While there are many ways to reduce the risk of theft and attacks, it is always best to sit on the side of caution during the current Covid-19 lockdown. This means it is important to consider ways to minimise the effect of criminal activity. While the country is in locked down criminals are active and will continue to target the vulnerable. I hope this document provides you with some comfort in mitigating the potential risk.

Property maintenance

You should check your premises regularly, at least once a week, to see if there are any obvious signs of an attempted break-in or damage. It is important that premises continue to be well-maintained during this extended period of closure to prevent the spiral of decline. This includes removing litter and graffiti as soon as possible and making sure that landscaping is cut back to assist with surveillance from passers-by and your CCTV system. Flammable and combustible materials and substances should be stored in a secure, lockable container, cage, or room. Bins should be securely stored away from the building to prevent arson.

Monitored intruder alarm

Monitored intruder alarm system A monitored intruder alarm system is a deterrent to burglary as it increases the likelihood of being caught. Make sure it is regularly maintained, in good working order and is remotely monitored for a police response by a National Police Chiefs' Council Compliant Alarm Receiving Centre (ARC). Ensure that staff are familiar with opening and closing procedures to prevent false alarm activations. Update your key holder list and share it with third parties, where necessary, e.g. your intruder alarm company. Security alarms which detect forced entry or movement within your property can work very effectively, particularly if they are connected to a security service who can take action and attend your property during a breach on your behalf. However, these systems are only as good as the person who maintains them. Before travelling or locking down, always ensure that all security alarms are in good working order and, if possible, test them for peace of mind. Also be sure to test fire and gas alarms before vacating the property, too.

Security fogging system

A security fogging system is triggered by an alarm sensor and will instantly fill the area you are trying to protect with a dense, harmless fog that reduces visibility, making it virtually impossible for an intruder to access the items they want to steal. If you already have such a system, check with your supplier that it is still in good working order and or test remotely.

CCTV

CCTV If you have CCTV, make sure it is regularly maintained, in good working order with sufficient storage capacity and as a minimum, is providing coverage of the most vulnerable areas, including doors and windows where access is likely to be gained. The recording equipment should be kept in a secure cabinet inside a lockable room within the building. All CCTV should comply with the Information Commissioner's Office guidance, see www.ico.org.uk. For a temporary solution why arrange for your CCTV to be monitored off site by an approved Security Partner.

Doors and windows

Doors and windows Doors and easily accessible windows should be in good working order, free from rot or damage and have good quality locks that have a Kitemark showing that they meet the relevant British Standard. There are various types of doors and windows, e.g. U-PVC, aluminium, timber, etc. and these may have multi-point or single-point locking mechanisms. All external doors should have a minimum of two locking points with locks that meet the British Standard. All doors and windows that are not part of a designated fire escape route, should be closed and locked. It is not just doors and windows that can provide easy entry and exit points to your property. Before leaving on your travels, be sure to consider any other point which could be a vulnerability or weakness. This could include rooms of your home which have their own separate entrance, such as a garage or guest house. Also think about any outbuildings you may have, such as sheds or pool houses, which may contain valuable items and prove to be high target areas for potential criminals operating in your area.

Although it is essential to lock all external doors and windows before vacating your property, it can also be a good idea to lock internal doors, particularly doors that are located in high-value areas of the home. Reports show that rooms located on the second storey of a property are typically most likely to be targeted as these rooms are often bedrooms and studies that contain small, valuable items. By restricting access to these parts of the home, you could reduce the impact of a security breach.

Glazing All easily accessible glazing should be laminated to resist forced entry. Double glazed units only require either the inner or outer pane to be laminated. Alternatively, security film can be applied to the internal glazed panel, ensuring it is fixed under the beading, where possible.

Roller shutters and grilles Roller shutters and grilles can provide additional protection to external doors and windows in vulnerable areas around your business premises. They are particularly useful for protecting recessed doors that create hiding places because they are set back from the building line. If you have roller shutters or grilles fitted, use them.

