted to partner with the Chartered Institute of Building (CIOB) to produce this guidance to help small-to-medium sized construction businesses protect themselves from cyber attacks.

The NCSC is the UK government's lead for cyber security. Our aim is to make the UK the safest place to live and work online, and to help us achieve this, we work closely with key organisations of all sizes across all sectors, including construction.

Like many other sectors that are embracing new technologies and adopting new digital ways of working, the construction industry continues to be impacted by cyber crime. This document includes clear and concise cyber security guidance that can help you to safeguard your business.

Whilst we cannot guarantee protection against all the cyber threats you face, by implementing the steps described, you'll be protected from most common cyber attacks. And should the worst happen, you should be able to quickly recover.

We're always looking to improve our guidance, so if you have any feedback, good or bad, please get in touch with us using the NCSC website.

Caroline Gumble
Chief Executive of the Chartered Institute of Building (CIOB)

Understanding the role of cyber security within the construction industry is now an essential requirement for organisations of all sizes. Digital assets are commonplace in most businesses (including those in the construction sector), so managing data and digital communications channels is more important than ever.

The consequences of poor cyber security should not be underestimated. They can have a devastating impact on financial margins, the construction programme, business reputation, supply chain relationships, the built asset itself and, worst of all, people's health and wellbeing. Understanding the digital aspects of a business (and then minimising and managing the risks presented) is therefore of prime importance.

Caroline Gumble

Cyber security has been highlighted by the CIOB for some time. Our Digital Technologies & Asset Management Special Interest Group has supported members and the wider industry (with particular reference to supply chains and client relationships) to understand the principles of good security planning, and to encourage the use of design measures to mitigate and manage the potential risks for construction projects. We're now delighted to partner with the National Cyber Security Centre (NCSC) and the Centre for the Protection of National Infrastructure (CPNI) to produce another invaluable resource, the Cyber security for construction businesses guide.

This guide provides a timely opportunity to focus on the risks presented by cyber crime. It's particularly aimed at the small-to-medium sized businesses which make up the majority of construction companies in the UK, and is an accessible resource that can help organisations understand and prevent cyber crime across the sector.

About this guidance

This guidance is aimed at small-to-medium sized businesses working in the construction industry and the wider supply chain (including the manufacture of building supplies, surveying, and the sale of buildings).

- **Section 1** of this guidance is aimed at business owners or managers. This section describes why cyber security matters to the construction industry, and then summarise the cyber threats associated with each stage of the construction process (design, construction and handover).
- **Section 2** provides guidance that can be implemented to make your construction business more resilient against common cyber attacks. The guidance is aimed at staff responsible for IT equipment and services within a construction business. Smaller businesses with no such role may want to start by reading the NCSC's Small Business Guide.

In this guidance

Section 1
For business owners and managers

- Why cyber security matters

  Who is behind cyber attacks?

  Design stage
  Construction stage
  Handover stage

Section 2
For staff responsible for IT

- Cyber security guidance

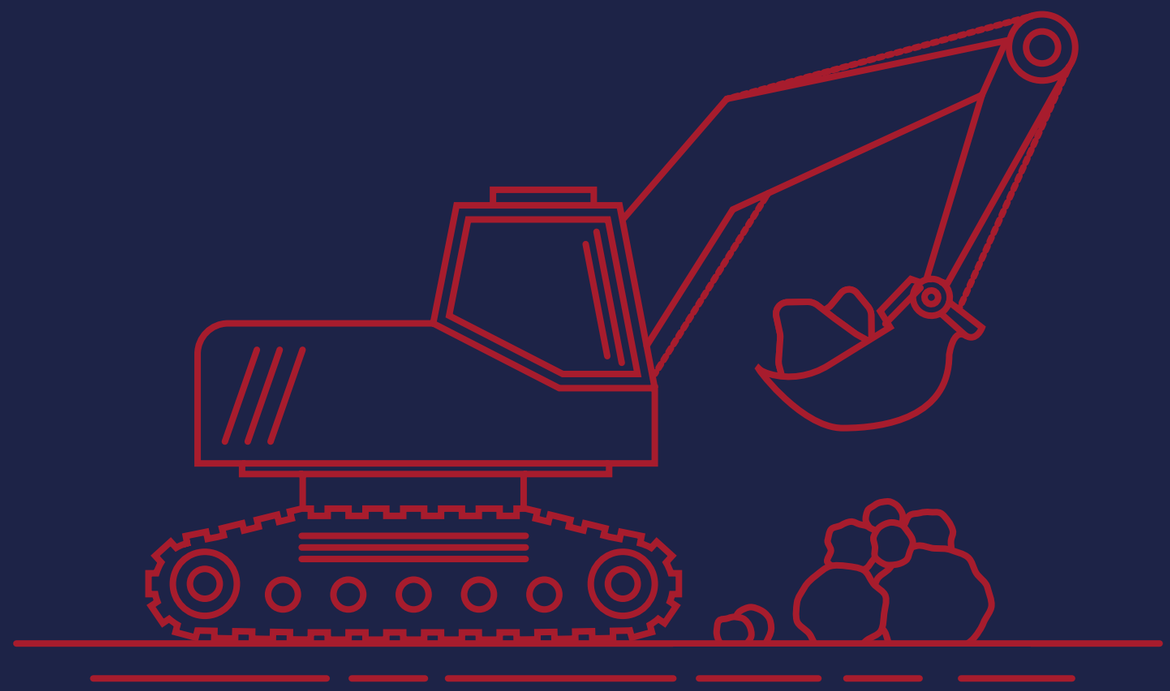
  1. Back up your data
  2. Protecting your office equipment from malware
  3. Keeping your phones and tablets safe
  4. Using passwords to protect your data
  5. Dealing with phishing
  6. Collaborating with suppliers and partners
  7. Preparing for (and responding to) cyber incidents

- Where to go for more help

Section 1

Why cyber security matters

For business owners and managers



Why cyber security matters

Recent high profile cyber attacks against the construction industry illustrate how businesses of all sizes are being targeted by criminals. As the industry continues to embrace and adopt new digital ways of working, it is more important than ever to understand how you might be vulnerable to cyber attacks, and what you can do to protect your business.

