businesscompanion
trading standards law explained

Business scams

In the guide

This guidance is for Scotland

A wide range of scams are targeted at businesses, where scammers will use deliberately misleading sales techniques to persuade businesses to part with their money. Common scams include publishing, advertising and directory scams, unnecessary services and unsolicited goods scams, advance-fee fraud, and investment scams.

Scammers use similar techniques across the whole range of scams, and across the range of victims they

are targeting. If a business understands the scammers' techniques and is aware of the common types of business scam, it can minimise the risk that it will be caught by a scam.

These scammers are usually difficult to track down; they operate both in and out of the UK (more often the latter), which makes any potential enforcement action very challenging. It is therefore preferable for businesses to be aware of and be able to avoid these scams in the first place.

What is a scam?

A scam is a dishonest scheme that aims to get money, or something else of value, from its victims.

Many well-known scams are targeted at private individuals or consumers, but there are also scams that target businesses. All sizes and types of businesses can be vulnerable to scams. The losses to individual victims range from a few tens of pounds up to millions.

If a business understands its own vulnerabilities and can recognise a scam for what it is, it can reduce its risk of being caught out.

Persuasion techniques

Scammers use persuasion techniques that are well known to good salespeople. Many of these techniques are used quite legitimately by genuine businesses, but in the wrong hands they are used to draw victims into a scam. The following techniques are commonly used by scammers.

The 'good cause'

Often, a scammer will try to associate their offer with a good cause, such as a local charity or school, a hospital or social objective (such as drug awareness or crime prevention). Businesses can easily be drawn into this as they see it as a way to enhance their own social responsibility in the eyes of customers, and as they see the benefit of associating themselves with a popular cause.

Sometimes the scammer will even deceive a 'cause', like a local charity, into agreeing to be associated with their marketing. When the deception is eventually revealed, enormous damage can be done to the cause and its reputation, as well as to victims' businesses.

The appeal to authority

Scammers will appear to associate themselves with individuals or organisations that are highly respected, well-known or in a position of authority. This can make victims feel more comfortable about agreeing to hand over their money.

For example, advertising scams often claim to be connected with, or approved by, police, fire or health services. Sometimes scams will make reference to Government or local authority schemes, or to new legislation, in order to make their offers appear genuine.

Similar techniques include celebrity endorsement and references to trade associations or large companies.

Foot in the door

It is quite common for scammers not to demand money during their first interaction with their victims. Parting with money is quite often a step too far at this early stage, even for those who eventually do fall victim to the scam.

Typically, scammers will seek just a small, non-financial, commitment to begin with. A mere expression of interest or response to an email may suffice. Once the target has taken this seemingly innocent step, they have in their own mind associated themselves with the scammer's enterprise. When the demand for payment eventually comes, this earlier commitment makes it harder for the victim to resist following through by handing over their money.

Limited offers

Scammers may pretend that their offer is limited, either in volume or in time, so as to elicit a quick decision before the victim has had time to reflect on it. When selling advertising space, a scammer may claim that they are offering the last slot in a publication, or even that they are trying to fill a gap created by a cancellation before a print deadline. Where a busy business is faced with a rushed decision, it is quite likely that the wrong decision will be made.

If an offer is genuine, then there is no deadline so rigid or so tight as to exclude a period for reflection before you make a commitment.

Divide and conquer

In all but the very smallest businesses, incoming enquiries may be picked up by more than one person. Scammers can exploit this fact by making an initial approach to one person in the business and then following up with another person. It is easy for them to lie to the second person that the first person has agreed to something. Although the scammer may have recorded the call, the recipient is unlikely to have done so. The victims can lose confidence in their position and start to believe that they might have made an agreement to the point where they believe they have no option but to pay up.

A twist on this method is the 'authorisation scam'. An initial call is made to the target business and the scammer asks for the details of two people who can authorise an advertisement to be placed. The scammer then calls one of those people, saying that the other person has provisionally booked the advert, and asking for authorisation. Often, the victim accepts the story at face value without speaking to the other person, and authorises the advert.

Distraction and inattention

Scammers are clever at making sure that the important terms of an agreement are both communicated to, and ignored by, victims. Telesales scripts can be designed so that they include information, which is audible in a recording, but which the recipient of the call has no recollection of whatsoever. Written contracts are designed to lead victims' attention away from the all-important small print, so that they do not realise what they have agreed to until it is too late. When a sales representative asks a victim to sign to 'express their interest', and the victim then finds that they have signed a seven-year lease agreement, it can be difficult to prove what was said in the heat of the moment.