Lighting

Lighting The need for external lighting will be determined by local circumstances and the quality of street lighting in the area, e.g. inner city, rural, adopted, non-adopted areas, etc. Internal lighting should be operated by detection devices which will automatically switch lights on where movement is detected. Check that all lights are in good working order. Before leaving, set up the lights to turn on and off throughout the evening. Some systems also allow you to control this using a smartphone or tablet and the wifi plugin adaptors are easily purchased through Amazon.

Safe storage

Safe storage of valuables, assets and stock Valuables, assets and stock should be either removed from the premises or stored in a secure, lockable container, cage or room or even off site and the keys stored in a secure key cabinet or removed entirely. It is advisable to check the continued performance of essential equipment and services, such as fridge freezers, electrical and water supplies, including central heating pipework.

Gaming and vending machines

Gaming and vending machines Gaming and vending machines should be emptied of all stock and cash with visible external facing signage displayed to advertise this fact and deter a potential intruder.

Arrange for Security Mobile Patrols

Whilst in locked down, and how long you are planning to be away for, you may wish to arrange of regular maintenance of your common areas and front of house to give the illusion of the property being occupied. Unmown grass and overgrown weeds can suggest that the homeowners and business owners are not present. You may wish to employ a Professional Security Partner that carries out random Security Mobile Patrols.

Check Business Insurance

Although business insurance cannot directly keep your property safe and secure while you are travelling or locking down, a good and valid policy can help to reduce the impact of a breach should the worst happen. In the unlikely and unfortunate event that a property crime does take place while you are travelling or in lockdown, you may be able to recover some of the financial loss through your insurer to minimise recovery time. Always be sure to not only check your contents insurance but also building insurance to cover any damage during entry/exit.

Cyber Security Tips for Working at Home

Strong password policy Use a strong password for all devices and social media accounts. Change default passwords on all your devices when initially installed (especially your Wi-Fi router at home or any Internet of Things devices you may have) and consider using password managers to store and protect your passwords.

Turn on the two-factor authentication setting on all your accounts and devices

VPN Use a Virtual Private Network (VPN) to protect and encrypt the data you send or receive. It will also scan devices for malicious software.

Software update Set all your devices and apps to download and install updates automatically to ensure that any crucial fixes are not missed, and the risk of your devices being infected with malware is reduced.

Back up to safeguard your most important personal data and information, back them up to an external hard drive or cloud-based storage system

Cyber criminals are targeting people and businesses with fake emails about the coronavirus. Phishing emails may appear genuine but are embedded with a virus that could compromise your device, as well as manipulate you into sharing personal or financial information.

Install anti-virus Install and activate anti-virus software on all your devices, preferably set it to update automatically. This will help you to run a complete scan of your system and check for any malware infections.

Safe online browsing Only visit trusted websites especially when online shopping. Keep an eye out for websites that have a padlock sign in the address bar, as this shows that the connection and your personal information (e.g. credit card information) is encrypted and secure

Social media It is important to review the privacy, password, and security settings for all your social media accounts to ensure they are as secure as possible.

Communication Maintain contact with your team and family members, as it is easy to feel isolated or lose focus when working at home.

Fraud

The impact of business fraud can be dramatic, particularly for small or medium-sized enterprises (SMEs), where the losses can ruin them. It is important to understand what the threats are and where they come from so you can take action against them. Find out about the common types of business fraud and what steps you can take to protect yourself, your staff, and your business.

Business fraud and how to prevent it

Business fraud is simply the intent or the act of misrepresentation – scammers lying about themselves or their actions and services – to cause a gain or loss.

With limited resources and in tough economic conditions, small and medium-sized enterprises (SMEs) tend to think more about innovation, growth, and survival rather than due diligence, internet controls and risk management. These can often seem expensive, hard work and involve a lot of paperwork.

But this approach leaves SMEs particularly vulnerable to fraud, with many owners and managers unaware of the risks their businesses face.

It is important to recognise that a fraud can come from anywhere, including:

- staff members
- customers
- suppliers
- third parties, unconnected to the business.

From the start, fraud can seem complicated and difficult to understand, as criminals use a variety of tools and techniques.

We cannot provide a single solution to prevent all business fraud, but the information below will help you identify the most common types and take action to protect yourself, your staff, and your business.