Cyber security is about safeguarding the technology we rely on, and protecting the services and information that all businesses, large and small, need to function. The construction industry specifically needs to take the cyber threat seriously for the following reasons:

- Construction businesses are seen by cyber criminals as an easy target, many of which have high cash-flows. Perhaps understandably, smaller and mid-sized businesses have a 'We're only a small business, it won't happen to us' attitude towards cyber security, and are reluctant to invest time, money, and training into what they perceive an unlikely threat.
- The extensive use of sub-contractors and suppliers involving large numbers of high value payments makes construction businesses an attractive target for spear phishing, which is when attackers send a targeted email that's pretending to be from a legitimate organisation, in an attempt to trick the construction business into paying money into a criminal's account.
- Although construction businesses don't store the same kind of financial information a bank does, they still store (and have access to) valuable data. Criminals could be looking for details about the company's next bid (or building design) in order to gain an unfair advantage. Cyber criminals might be looking for sensitive employee data, like national security numbers, bank account numbers and payroll data, in order to engage in identity theft, or to craft realistic authentic-looking emails for phishing attacks.

You may not think it, but regardless of the size and nature of your business, the information that you hold is of value to a criminal. And although they may not target your business directly, it's all too easy to be damaged by phishing emails that cyber criminals send out, indiscriminately, to millions of businesses.

Even if you don't lose money directly, a data breach (which is when information held by an organisation is stolen or accessed without authorisation) or a ransomware attack could cause a temporary shutdown of your business whilst the breach is investigated, and systems are recovered, as well as reputational damage with customers and partners. It could also leave you open to an investigation (and fines) from the Information Commissioner's Office (ICO).

Who is behind cyber attacks?

The construction industry faces numerous groups and individuals that seek to take advantage and do harm, which is why it's so important to secure all digital aspects of your business. You may be targeted by:

Online criminals: they are good at identifying and conducting cyber attacks to make money, for example stealing and selling sensitive data, or holding systems and information to ransom.

Hacktivists: individuals with varying degrees of expertise, often acting in an untargeted way (perhaps to test their own skills or cause disruption for the sake of it). This might include political activists, out to prove a point for political or ideological and environmental reasons, or to expose or discredit your businesses activities.

Malicious insiders: they use their access to businesses data or networks to conduct malicious activity, such as stealing sensitive information to share with competitors.

Nation states: target both public and private sector organisations. Even if you don't think you're large enough to be of interest to foreign governments, you should understand the value you might represent. Perhaps you work with larger organisations (or on government projects) who are their main target.

Why cyber security matters

The three key stages in the construction industry (design, construction and handover) all involve extensive digital workflows, so all of them are at risk.

Everything from the computers, phones and tablets used to access emails, to the essential software used to process and store information, to sophisticated site equipment and digital-based systems installed within buildings. And of course, throughout the entire construction process, you'll need to manage and protect your business information (including client, staff, and project information).

The early stages of the construction process, such as the tender process, will generate for example, detailed quotes and signed contracts. A cyber attack at this stage might prevent a business from being able to win current tenders for work, and impact on future opportunities. By implementing the guidance in this document, your business will be in a more secure and resilient position against cyber attacks. You'll also find it easier to obtain related certifications (such as Cyber Essentials and ISO27001) which can demonstrate a degree of cyber maturity which some government contracts require.

Design stage

Construction stage

Handover stage

Looking after critical documents and data

It's important you have a system in place to receive, track and store electronic and paper-based documents. The system, whether physical or digital (or a combination of the two) should control access to sensitive information, as well as maintaining a 'golden thread' of information (quality and up-to-date information records throughout the asset lifecycle) that is critical to a project or business transaction. This is formerly recommended in the Independent Review of Building Regulations and Fire Safety: Hackitt review.

Having a system in place to keep records of **what** has been shared, **when**, and with **whom** helps prevent sensitive information, such as client or employee details, being accessed by the wrong people. You should also take steps to protect your business so that staff, suppliers, contractors and other third parties only have access to resources required to do their job. This authorisation helps control who has access to your physical and digital assets, and is covered in detail in the NCSC's guidance on Identity and access management.

Engagement and training

At all stages of construction, it is important to ensure that you communicate cyber security requirements with your staff, both on site and at any remote locations. **The importance of - for example - wearing a hard hat, is self explanatory. By contrast, explaining the danger of clicking on links within suspicious emails might be a harder sell, especially within a construction business where the IT function is less prominent.**

Good cyber security takes into account the way people work in practice, and doesn't burden them with processes or procedures that get in the way of getting their jobs done. Supporting your staff to obtain the skills and knowledge required to work securely is often done through the means of awareness or training. If you conduct safety briefings for visitors or staff, use them to provide guidance (including on cyber security) and to raise security awareness.

Staff generally want to do the right thing, but not knowing why they're being asked to do (or not do) something can seem like 'security for its own sake'. Try educating staff on security in a positive way, rather than using fear. Focus on how their actions have a positive effect, rather than the trouble they'll be in if they make a mistake.

To educate employees on cyber security the NCSC has developed an e-learning package 'Top Tips For Staff', which can be completed online.

Why cyber security matters

Design stage

The design stage is the process of developing the project brief so the building can be constructed. Much of this stage is carried out digitally, and you probably use a wide variety of different software tools during the design process, such as:

- computer aided design (CAD) and 3D modelling packages
- collaboration tools for sharing project information
- simulation packages to assist in structural and other specialist engineering disciplines
- general IT systems for storing information and data (either locally or on a business network

It's really important to make sure that the software is always kept up to date. Applying these updates (a process known as patching) is one of the most important things you can do to improve cyber security.