Warning signs

As well as looking out for the use, and misuse, of persuasive sales techniques, there are certain warning signs that can indicate that an offer is likely to be a scam. None of these signs are totally reliable, as scammers make efforts to conceal or avoid them, but it is worth looking for them.

Telephone calls

Many business scams are perpetrated through telesales. Without a record of what has been said, phone calls provide an ideal opportunity for scammers to claim that an agreement has been made.

Do not agree to place an advert over the telephone unless you are absolutely happy with the publisher with whom you are dealing and what you are being offered. Insist on seeing written details and a copy of the publisher's full terms and conditions before placing an order.

Some victims receive a string of calls that become increasingly threatening and abusive. Try to keep a record of such calls, including the time, date, name of caller and a note of what was said. By law, any callers should identify themselves and the company from which they are calling.

Be particularly wary if the initial caller transfers you to someone else during the call and always ask the next person you speak to for their name, the name of the company, which department they work in and their contact number. If the person you are speaking to cannot or will not provide these details, or if they become abusive, end the call straight away.

You may be able to request a copy of a recording of a call if it is claimed that one of your employees has placed a definite order. However, some rogue publishers have been known to edit recordings to their own benefit before sending out copies. Consider signing up for the Corporate Telephone Preference Service to cut down the number of unsolicited marketing calls your company receives (see 'Be prepared' below).

Letters and emails

Some business scams come by letter or email. These documents may contain what looks like a simple call to action without any obvious commitment - for example, a request for the victim to check that their details are correct, then sign and return. On closer inspection, the document turns out to be a long-term and/or expensive contract.

In some scams, the quality of the letter is poor, with grammar and spelling mistakes, or maybe poor alignment and layout. This is particularly likely with advance-fee fraud scams.

Contact details

Some scammers, particularly those operating advertising and directory scams, operate in the open. They use genuine company registration and genuine contact details, and simply rely on an expectation that they will not be caught or challenged often enough to cause significant damage to their business model.

Other scammers go to great lengths to avoid being traced or caught. Typically, they will use 'disposable'

email addresses from large providers of free internet email services. Their phone numbers will also be redirects, which are unlikely to relate to any physical location, even if they look like they have a UK area code. However, these same scammers often 'borrow' a postal address, and even a company name and registration, from a real company so as to make themselves look credible. They know that most customers will not write them letters or visit them, so it does not matter to them that post goes to the address of the real company instead.

Payment methods

Where scammers are operating in the open, they often accept the same payment methods as any legitimate business. Other scammers, include those operating an advance-fee fraud, are unlikely to accept payment cards. Instead, they will either ask for payment by a hard-to-trace wire transfer or direct to a UK bank account. Where a bank account is used, this usually belongs to a 'money mule' who is also an unwitting victim of the scammer.

The 'agent transfer' scam

The business receives a call from a telesales agent who falsely claims to be from a legitimate supplier that the company has used before (contact details are often obtained from genuine suppliers or publications). If the targets of this scam express an interest, they are transferred to another person, allegedly in a different department. Victims often agree to place an advert or buy a product because they believe they are dealing with a supplier or publisher they have used before. Only when the invoice arrives, and they do not recognise the company name, do they suspect anything.

If the victim tries to contact the supplier, they are usually told that the call was recorded, and that this is evidence of a 'verbal contract'. The conversation with the first agent (during which the victim has been deceived as to who they were doing business with) is never recorded - only the conversation with the second agent who has actually done the 'selling' - and the caller is careful not to mention the name of the company that they represent.

Repeat business scam

The target business is contacted by phone or letter and the victim is asked if they wish to place an advert in the next edition of a publication. The business is falsely informed that they have advertised in this publication before, but in all likelihood there was no previous edition. In some instances where the approach is by letter, photocopies of adverts taken from, for example, business directories are included to lend an air of authenticity. Many victims authorise the 'repeat advert' without checking any further.

Common business scams

Support publishing and advertising

In this scam, a rogue publisher approaches a business offering advertising space in a publication associated with a worthy cause. Publications might include booklets, yearbooks, diaries, calendars or

magazines for charities, crime prevention, drug awareness, hospitals or emergency service staff. Sometimes publishers make false claims about their connections with, for example, charities or local police, and sometimes they even mislead these organisations into becoming associated with them.

If the publication is ever printed at all, it is sometimes only in a small print run or with very limited distribution, and there is little or no guarantee that the audience will be relevant or local to the advertiser. If a charity donation is made, it is usually a tiny proportion of the overall revenue.