Ten tips to prevent business fraud

Remember these ten simple tips to reduce the risk of business fraud and keep your business and staff safe.

1. Be sceptical

If it sounds too good to be true, it probably is. Thoroughly question all:

- Deals
- Opportunities
- Documents
- Transactions
- Information

2. Know your business inside out

Have a thorough understanding of your business so you know:

- how it operates
- the staff you employ
- the products and services it provides
- your target market and your business
- your legal and regulatory obligations

This will help you realise immediately when something is not right.

3. Know your customers and suppliers

When you understand who you do business with you can spot any business request or transaction that looks wrong for that customer or supplier and may be fraudulent.

Conduct due diligence using a risk-based approach, such as checking the customer or supplier details you have on file, as well as online searches.

4. Identify areas where your business is vulnerable to fraud

Imagine how a fraudster might target your business, both internally and externally, and test the systems you already use to reduce risk. Make sure you and your staff know those systems and regularly review them.

5. Develop a strategy and talk about fraud

Think about the right fraud prevention and detection strategy for your business: it should detail controls and procedures.

Staff look to owners and managers for guidance to acceptable behaviour. Talk about fraud with your staff, suppliers, and other contacts. Your staff need to understand the risks and how losses affect the business and themselves.

6. Take extra care against cyber attacks

With increasing threats from cybercrime, protect your business technology against attacks. Make sure you back up your systems in case they go wrong.

7. Understand your finances

Understand how money leaves your business, including:

- Methods of payment
- Who has authority to make those payments?
- Who checks payments are legitimate?
- Always check your bank statements.

8. Secure and protect your property

This includes laptops, computers, smartphones, and intellectual property. Factor in business insurance to cover these items if they are compromised or stolen. Use and maintain inventories.

9. Develop an action plan

Consider when you might need professional or legal advice. While prevention is better than cure, it is important for you and your business to be prepared for the worst. Having an action plan in place will help limit your losses to fraud.

10. Always report fraud and get help

Action FraudExternal Link is the UK's national fraud and cybercrime reporting centre. You can also get information about fraud and financially motivated internet crime.

You can also report fraud to the police if you know the suspect or they are still in the area. Call 101 to speak to one of our operators. If you are deaf or hard of hearing, use our textphone service on 18001 101.

E-commerce fraud: credit card and online data theft

Fraudsters use stolen credit card details to target online retailers. Online business appeals to them because there is no physical contact with the business or the legitimate cardholder.

Make sure you are fully aware of the risks, otherwise your business is more likely to be targeted.

What you should know

When payments are accepted over the internet and processed, your business asks for authorisation from the card issuer. But even this does not confirm or authenticate the customer as the genuine cardholder. The standard authorisation only confirms that:

- the card has not been reported lost or stolen
- there is enough money in the account
- the card number is valid

If it turns out to be a fraudulent sale and your company did not get authorisation from the issuer, the full amount may be charged back to your business if the genuine cardholder says they were not part of the transaction.

It is important to maintain chargeback records. Get as much information as possible and give it to your acquirer. If you suspect a fraudulent transaction report it to your authorisation centre.

Businesses are responsible for protecting cardholder data at the point of sale and as it flows into the payment system. Get more information at PCI Security Standards External Link.

Minimise your risk to ecommerce fraud

Consider using:

- card security code (CSC)External Link
- MasterCard SecureCodeExternal Link
- Verified by VisaExternal Link

Treat high-value items and overseas transactions with extra caution. Always verify the delivery address. If it is overseas ask a third-party service to give you the details.

Watch out for changes to the details they gave you, a change to the delivery address, for example. Insist that you will only deliver to the customer's permanent address.

If you use a courier, tell them to:

- Only deliver to the address you give them
- Return the item if they cannot deliver it
- Always get signed proof of delivery

Make sure you store your customers' card payment information securely. This data is prone to hacking, so comply with data security requirements.

Keep records of any fraudulent activity: it is a good way to find patterns and areas of potential risk. Many businesses use this process to predict higher-risk transactions.