On some projects, you may join or create a Common Data Environment (CDE) with other businesses. These environments include large amounts of project information with access given to third parties. The NCSC's identity and access management guide can help you control who can (and who can't) access your data. You should also implement a 'need to know' process, where access is only granted for the information that is required for that task, and ensure staff are removed when they leave the project or business.

Cyber security risk assessment

A risk assessment is a vital part of any construction project, and this should include cyber security risks (as well as long-established health and safety ones). Conducting a cyber security risk assessment at the outset of the project allows you to identify what cyber security risks your business might face, and to build in precautionary steps you can take.

Cyber security is as much about knowing how your business functions as it is about technology. Think about what people, information, technologies and business processes are critical to your business. What would happen if you no longer had access to them (or if you no longer had control over them)? This basic understanding of **what** you care about, and **why** it is important, should help you to prioritise where to protect your business most.

Cyber security requirements should then be identified and implemented to manage the assessed risks. This includes access to information, access to IT systems and software and access to offices and sites. You should continue to revisit and refresh your assessment as the project develops to ensure that you are continuing to manage risks effectively.

For more information about using risk assessments to improve cyber security, refer to the NCSC's Board Toolkit guidance.

Why cyber security matters

Construction Stage

Compared to the design stage, activities during the construction stage usually require a larger workforce, more materials and equipment, and more interaction with third parties. As the complexity and scale of a project ramps up during construction, businesses will naturally focus on project deliverables and deadlines. It's important that security is not overlooked at this stage of the project.

Securing construction sites and high-tech equipment

The use of high-tech equipment to survey buildings or sites is becoming increasingly common. Drones and GPS equipment can create detailed models and visualisations. The data and information gathered might also include neighbouring assets whether above or below ground.

Equipment can be a target for thieves, both for resale and especially if they store site, project, or sensitive data. While some equipment may not be especially expensive to replace (for example a camera or GPS device), the data stored on them could be very valuable to a cyber attacker. You should secure surveying tools, cameras, tablet computers, lifting equipment and suchlike, to prevent their theft and any data stored on them. CCTV and other security technologies provide significant defence against casual and opportunistic theft.

Consider how IT equipment used on construction sites differs from equipment in the office. For example, the premises themselves may be less secure, or they might be limited/no space to securely house your IT equipment. There may be restricted access to your businesses networks or services. You may even have no (or limited) connection to the internet. All these factors may make it more difficult to access and secure you data. IT equipment left or stored in vehicles or site office can be particularly vulnerable to opportunistic thieves.

You should also consider what personal data is stored on a construction site. For example, details of individuals and their emergency contacts, biometric data, and health and safety incident reports. Remember that this information is personal and covered by data protection legislation and should be protected accordingly. The NCSC provides information on GDPR and what it means for cyber security.

Digital technology and connected systems

If you're involved in any way with the following:

- building management systems (BMS)
- building automation and control systems (BACS)
- building energy management systems (BEMS)
- industrial automation and control systems (IACS)

- then in addition to your regulatory requirements, you'll need to consider the cyber security aspects. This is beyond the scope of this document, so please refer to the following resources:

- 2021 IET Code of Practice for Cyber Security in the Built Environment (sponsored by the NCSC)
- NCSC Connected Places Cyber Security Principles

