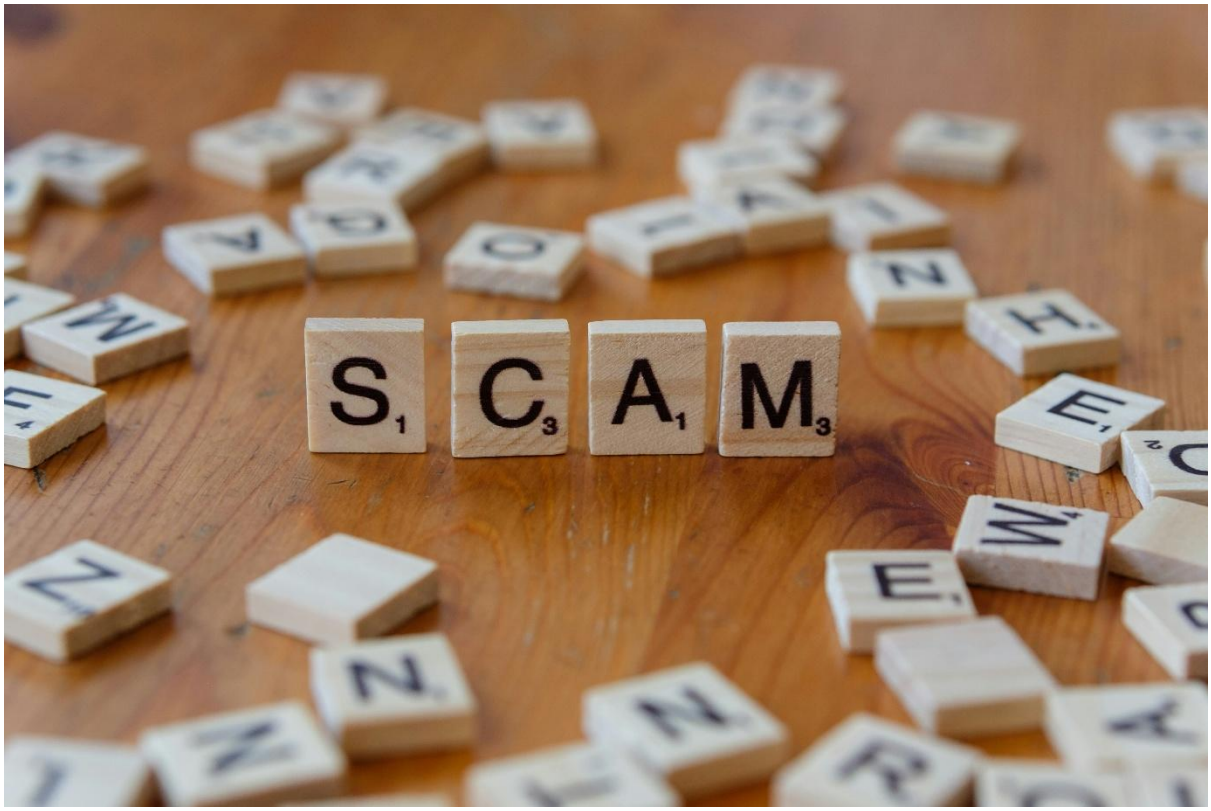
# Scams- How to Identify Them and Report Them




## Introduction

There are many types of scams, some of which are initiated through phone calls or sent via text messages to your mobile phone. Remember that messages can be received on Facebook, WhatsApp, or other apps, and they may also be scams. You could also get scam voice calls on your mobile or landline. Scam advertisements can be displayed on social media sites, on notice boards and on lampposts, even sent through regular mail as addressed letters to you, or as leaflets put through the door. They can also be seen on TV, displayed on your smart speaker, or in newspapers as advertisements.

How to identify them and avoid being caught, as well as how to report and recover from the scam if you are caught, is detailed below, together with a list of over 30 current scams in operation. Remember that leaked Meta documents (concerning Facebook and Instagram, etc.) stated that 10% of its revenue came from scam ads in 2024.

## What to Look Out For

If you receive a phone call and do not recognise the number, or the number is withheld, be cautious before answering it. Similarly, if you get a message from an unrecognised number or person, it could be a scam. If you get a call and there is a period of silence before

someone speaks (or the call drops out), this will be a call from a call centre where, say, an automatic call system dials 15 numbers and the first 10 calls that are answered are put through to the waiting 10 agents. The call may be from a legitimate organisation or, more likely, a scam organisation. If you do answer it, you will soon learn whether it is a scam, as it is most likely one of the 30-plus scams listed below.