For more information and help or to report this and many other types of fraud, go to Action FraudExternal Link, the UK's national fraud and cybercrime reporting centre.

Online fraud

As the number of channels and markets we operate in rises, so does the risk of fraud. Cybercrime is more sophisticated, and fraud is increasingly difficult to detect. As a result, the standard fraud verification tools may not be good enough.

What you should know

Fraudsters may target your online business to get customer information, such as names, addresses and payment details, to commit crime.

When using public Wi-Fi networks, many do not secure their connection when they send personal and business emails, banking, or credit card details. These networks are open to hacking, identity theft and fraud. Lots of simple tools and free apps can hack public Wi-Fi networks, a process called 'sniffing'.

Employees can be targeted by 'spear phishing', when a fraudster sends an email to a particular person. They pose as someone else within the company, usually someone important or in a position of trust, and ask for information like login IDs and passwords. They may ask the employee to update their username and passwords.

Once the fraudster has this information, they can access your secured networks to get confidential information and customer data.

Other methods include asking the employee to click on a link in the email, which deploys malware that takes personal or confidential data from your business.

Be wary of where you store your information. If you use a third-party hosting company, find out:

- Where your information is kept
- How it is shared
- How it is stored

A recent computer threat to businesses is called Cryptolocker, ransomware that is usually disguised within a legitimate-looking email attachment.

When the attachment is opened, the malware encrypts files in your computer. You then get a message asking for money to decrypt the data, usually via bitcoin or pre-paid vouchers.

There's not much you can do in this situation, which is why you must back up your data on a regular basis.

Minimise your risk to online fraud

It is essential that you back up data; if you do not, it may have a huge effect on your business.

Make your passwords robust by using a mixture of upper- and lower-case letters, numbers, and symbols.

Do not use obvious passwords, like your mother's maiden name, as fraudsters can easily get this information.

Challenge anyone who asks for your personal or financial details.

Test all your security systems to make sure they are working, and you are not vulnerable to invasion. This includes your website.

If your bank offers it, consider using dual authentication. This can reduce your fraud risk from malware and insider threats.

Visit Cyber AwareExternal Link for step-by-step instructions on keeping your devices up-to-date with the latest security updates, and for further online security advice.

For more information and help or to report this and many other types of fraud, go to Action FraudExternal Link, the UK's national fraud and cybercrime reporting centre.

Phone Frauds

If fraudsters hack into your business phone lines, they can get personal or confidential information. Make sure you have the right security systems to protect you.

Phone and videoconference hacking

Some businesses regularly use conference or video calls to talk to other businesses. But fraudsters can access them and overhear conversations to get passwords and codes.

Private automated branch exchange (PABX) hacking

Call centres and other businesses and organisations use private automated branch exchange (PABX) phone networks. A PABX is a single-access number with multiple lines to outside callers, which also gives external callers or staff a range of external lines.

Fraudsters use vulnerabilities to:

- hack your system
- access passwords
- listen in to conversations and voicemails

They also use your PABX system to make international or long-distance calls, often to premium rate numbers that the fraudster has set up. Your business unknowingly lets the fraudster sell on the access and use of your system, which could increase your phone bills by thousands of pounds.

Remember, your business is responsible for any fraudulent use of your system, not the phone provider.

These frauds often occur over the weekend or bank holidays where staff are out of the office for long periods: it gives fraudsters the chance to rack up huge bills on behalf of your company.

Take steps to avoid vishing

'Vishing' is the phone equivalent of phishingExternal Link. Criminals call you, pretending to be from a legitimate business, and persuade you to give them private information that they use to make money.

Be wary of cold callers who suggest you hang up the phone and call them back to check they are genuine. Fraudsters can keep your phone line open by not putting down the receiver at their end.

Unless you are absolutely sure who you are talking to, never give your company's:

- Payment card PIN
- Passwords
- Online banking codes
- Financial details

Your bank, the police or a legitimate organisation will never:

- Ask for your PIN
- Ask you to withdraw money to hand over to them
- Ask you to transfer money to another account, even if they say it is in your company's name
- Come to your building to collect your business account card or cheque book

Remember to wait at least five minutes after a potentially fraudulent phone call before using that phone again, as the person may have left the line open.