Why cyber security matters

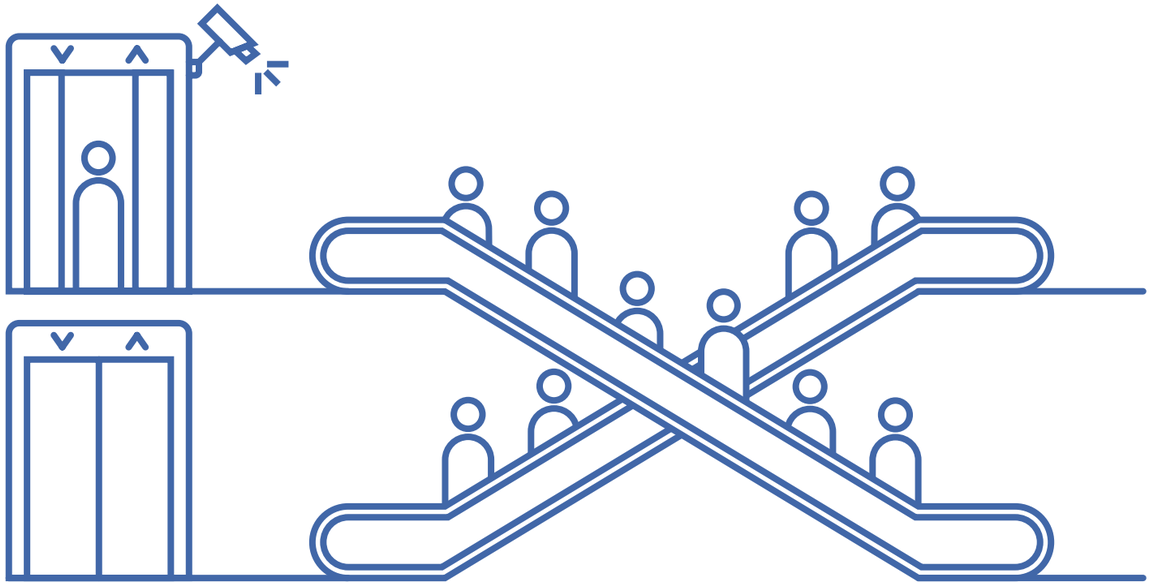
Handover Stage

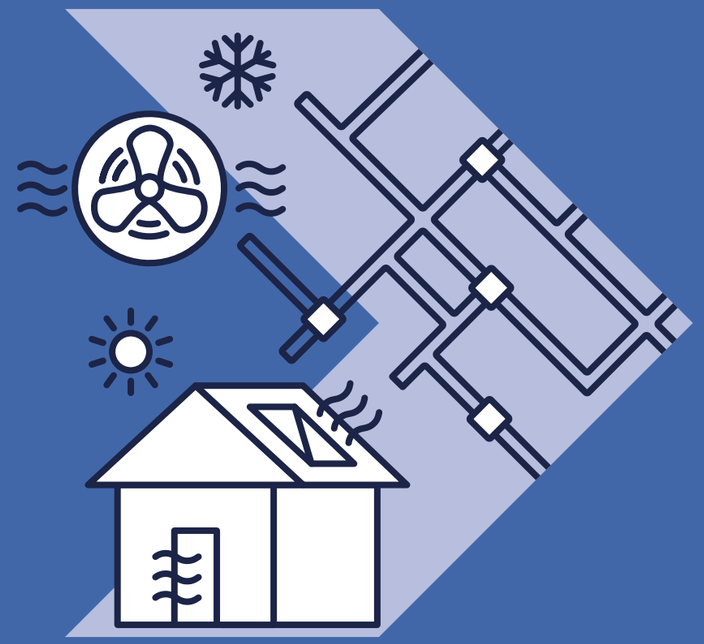
On completion of the project, there may be installed building management systems (for example BMS, BACS, BEMS and IACS). It is important that these systems are handed over to the client so that they can continue to secure the building and any digital-based systems it might contain.

The installed systems will depend on a project's nature and use, but may include combinations of the following:

- lighting automation and control
- heating, ventilation and air conditioning (HVAC)
- fire, smoke detection and alarms
- motion detectors, CCTV, security and access control
- lifts and escalators
- industrial processes or equipment
- shading devices
- energy management and metering

It is extremely important that these are fully documented, and all details of installation, operation and maintenance are included in any handover to the client or building operator. These details should include any steps taken to secure the systems as well as any steps or documentation required to maintain the security of these systems throughout their lifetime. You will likely retain information relating to the project after handover for insurance purposes. For more detailed information refer to the CPNI's guidance on releasing documents.

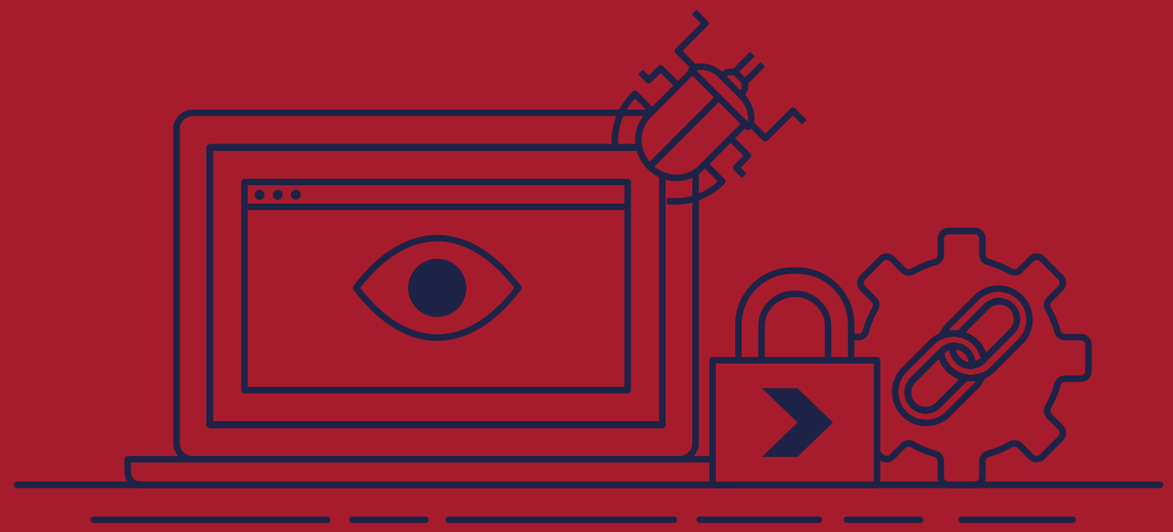




Section 2

Advice & Guidance

For staff responsible for IT



Cyber security guidance

Following the steps described in this section will reduce the likelihood of your construction business being a victim of a cyber attack, and will help you get back on your feet should the worst happen.

01 Back up your data

Think about how much you rely on your business-critical data, such as project plans, CAD models, customer details, quotes, orders, and payment details. Now imagine how long you would be able to operate without them.

It's important to keep a backup copy of this essential information in case something happens to your IT equipment, or your business premises. There could be an accident (such as fire, flood, or loss), you could have equipment stolen, or ransomware (or other malware) could damage, delete, or lock your data.

Identify what you need to back up

Start by identifying your most important information (that is, the information that your business couldn't function without or that you're legally obliged to safeguard). Make a backup copy on a USB stick, an external hard drive, or 'in the cloud'. Having made your backup, make sure you know how to recover the information from it. To get you started, here are some 'how-to' guides for setting up cloud storage:

- Apple (iPhone, iPad and iPod Touch, and Mac)
- Google (Android)
- Microsoft (Windows 10) devices.

Keep your backup separate from your computer

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

- can only be accessed by appropriate staff
- are not permanently connected (either physically or over a network connection) to the device holding the original copy

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 business with cloud-based storage 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.

Before contacting service providers, we encourage you to read the NCSC's Cloud Security Guidance. This guidance will help you decide what to look for when evaluating their services, and what they can offer.

Ransomware often encrypts online backups, which means your cloud-based backups could also be unavailable, leaving you with no backup to recover from. For more resilience, create offline backups, the importance of which is covered in the NCSC blog Offline backups in an online world.

Make backing up part of 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.

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.

For more detailed information about backing up your data, refer to the NCSC's Small Business Guide.

Cyber security guidance

02
Protecting your office equipment from malware

Malware is malicious software, which - if able to run - can cause harm in many ways, including:

- causing a device to become locked or unusable
- stealing, deleting or encrypting data
- taking control of your devices to attack other businesses
- obtaining login details which can be used to access your businesses (or services that you use)
- using services that may cost you money (e.g. premium rate phone calls).