In any case, you should always check incoming call numbers (using Google search) to see if they have been reported. Unfortunately, some scam organisations use other people's legitimate numbers when they call, so the incoming call may appear legitimate.

There are over 30 different types of scams in operation, and I am sure other scam schemes are being devised and developed as you read this article.

If you receive a message or notification on your mobile device, do not rush to open it without first examining the displayed information. Obviously, if you are comfortable knowing the sender, you can proceed as usual; however, bear in mind that it could still be spam. Also, be aware of slight changes in the wording (e.g., 1ONOS or !ONOS instead of IONOS). If you spot such changes, you can be sure it is a scam. If you have a preview pane in your email client, you can also check the message details before opening it. If in doubt, do not open it.

Please remember that legitimate websites always use HTTPS website addresses (for example: https://technicalauthorsuk.org). To check any displayed links to see if they are genuine, hover over the links and inspect the link addresses (also called URLs) that are shown when hovering with the mouse pointer or keeping your finger on the address if you are using a tablet or smartphone. If the link shown matches the one displayed (and starts with https), it is a genuine link, but it may still direct you to a site you do not want to visit. The same mouse hover or finger on the address check applies to email addresses at the top or in an email, since the actual email address may not match the one displayed.

As a safeguard for your PC, phone, or tablet, always enable spam filters and ensure two-factor authentication for changes to your bank details and payments. There should be at least a double sign-off for company payments as well. You should never open unexpected attachments unless you are certain the message containing them is legitimate.

Suppose you are unsure about a message after opening it, and it includes contact information. In that case, you can verify any email address or website address by contacting the company directly through its official website, rather than using the information in the message. Of course, the message could purport to come from the company you work for or from a government body; even so, it may not be genuine. So, never give your contact information or bank details to anyone unless you are 100% certain you know the person or company. As an extra precaution, you should always enable **your mobile network's spam protection (this will vary depending on your network).**

Be cautious of any "get rich quick" schemes and do not transfer money or cryptocurrency to unknown accounts or wallets. You must always seek independent financial advice before investing in any scheme. Also, be suspicious of short website URLs (e.g., http://ot.ly) and any pressure to act quickly, regardless of the reason given.

Always call a verified number to verify if any message is legitimate. You should also check for unusual payment instructions, slight variations in the sender's address, or requests that appear to bypass standard approval procedures. Some organisations have email authentication processes that enable you to verify authenticity.

It is a good idea to have a Chase, Revolut, or similar account that requires loading money to use. If you keep a zero balance in such accounts after using them, you can always provide these account details to anyone who legitimately requests them. Whilst the major banks will tell you that nobody can draw or transfer money from your main bank account without your permission, there have been many cases where people have had their bank accounts drained. Only use Chase or Revolut, or similar, account details for incoming payments, even though you think you know the person paying you. You can always transfer any payments to your primary bank account.

If, after all your checks (if you have done them), you become a victim, and depending on the scam type, you must change all applicable passwords, scan your device for malware, disconnect the equipment from the network, and stop any remote sessions. You must also alert any banks or payment platforms (such as PayPal) if any financial information has been disclosed and try to recover or reverse any payments.

# Reporting Scams and Other Checks

Depending on the type of scam you might have fallen for, there are different methods to report and check the details you have.

## Checks If You Are Offered an investment or Pension Scheme

Check whether the company is registered at https://www.fca.org.uk/scamsmart. If not, it is a scam.

## Check Whether a Limited Company is Registered and Legitimate

You can check by visiting https://www.gov.uk/get-information-about-a-company, and if the company is not there, it is a scam.

## To Report a Scam Email

Forward the email to report@phishing.gov.uk, and you can also report it to Action Fraud (https://www.actionfraud.police.uk) or phone 0300 123 2040. Depending on your email client, you should also mark the email as spam and block/report the sender. If you have an iPhone, then also forward the message to **reportphishing@apple.com.**

## If You Have Given Your Bank Details

**Contact** your bank immediately and report the scam to Action Fraud (https://www.actionfraud.police.uk) or phone 0300 123 2040.