Business directories

Another regular scam relates to business listings in published or electronic directories, or on websites. Beware of 'official-looking' documents from trade directories asking you to provide or confirm your website, email and other contact details. These often look like simple requests inviting a free listing, but the small print can commit you to pay hundreds of pounds for an entry. The listing in the directory is generally worthless; ask yourself whether, if you were a customer looking for your business, you would be likely to turn to this directory rather than to an established search engine.

Unsolicited goods

Scammers sometimes send unsolicited goods to businesses and then, having waited long enough for the business either to use or dispose of the goods, they send an invoice. The goods are often of poor quality, and the prices are usually well above fair market value. Usually, this scam involves business consumables that are cheap for the scammer to obtain, such as stationery, till rolls, generic printer cartridges and cleaning products.

In some variations of this scam, the rogue trader legitimately supplies an order and, some months later, says they have made a mistake and there are some items still to be supplied. The unsuspecting business agrees to the offer of the remaining items and is also given some vouchers or another item to make up for the supposed mistake. When the goods arrive, they do not come with an invoice, and the business uses them. A short while later an invoice for a huge amount arrives and the receiver, despite their protestations, is told to pay.

Bogus invoice scam

The simplest and most blatant scam is that, without any prior contact, bogus invoices are sent to businesses. These invoices might be for adverts in fictitious publications, or for goods that did not exist, or for any other fictitious service. This is a very crude hit-and-miss approach, but a surprising number of victims pay the invoice without question, particularly if the amount involved is relatively small.

Leasing scams

Often involving a personal visit from a sales agent, the target business is persuaded to sign up for a contract, usually for a combination of goods and services, involving a lease on expensive equipment. The goods might include telecommunications equipment, computer equipment, photocopiers or other business / industrial equipment. The services may be related to the usage and/or maintenance of the equipment.

Headline prices appear to be very attractive, but the victim is misled about the extent of their commitment. They often end up tied into long-term (for example, five to seven years) lease agreements, which are very expensive to escape, and the equipment may be poor value for money. It is also common for the service and maintenance agreements to increase in price arbitrarily, or for them to cease when the supplier decides to stop trading and move on to another scam.

Unnecessary services

For a lot of businesses, it can be daunting to try to navigate the range of regulatory requirements that apply to them. Businesses may need licences and approvals, or they may need to file reports and returns with official bodies.

The cheapest, and usually easiest, way to meet all these requirements is to deal direct with the body concerned. In many cases, there is no charge at all to notify, register or supply information in accordance with a regulatory requirement.

However, there are numerous scammers who not only offer a paid service to do this work for businesses, but who mislead businesses into thinking that they are doing so through an official channel. Sometimes, they will write official-looking letters to businesses, making references to legislation and penalties, and demanding information and payment. Sometimes they simply set up websites that businesses can stumble upon when they are looking for the correct, official website to meet their obligations.

This type of scam gained a lot of publicity when registration requirements were introduced under data protection legislation, but similar versions are constantly appearing to reflect new rules and regulations. A similar scam also operates in relation to services that a business might choose to use (rather than be required to use), but where the additional services of the scammer are unnecessary - for example, to request a review of business rates or to register with the Corporate Telephone Preference Service.

If you need assistance in completing an official process, you should approach your own advisers, such as your accountant or solicitor. Otherwise, go straight to the official body concerned, such as the Scottish Information Commissioner (for data protection registration), the Health and Safety Executive (for health and safety registration) or your local valuation officer can discuss your rateable value and provide an appeal form for free - information is also available on the Scottish Assessors Association website.

Investment scams

Some scams are targeted at individuals who run successful businesses, on the assumption that these people may have high incomes or access to investment capital. These scams are also targeted at private investors who are assumed to have disposable capital.

Investment scams are often marketed through call centres known as 'boiler rooms'. They persuade individuals to buy into high-risk investments with the promise of exceptional investment returns. These investments might include shares in small, high-growth companies, precious metals and gemstones, fine wine and art, speculative land investment and forestry, carbon credits and energy investments. Sometimes the investments are real, but the true risks are not communicated properly to the investor; in other cases, the investment just does not exist at all.

Although people in business often think that they would spot such a scam and avoid it, the victims of these scams tend to have been successful and well respected in their working life, whether running their own

businesses or as top managers and professionals.

Advance-fee fraud

There are numerous guises for advance-fee fraud, but the underlying principle is always the same. In return for helping out the scammer (who might pose as a high-ranking official in a troubled regime, or as a lawyer trying to distribute a large inheritance, or a business trying to establish a new product or market), the victim is promised a very large return, often hundreds of thousands, or millions, of pounds. At the early stage, no money is requested, then small incidental charges (such as 'taxes' or 'legal fees') start to crop up and the payments gradually escalate until either the victim spots that it is a scam or runs out of money.