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, it is as easy as clicking 'enable', and you're instantly safer. For phones and tablets, separate antivirus software might not be necessary.

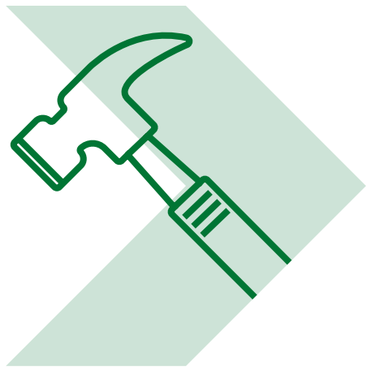
Similarly, you should make sure that your firewall is switched on. Firewalls create a 'buffer zone' between your own network and external networks (such as the Internet). Most popular operating systems now include a firewall, so it may simply be a case of switching this on.

Only download approved 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 unofficial sources, as these will not have been checked.

Keep your IT equipment up to date

Like power tools or machinery, IT equipment (including computers, laptops, tablets and mobile phones) need maintaining and servicing to ensure they work effectively and securely. This maintenance includes updating the software the equipment runs on.
Across all your IT equipment, make sure that the operating system and other installed software is always kept up to date with the latest versions. Applying these updates (a process known as patching) is one of the most important things you can do to improve security. Devices, operating systems and apps should all be set to 'automatically update' wherever this is an option.



As IT equipment reaches the end of its supported life, you should replace it with a supported alternative. If you continue to use equipment that is no longer supported:

- it **won't** receive updates that contain new features and performance improvements
- it **won't** receive the security updates from the manufacturer (and without these your device is easier to hack)

Switch on encryption

Make sure that your office IT equipment - so your laptops and PCs - all use an encryption product (such as Bitlocker on Windows devices, or FileVault for macOS). This means that if even if your computer is lost or stolen, the data stored on it can't be accessed. For advice on configuring disk encryption, please refer to Bitlocker and FileVault guidance.

Control how USB sticks/removable media are used

It's tempting to use USB drives and SD cards to transfer files between businesses and people. However, it's all too easy to plug in an infected stick into a device, only to inadvertently introduce potentially damaging malware into the business.

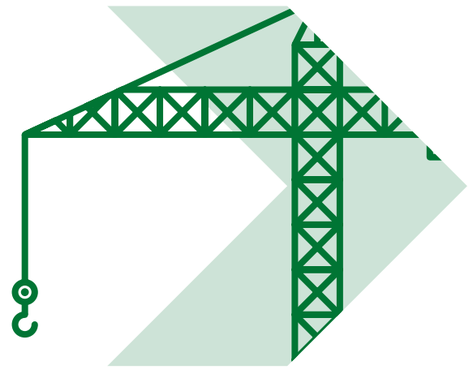
When drives and cards are openly shared, it becomes hard to track what they contain, where they've been, and who has used them. You can reduce the likelihood of infection by:

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

Manage how your IT equipment is accessed by third parties

Organisations and individuals outside your business may have legitimate reasons to access your IT equipment. Perhaps a service provider or consultant provides your business with IT (or construction-related) services.
You need to understand how this access is granted and monitored, and ensure that third parties only have access to what is required to carry out their work. Left unmanaged (or set up incorrectly), criminals can exploit this 'remote access' to carry out cyber attacks, or steal information.

For more detailed information about protecting your business from malware, refer to the NCSC's Small Business Guide.



Cyber security guidance

03 Keeping your phones and tablets safe

Mobile technology is now an essential part of a construction business, with more and more being used on construction sites and on the move, storing increasing amounts of important data. 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.

Don't leave your phone (or tablet unlocked

Set a screenlock password, PIN, or other locking method (such as fingerprint or face unlock). As we explain in step 4, avoid using the most common passwords (such as '*password*').

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 on site. 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

Keep devices and apps up to date

As with office-based equipment, it is important to keep phones and tablets up to date at all times. All manufacturers release regular security updates to keep the device protected. This process is quick, easy, and free; devices should be set to automatically update, where possible.

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.

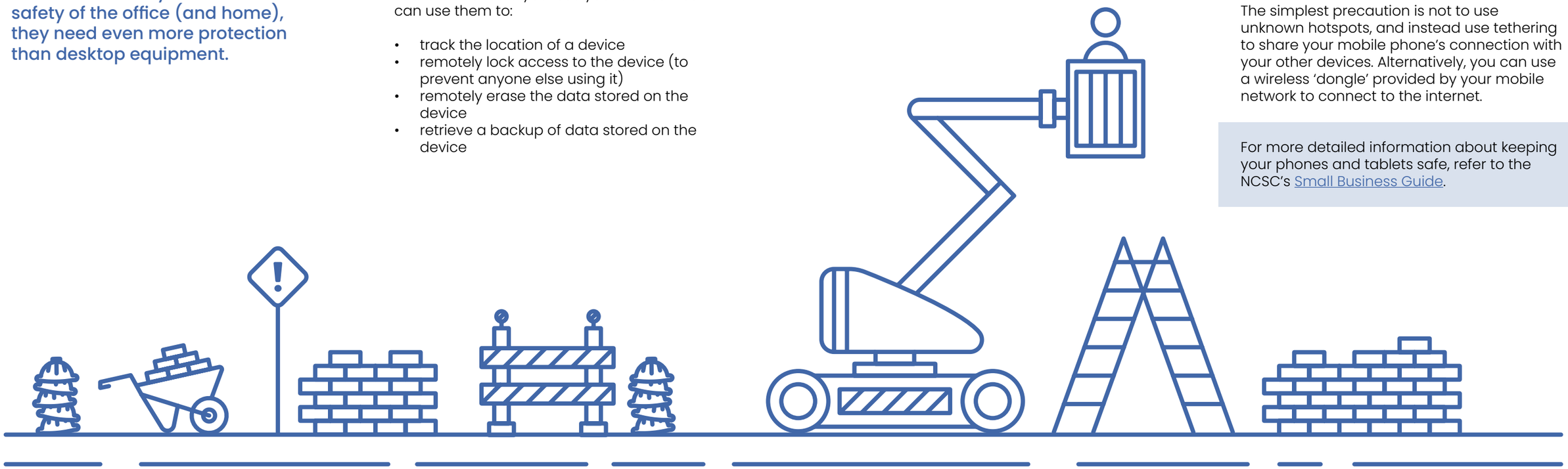
Take care when connecting to public Wi-Fi hotspots