## Report Fraud or Financial Crime In Scotland

Contact Police Scotland by calling 101 in Scotland.

## Report a Suspicious Website

Contact the National Cyber Security Centre (https://www.ncsc.gov.uk/collection/phishing-scams/report-scam-website), and they can take down the suspicious website.

## Report a Suspicious Text

Forward the text to 7726 (spells SPAM on a phone keypad) for free. You should always report scam calls and messages to your applicable service provider. Obviously, if you have received a threat, you should report the details to the police. To report the scam text, open the Messages app, and then open the scam message (do not tap any links). Press and hold the message bubble, and then tap More and tap the arrow/forward/share icon. A new message window should appear with the spam text copied in. In the To: field, type 7726 and send. You should get a reply asking for the sender's number, so copy the sender's number from the original message and send it back.

## Reporting and Blocking a WhatsApp Scam Message

Open the chat containing the suspicious message and tap the three dots (Android) or the contact name (iPhone) and select Report and then choose Report and Block. If you received a message from an unknown number, WhatsApp will show "This number is not in your contacts". You should then tap Report and then choose Report and Block.

## Report a Scam Advertisement

**Contact** the **Advertising Standards Authority (https://www.asa.org.uk/make-a-complaint/report-an-online-scam-ad.html).** You should also flag scam ads directly on platforms like Google, Facebook, and Instagram.

## Report a Scam Phone Number

Contact Action Fraud (https://www.actionfraud.police.uk) or phone 0300 123 2040. You should also forward the number as a text to 7726 (spells **SPAM** on a phone keypad). Additionally, you should always report scam calls and messages to your applicable service provider and block the phone number (if displayed) on your phone. Obviously, if you have received a threat, you should report the details to the police.

# List of Scams

Below is a list of over 30 different scam types. There are probably more types of scams, as fraudsters keep coming up with new schemes. If you diligently carry out the checks listed above, you should not fall for any scams.

## Phishing Emails

The scammer sends a message pretending to be a bank, service provider, streaming site, or even someone you know. The email will contain a link to a fake login page or an attachment that contains malware.

## Spear-Phishing

This is also known as Business Email Compromise (BEC) and involves targeted phishing that uses your personal information or appears to be from a company you work for (such as from the CEO or payroll department) to trick you into transferring funds or revealing credentials.

## Supposed Debit Scams

You are notified that a possible debit may be made to your account. This could be from any financial institution, including PayPal or other online payment systems. Typically, a "specially arranged" phone number or email address will be included in the message for you to contact the financial institution to stop the debit. Once you make contact, you will find that the debit cannot be stopped. To compensate, the amount will be credited to your account if you verify your account details to the scammer. If you give your details to the scammer, your account balance will be withdrawn very quickly.

## Fake Invoices and Payment Requests

Criminals will send invoices that appear legitimate (often for services never ordered) or alter bank details on genuine supplier invoices to divert payments. You should look out for new or unrecognisable bank account details, invoices for unfamiliar amounts, companies that you have never heard of that may not even exist, and invoices sent from personal email addresses.

## Fake Login Pages

This is also known as credential harvesting, where a convincing replica of a login page collects credentials when you unknowingly log in. Typically, the webpage URL will not be exact, and the https padlock will be missing. Additionally, the browser may display certificate warnings, and unexpected redirects may occur. If you use a password manager, it will only autofill on legitimate domains, check certificates, and bookmark official login pages.

## Smishing

This is SMS phishing, where text or other messages purport to be from banks, parcel services, or other legitimate providers, but contain links to fake pages or prompts to call a phone number.

## SIM Swap

This is a SIM porting attack, or SIM hijacking, in which a scammer convinces a mobile operator to transfer your number to a new SIM (often using stolen ID information). The scammer then receives all calls and texts, allowing them to receive one-time passwords (OTPs) and account recovery codes via SMS, which can be used to access all your accounts. If you experience a sudden loss of mobile service or an unexpected OTP or other request, contact your mobile provider ASAP to check whether your SIM has been hijacked. To prevent this, set a carrier-level PIN or password on your mobile account, and use an authenticator app (like Google Authenticator) instead of SMS for MFA.