If you are unsure about providing information a caller asks for, check company policy on what you can and cannot disclose.

If you are suspicious or feel pressured or vulnerable, do not be afraid to say no to any requests for information and end the call.

Criminals may already have basic information about your organisation, such as the name, address, and account details. Even if a caller has this information, do not assume they are genuine.

Minimise your risk of phone fraud

Make sure you know your business systems so you can detect suspicious activity.

Keep your systems in a secure place. If you have a multiple-occupancy office, you should use locked areas.

Always use strong passwords, manage access to them and never use default password settings.

Consider using settings that restrict international or long-distance calls. You can also ask your phone provider for this restriction.

If you are using Skype, Zoom, Teams or something similar to videoconference, use up-to-date antivirus and firewalls. This will also help protect you from PABX hacking.

Always keep your software up to date, especially if you are using PABX.

Make sure you know your business call patterns and consider monitoring them, especially if there are calls out of hours, weekends, and bank holidays.

For more information and help or to report this and many other types of fraud, go to Action FraudExternal Link, the UK's national fraud and cybercrime reporting centre.

Little Book of Big Scams: Business Edition

Personal Safety

General Personal safety

- You will be safest in bright, well-lit, busy areas.
- Appear and act confident - look like you know where you are going and walk tall.
- Concentrate on where you are going, not on your mobile phone or gadgets.
- You might like to spread your valuables around your body. For example, keep your phone in your bag, your house keys in your trouser pocket and your money in your jacket.
- If someone tries to take something from you, it may be better to let them take it rather than get into a confrontation and risk injury.
- You can use reasonable force in self-defence. You are allowed to protect yourself with something you are carrying (for example keys or a personal alarm) but you may not carry a weapon.
- If you decide to defend yourself, be aware that your attacker might be stronger than you or may take what you are using in self-defence and use it against you. It is often better to shout loudly and run away to a place of safety.
- If you use a wheelchair, keep your things beside you rather than at the back of the wheelchair.
- Try not to advertise your valuables such as mobile phones, laptops, notebooks, tablet or iPod/MP3 player, jewellery, or watch.
- When out walking, be careful not to make your personal items, as mentioned above, an easy target for robbers. Try to keep them hidden also change your daily walking route.
- Stay alert - your phone is a valuable item. When you are out, be aware of your surroundings and do not use your phone in crowded areas or where you might feel unsafe. Do not be distracted by it!

Personal Safety Apps

Smartphones can be utilised for personal safety. Apps such as bSafe, Life360 or Send Help allow you to track and locate family member, send a text message alert when in danger, securely store the voice, location, and timestamps of any incidents that occur to assist police and prosecution. PanicGuard is a personal safety smartphone application that achieved ACPO 'Secured by Design' accreditation. If you feel anxious consider carrying a personal attack alarm.

Theft and Robbery

Street robbery is generally known as mugging. It can also cover snatching bags.

Pickpocketing is slightly different, as you will not be aware of the offence taking place.

Robbery is more likely to take place in quiet or dark areas, and pickpocketing where it is busy, for example on a busy train in rush hour or in a secluded area.

Tips to avoid becoming a victim:

- Remember - be aware of your surroundings. Concentrate on what and who is around you. Do not be distracted by using mobile gadgets and MP3 players. If you are listening to music, use just one headphone so that you are aware of someone approaching you.
- Do not give thieves the chance to take your valuables from you. Do not put them on show.
- Do not leave your bag, wallet, valuable jewellery, mobile phone, or MP3 player on display to thieves.
- If someone tries to take something from you by force, it may be best to give it to them. This will help you avoid getting injured.
- Do not leave bags or pockets open or unzipped. It is easier for a thief to dip into an open bag. Purse bells are a great way of further protecting your purse.
- Always check your surroundings and the environment that you are in

You should think about how you would act in different situations before you are in them. Think about whether you would stay and defend yourself (using reasonable force) or simply get away as quickly as you can.

There is nothing wrong with doing either, but you should think about the options.