As with investment scams, these scams are targeted at private individuals, but successful business people make attractive targets as the scammers assume that they have access to plenty of capital.

Refusing to pay

If you receive demands for payments for something you believe you have not ordered, it is well worth taking a few minutes to send a written reply, stating clearly why you feel you do not owe any money. Always keep a copy for your records. It is common for businesses to refuse to pay an invoice if they feel that they have been caught out by a scam.

Debt collectors

Some types of business scams are followed up with relentless and aggressive debt collection practices if the victim does not pay. This is particularly the case with rogue publishers, directory scams and unsolicited goods scams.

Some victims pay up even though they feel they have been conned, because they feel it is simply not worth the time and effort to make a stand. However, if they do this, they may be identified as an 'easy touch' and will be targeted again. The details of businesses that can be relied upon to pay up are a valuable commodity, and these details are saved and shared by the more-organised scammers in so-called 'sucker lists'.

Where payments are chased through 'debt collection agencies', these are often owned and run by the publishers themselves, sometimes from the same premises. They are likely to use methods that legitimate agencies would not.

Seizure of goods

Some victims have been threatened with having their goods or belongings seized to pay the alleged 'debt'. The only lawful way a supplier can do this is to first obtain an order in the Sheriff Court, instructing you to pay (for which there has to be a hearing that you are entitled to attend and defend yourself). Then, if you do not pay, the supplier could go back to court for a warrant that empowers the holder to seize goods to the value of the debt.

Threats of court action

Victims are known to have received letters that have stated something like 'This is your last chance to pay. Attached is a summons we have obtained to take you to court if you do not pay now.' The document that accompanied such letters was not, in fact, a summons, but a copy of the application form that must be submitted to a Sheriff Court to request a hearing (this form is freely available in the public domain).

Some victims have been limited companies and the scammer threatened to start insolvency proceedings by applying to the courts for a 'winding up order'. In most cases, the threat was an empty one because such proceedings can only be started for debts in excess of £750 and the amount owed was less than that.

It is useful to note that it would cost a scammer money to take you to court, often much more than it claims you owe. They would have to prove that you owe the money before the court can make a decision against you, and you will have the chance to defend yourself.

Rather than have their tactics aired before a court, and risk losing money even if they win their case, scammers usually prefer to spend their time looking for new victims who will pay up without a fuss. Take independent legal advice if you are in any doubt.

Be prepared

The majority of publishers and suppliers to businesses are reputable; however, some resort to dishonesty for illicit gains. Rogue publishers make huge sums of money by inducing large numbers of victims to pay for adverts in publications that do not exist or are not what people are led to believe. Rogue suppliers enjoy huge mark-ups on poor quality goods sent to businesses without their agreement. Although financial losses to individual businesses are not usually large, they can be enough to cause financial difficulty for some. The tactics used by scammers (particularly when chasing payments) often cause nuisance and, on occasion, genuine alarm or distress.

To improve your chances of avoiding scams:

- register with the Corporate Telephone Preference Service (CTPS), which operates a central opt-out register. It is a legal requirement that companies do not make such calls to numbers registered on the CTPS. This service is free of charge, and it will stop legitimate marketing calls as well as some from scammers
- if you want to place adverts, do your own research before you choose where to advertise. If you want to buy supplies, choose your own suppliers, and if you want to support a charity or good cause, identify that cause yourself and ask how you can help
- look out for the persuasion techniques used by scammers, and for warning signs that you are being targeted by a scam
- don't make a rushed decision, and do check small print carefully before signing any document. Make notes of any telephone conversation, and make sure that everything is confirmed in writing before making an agreement
- remember that a verbal contract is binding. Although you may be able to escape a contract if you were misled into making it, it is easier not to make the contract in the first place
- be aware that, as a business, you do not have the same cooling-off periods that are available to private consumers
- make sure that all staff who take external calls are aware of business scams, and circulate a copy of this guide to them
- check your systems and procedures for invoicing and payment to satisfy yourself that you are adequately protected
- if you wish to complain about what you suspect is a scam, or want further information, you can

contact Action Fraud

In this update

No major changes.

Last reviewed / updated: October 2024

Key legislation

- there is no key legislation for this guide

Please note

This information is intended for guidance; only the courts can give an authoritative interpretation of the law.

The guide's 'Key legislation' links go to the legislation.gov.uk website. The site usually updates the legislation to include any amendments made to it. However, this is not always the case. Information on all changes made to legislation can be found by following the above links and clicking on the 'More Resources' tab.