## Vishing

This is voice phishing, where a caller claims to be from a bank, tax office, technical support, or a government body and requests account details, OTPs, or immediate payments. If the call is unsolicited or the caller insists on secrecy and claims it is a matter of urgency that you make a payment, be very suspicious. Do not provide any information or OTPs, etc., and hang up and call the organisation using a known official number. Never allow remote desktop access unless you initiated the contact and trust the provider.

## Technical Support Scams

This is where you get an alert (a pop-up on the screen or a phone call) claiming your computer or other devices are infected. The scammer will request remote access to clear the infection, and then charge you for fake repairs or install malware or ransomware on your equipment. Be cautious of random tech support pop-ups and callers, and never agree to remote control of your equipment or provide credit card details, even for a one-time fee, without verifying the legitimacy of the service. Legitimate companies do not call you out of the blue to fix your equipment.

## Service Provider Scams

This is where you are called by your mobile phone or internet service provider with a special deal. Very often, callers claim to be from a particular service provider with which you are not actually associated, and then you will know it is a scam call. If the caller claims to be from your current service provider, ask for their name and phone number so you can call them back. If they refuse or hang up, you know it is a scam. If you get the information, call the service provider on their regular number and ask to speak to the original caller.

## Investment and Crypto Scams

These are often referred to as Ponzi (pump-and-dump), money transfer, and financial scams, where promises of high, guaranteed returns are made. Sometimes, they use fake endorsements or create a false sense of urgency. Crypto scams often push people to wire money or send crypto to a wallet. Be cautious when there are guaranteed high returns and pressure to invest immediately. Frequently, they use unregulated platforms and promoters who fail to provide verifiable credentials.

## Romance and Dating Scams

Scammers will build trust or establish a relationship online, then ask you for money under the guise of an emergency, travel, or an investment. Often, the scammer will build a long-term relationship with you before requesting money. Be suspicious if the scammer quickly professes love, avoids meetings or video calls, and asks for money or for you to transfer funds due to some unverifiable reason or sob story. You should never send money to someone you have only met online unless you have verified their identity with video calls and by some other means.

## Overpayment and Fake Marketplace Scams

The buyer “accidentally” pays you too much for something and asks you for a refund of the difference. The buyer asks you to send the difference via a money transfer, a gift card, or to

pay it back on a different payment platform. Be suspicious if the buyer offers to overpay, requests a refund using a different platform or asks for a quick payment by wire transfer or gift card. Typically, the scammers' payment will not be honoured by the payment system and will bounce after a few days. Therefore, you should accept payments only through a payment platform of your choice and wait for the funds to be fully cleared. Legitimate overpayments can then be resolved using the same payment platform.

## Prize and Inheritance Scams

You would typically receive a message stating that you have won a prize or inherited money, but must first pay fees or taxes to receive the funds by providing your personal details. You may also be asked to pay “processing fees” on some pretext. Legitimate prize awards do not require advance fees, and if you did not enter the competition, it is likely a scam. If you do know of the person or body that left you the inheritance, it should be simple enough to check the information to validate it.

## Family Emergency Scam

A scammer will call claiming to be a relative (grandchild, child) in urgent trouble, or that they are in contact with the relative and are ringing you on their behalf, and will discreetly ask for money. Before parting with any money, try to contact the person in trouble or a relative to verify the emergency. Never pay any money unless the emergency is verified, even if the caller requests confidentiality.

## Charity and Disaster Scams

After a disaster or high-profile event, scammers posing as fake charities will send donation requests to numerous people, soliciting donations. You should only donate to well-known, registered charities (check official registries) and use credit cards for payment on official charity websites.

## Malware and Ransomware Scams

Opening an infected attachment or downloading a malicious app can encrypt files (ransomware) or steal your data. If you receive unexpected attachments, requests to enable macros, unknown software installations, or apps from unofficial app stores, be highly suspicious and seek advice from a trusted IT support professional. For your security, it is always wise to keep backups of your system, regularly update your software, operating system, and apps, and not enable macros from unknown documents. Additionally, only install apps from official app stores.

## Fake Apps and App Store Scams

Scammers can upload malicious apps that impersonate popular services to steal credentials or payment info. These apps can sometimes be found on official sites or included in messages posted on other sites. These apps often have poor reviews, lack developer information, or request permissions unrelated to the app's functionality. To safeguard against this, only install official apps from the Google Play Store or the Apple App Store, and check reviews and the developer's credentials before downloading.