When you use public Wi-Fi hotspots (for example in hotels or coffee shops), make sure that you're connecting to a legitimate service; a member of staff will be able to confirm the name of the service to use. If you connect to a 'rogue hotspot' (that is, a Wi-Fi hot spot set up by a cyber criminal), they 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 not to use unknown hotspots, and instead use tethering to share your mobile phone's connection with your other devices. Alternatively, you can use a wireless 'dongle' provided by your mobile network to connect to the internet.

For more detailed information about keeping your phones and tablets safe, refer to the NCSC's Small Business Guide.



Cyber security guidance

04
Using passwords to protect your data

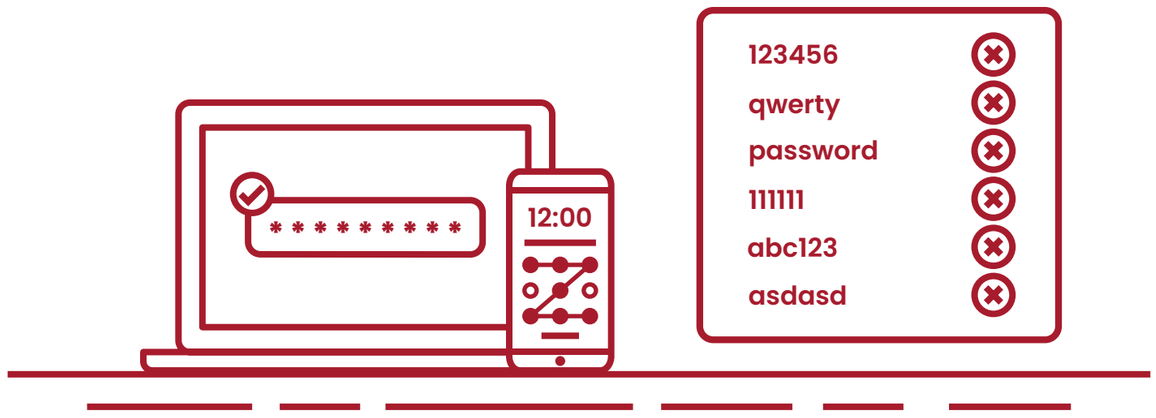
Your laptops, computers, tablets and phones will contain a lot of your own business-critical data, the personal information of your customers, contractors, suppliers, and also details of the online accounts that you access. Passwords - when implemented correctly - are a free, easy and usually effective way to prevent unauthorised people accessing your devices. The NCSC has some useful advice on how to choose a non-predictable password that you can remember.

Remember to switch on password protection

Set a screenlock password, PIN, or other locking method (such as fingerprint or face unlock). Most devices will require you to set up a password when you use them for the first time, but it may have been switched off by somebody else.

Avoid using predictable passwords

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 (such as '*password*'), which criminals use to brute force access to your account, or ones that someone could guess from your social media profile (so avoid using family names, pet's name, place of birth, or something related to a favourite sports team).



It's really important not to re-use the same password for your different online accounts. In particular, use a strong and separate password for your email. If a hacker can access your mailbox, they could access information about your payments, invoices, contractors and suppliers), as well as send emails pretending to be from you.

Use 2FA for important accounts

If you're given the option to use two-factor authentication (also known as 2FA) for any accounts you should, and especially for **email**, **banking** and **purchasing**. This 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 something you *know* (like a password) and something you *have* (like a phone). This could be a code that's sent to your phone (or a code that's generated from a bank's card reader) that you must enter in addition to your password.

Looking after your passwords

Of course most of us have *lots* of online accounts, so creating different passwords for all of them (and remembering them) is difficult. However, to make this easier, you can:

1. Write all your passwords on a piece of paper and keep it somewhere safe (and **away** from your computer).

2. Let your browser save your passwords for you - **it's safe for you to save them when you're asked**, (although if you share your computer with anyone, they'll also be able to access the accounts).

You can also use a password manager, which can create and store passwords for you that you access via a 'master' password.

If more than one person is accessing a computer, you should ideally have different accounts, and different passwords for each person. Where this isn't possible, make sure you know **who** has access to your devices, who knows the password, and that you're OK with this. Don't write the password on a Post-it that's stuck to the computer, for anyone to use. For the same reasons, lock your device when you're not at your desk, and make sure you change your passwords when a member of staff with access to your devices leaves.

Change all default passwords

Finally, one of the most common mistakes is not changing the manufacturers' default passwords that phones, laptops, and other types of equipment are issued with. These can be easily found online. Change all default passwords before devices are distributed to staff.

For more detailed information about using passwords to protect your data and devices, refer to the NCSC's Small Business Guide.

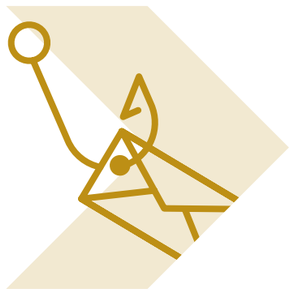
Cyber security guidance

05
Dealing with phishing

'Phishing' is when criminals use scam emails, SMS or chat messages, phone calls or social media to trick their victims.

Their goal is often to convince you to click a link, or open an attachment. Once clicked (or opened), malware may be installed via a dodgy website you have been sent to, or via the attachment you have opened. Over the phone, the approach may be more direct, asking you for sensitive information, such as banking details.

Some criminals may even send a more *targeted* scam message (a process known as spear phishing), which pretend to be from a legitimate company you deal with. These more targeted attacks appear to be from more legitimate sources, and are sent to senior staff or budget holders within larger businesses, who may have access to finances and more valuable information. Unlike standard phishing messages that are sent out indiscriminately to millions of people, spear-phishing attacks are crafted to appeal to specific individuals, and can be even harder to detect. Phishing (and spear-phishing) is a threat to all businesses of all sizes and across all sectors, including construction.



Reporting scam emails, texts, websites to the NCSC

If you or a member of staff have received an email you are not quite sure about, forward it to NCSC's Suspicious Email Reporting Service (SERS) at report@phishing.gov.uk Suspicious text messages should be forwarded to 7726 – it is free of charge.

Make yourself a harder target

Information about you that's easily viewed on your work and private websites (including social media accounts) can be used by criminals to make their phishing messages appear more convincing. Review your privacy settings, and think about what you post across your social and professional accounts. 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.

Think about how you operate

Consider ways that someone might target your business, and make sure your staff all understand normal ways of working (especially regarding interaction with other businesses), so that they're better equipped to spot requests that are out of the ordinary. Common tricks in construction include tricking staff into transferring money or information by sending emails that look authentic. Another is to send an invoice for a service that you haven't used, so when the attachment is opened, malware is automatically installed (without your knowledge) onto the computer.

Think about your usual working 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.
- 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.

Check for the obvious signs of phishing

Scammers hope to quickly gain your trust and persuade or pressure you into acting without thinking. Scam messages will often have one or more of the following 5 tell-tale signs.

1. **Authority** - Is the message claiming to be from someone official or an organisation you work closely with? For example, your bank, clients, suppliers, or a local authority. Criminals often pretend to be important people or organisations to trick you into doing what they want.

2. **Urgency** - Are you told you have a limited time to respond (such as 'within 24 hours' or 'immediately')? Criminals often threaten you with fines or other negative consequences.

3. **Emotion** - Does the message have a tone that can make employees feel panicked, fearful, hopeful or curious? Criminals often use threatening language, make false claims of support, or tease you into wanting to find out more.

4. **Scarcity** - Is the message offering something in short supply, like materials, tools or software? Fear of missing out on a good deal or opportunity can make people respond quickly.

5. **Current events** - Are you expecting to see a message like this? Criminals often exploit your relationships with clients and suppliers to trick you into paying sums of money and also make use of specific times of year (like tax reporting) to make their scam seem more relevant to you.

What to do if you've already clicked

If you've lost money or have been hacked as a result of responding to a phishing message, you should report it:

- In England, Wales or Northern Ireland, visit www.actionfraud.police.uk or call **0300 123 2040**.
- In Scotland, report to Police Scotland by calling **101**.
- Your bank may also be able to help if you think you've been tricked into transferring money to a criminal.

Cyber security guidance

06 Collaborating with suppliers and partners

Construction businesses rely upon suppliers to deliver materials, machinery, labour, and digital information (such as specifications and designs). Even for smaller businesses, your supply chain can quickly become large and complex, involving extensive use of sub-contractors and suppliers with a high degree of payments flowing to and from businesses.

Then there's the less-obvious organisations that you rely on. For example the provider of your email service, or the company behind the accounting software you use.

Cyber attacks on your suppliers can be just as damaging as an attack on your own business. This is why it's important to employ cyber security when collaborating with suppliers and partners. You may be targeted as a way into the organisation you are supplying. This is very common in the construction industry, as you might already be working with organisations that the attacker wants to access through you.

Conversely, your suppliers may be targeted as a route into your business. Or you may be sharing sensitive or valuable information that you want suppliers to protect.

Construction businesses may also want to encourage their suppliers to get Cyber Essentials certification. Cyber Essentials is a government-backed, industry supported scheme to help organisations protect themselves against common cyber attacks. Organisations with Cyber Essentials certification have demonstrated that they take cyber security seriously, and can use this reassurance to attract new business and reassure their customers.

Understanding your supply chain

Until you have a clear picture of your existing supply chain, it will be very hard to determine how to secure it. Ensure you have a list of all your suppliers, and partners, and identify which ones are highest priority (in terms of risk) to concentrate your efforts on. Where possible include subcontractors beginning with your highest priority direct suppliers.

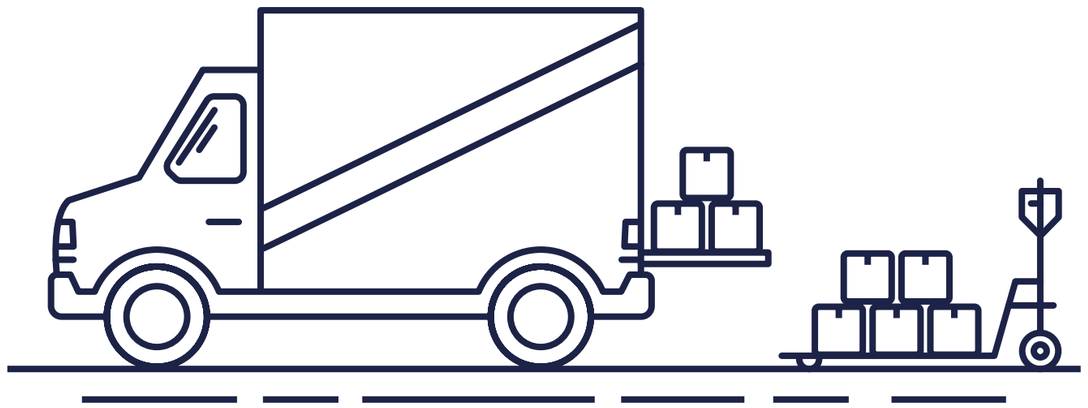
Look for information published by your existing suppliers that help you understand how they provide services securely. Ensure you understand the terms and conditions in your contract or licensing agreement, and what parts of security each are responsible for. This will help you to develop a common understanding of each party's security responsibilities, and what subcontracting decisions you are happy to delegate to them. It might be useful to include references to the following NCSC guidance that can help to establish a baseline of cyber security:

- 10 Steps to Cyber Security
- Small Business Guidance
- Cyber Essentials

Consider the implications if your supplier is attacked

No matter how good your own cyber security is, you should assume that you and your partners **will** experience a cyber incident at some point, and plan for this accordingly. This is also worth considering in your security agreements; what are you expecting of them and their response? Do they have to notify you? Do they have to assist you if you are consequently also attacked?

For more detailed information about collaborating with suppliers and partners, please to the supply chain section of the NCSC's Board Toolkit guidance.



Cyber security guidance

07
Preparing for (and responding to) cyber incidents

When something unexpected happens, such as a cyber incident, it can be difficult to know how to react. Naturally, you will want to resolve the problem as quickly as possible so you can resume business quickly. Malware (and especially ransomware) is becoming increasingly common in the construction industry, so it's essential to be prepared.

It's impractical to develop detailed step-by-step instructions to manage every type of incident, as the list could be endless. Instead you should prepare plans to handle those incidents most likely to occur.

The best way to test your staff's understanding of what's required during an incident is through cyber exercising, which involves rehearsing your response to a cyber incident. Consider using the NCSC's Exercise in a Box product, which is especially designed for smaller organisations, to test your business resilience and preparedness.

Prepare for incidents

Identify what **electronic information** is essential to keep your business running, such as contactor and supplier details, emails, invoices, and essential documents. Find out where this information is stored. Is it on single machine in your office? Is it on a remote server? Is it stored in the cloud, or by a third party?

Make sure you keep the important information you identified above in a safe place so that you can use it if your equipment is stolen or damaged by a cyber attack. Ensure you know how to restore a backup in the event of any type of data loss, such as a ransomware attack, and train the relevant people in your business so they can do the same. Being prepared and having relevant documents that are up to date and also **accessible** when an incident occurs could make all the difference.

If you have cyber insurance, have your insurer's details documented including policy number and any specific information your provider asks for. Understand any legal or regulatory compliance you must adhere to and implement any guidelines/policies/rules they set out for you. You should check if your trade association or professional body has any help or advice lines that you can contact to help you in this situation.

Identify if you're being attacked

The first step in dealing effectively with a cyber incident involves identifying it. That is, how can you detect that an incident has occurred (or is still happening)?

Things that might indicate a cyber incident include:

- messages demanding a ransom for the release of your files
- computers running slowly
- users being locked out of their accounts
- users being unable to access documents
- people informing you that they've received unusual emails from you
- redirected internet searches
- requests for unauthorised payments
- unusual account activity

To help with this, you can use the NCSC's Logging Made Easy tool, which has been specifically designed to help small businesses who lack the budget, time or understanding to set up their own logging system.

Your antivirus software can also provide you with indicators of compromise; complete a full scan and analyse the results to see if it has detected any malware. Advice about what to do is usually available on the antivirus company's website

(continued on next page)

Cyber security guidance

Resolve the incident

The actions in this step will help your business get back up-and-running as soon as possible. You'll also need to confirm that everything is functioning normally, and fix any problems.

If your IT is managed externally, contact the right people to help. These contacts are there to fix the problem and establish the impact to your business.

If you manage your own IT, put the plans you made earlier into action. Depending on the type of incident you are responding to, this may involve:

- replacing compromised hardware
- restoring services through backups
- patching software
- cleaning infected machines
- changing passwords

You could use a company in the NCSC's Cyber Incident Response (CIR) scheme if your organisation was the victim of a significant cyber attack. The CIR-certified company would conduct all the cyber incident response activities in relation to the attack to help your organisation recover.

Note that you're legally obliged to report certain incidents (such as a data breach) to the Information Commissioner's Office (ICO), regardless of whether your IT is outsourced. Check the ICO website to find out which incidents require this. Other regulatory bodies which you belong to may also require you to report a breach.

Learn from the incident

After the incident, it's important to review what has happened, learn from any mistakes, take action to try and reduce the likelihood of it happening again. To do this:

1. Review actions taken during your response. Make a list of things that went well and things that could be improved from the response stage.

2. Review and update your incident plan, and where necessary, make changes to the incident plan you created, to reflect the lessons learnt.

3. Strengthen your defences by making any necessary changes.

For example, if you were a victim of a password attack, you may need to create a new password policy.

For more detailed information about preparing for incidents, refer to the NCSC's Small Business Guide to Response & Recovery.

Where to go for more help

If you receive a potential phishing message, you can report it to the NCSC using the Suspicious Email Reporting Service (SERS). Just forward the message to report@phishing.gov.uk. If the message is found to link to malicious content, it will be taken down or blocked, helping prevent future victims of crime.

Suspicious text messages should be forwarded to 7726. This free-of-charge short code enables your provider to investigate the origin of the text and to take action, if it is found to be malicious.

If your business suffers a cyber incident or is affected by fraud (e.g. money lost a result of a phishing email or your IT systems are compromised), report it to Action Fraud by calling 0300 123 2040 or go to www.actionfraud.police.uk, or in Scotland through Police Scotland's 101 call centre.

If you are looking for advice on the security of built assets and the public realm, members of the CPNI sponsored Register of Security Engineers and Specialists (RSES) can provide specific advice or guidance, including the security of digital systems in the built environment.

If you want more information and advice on physical or personnel security issues or security-mindedness, including risk assessment, site security, accredited security products and information management, please refer to the CPNI website at www.cpni.gov.uk.

National Cyber Security Centre
a part of GCHQ

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 - **January 2022**

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