## QR Code Scams

Scammers replace legitimate QR codes (such as those used for menus and payments) with codes that link to phishing sites, or they trigger unwanted payments. Look out for stickers over original QR codes on payment machines, etc., odd website URLs after scanning the QR code, and prompts to enter personal credentials. If possible, verify the QR code's origin and check the website URL it links to for authenticity.

## Sextortion and Blackmail Scams

Scammer claims to have compromising material, such as a sex video from your webcam, and threatens to publish it unless you pay. They claim to have accessed your equipment and taken a video through your webcam. They will typically demand crypto payment as such payments tend not to be traceable. Never pay, as this will encourage future payment requests. Be careful if you strike up a relationship with someone online and exchange personal information and send explicit photos, as you may be subject to similar requests for payment.

## Threatening Calls and Ransom Extortion Scams

This is where a caller threatens bodily harm or legal action unless a certain amount of money is paid. The demand for payment is usually made via an unusual payment method. The threats should be treated as serious criminal matters, and the police should be contacted immediately.

## Job and Recruitment Scams

Scammers post fake job listings to harvest personal data, receive “upfront” payments for training or other purposes, or purchase equipment. If you are asked to pay to secure a job or to provide your bank account details for salary transfers before you have even accepted the role, it is a scam. You should research the employer and agency, refuse to pay fees, and never take money without verifying its legitimacy in case you are being lined up as a money mule.

## Gift Card Scam

This could take two different forms. Either you are notified that you have won a gift card for a subsequent purchase, or you click on a scam site to spend your gift card. The scam site might be offering a gift card you can use at high street or online shops. Getting an email that you have won a gift card is very suspicious, as in most cases, you have not even entered a competition to win one.

## Payment Declined Scams

This is where you are notified that your payment for something has been declined and asked to re-enter your payment details to complete the purchase. In most cases, this will be a scam, but if you are on a legitimate site and you pay for something, the message that your payment has been declined could be legitimate.

## Social Media Scams

A leaked Meta document stated that around 10% of messages on its sites are scams. Looking at Facebook, it appears this figure might be much higher. There are fake adverts for items that never

arrive, as well as items for sale that you pay for, which you can get on Amazon at a cheaper price and often without paying postage fees. There are also adverts for training courses, legal advice, and other services that you pay for but either never receive or receive inferior service.

## Missed Call Scams

Some scammers call your phone number and hang up after one second, which encourages you to call back. If you get such a call, check the missed call number on Google search before calling back. Obviously, if the search reveals the number has been used for scam calls, you should not call back. One thing to look out for is whether the number is legitimate. If you call back and say you had a missed call from them, they may say they did not call you. This most likely is the case where the scammer has used someone's legitimate phone number to call you, as the call equipment scammers use can pretend to call you from any number they wish.

## Duplicate Site Scams

You want to renew your passport or driving licence, or register for something, and you search for the applicable site. You click the top result, and very often the site is a mirror of the real one. You could probably renew your passport or driving licence at one of these sites, but you would pay more than the regular price, or pay for something like a driving licence renewal, which is usually free. Make sure you only click the correct site, not a look-alike.

## Ticket and Booking Scams

This is a popular scam for buying concert or other tickets, where you pay extra for a booking than you would on the legitimate site, or you actually end up with no real booking or fake tickets. Buying second-hand tickets is also an issue, as very often the original purchaser's name is on them, and you may be unable to use them due to security checks on entry.

## Cyber Attacks and Ransoms

This type of issue tends to occur in large organisations, but you could still have inadvertently picked up a virus that has compromised your computer equipment, tablet, or phone. In most cases, it would be cheaper in the long run to seek professional advice rather than pay a ransom upfront.

## Tax Rebate Scam

With this type of account, you are notified that you are due a tax rebate and that you need to provide your bank account details to receive the money. If, after doing all your checks, you decide this is a legitimate request, you can give the Chase or Revolut bank account details suggested. If you have been fooled, nothing will be lost. If no money turns up, you will need to change the account details by contacting Chase, Revolut, or another provider, as appropriate.

## Household Services Scams

You may be contacted by a company offering loft insulation, moss removal from your roof, gardening services, or window replacement. In most cases, it is best to avoid such services, even if you need the work done. There are many scam companies or people that operate in this manner, and many are not reputable. If you require a service, get three quotes from reputable, registered companies, pick the one you like best, and avoid using an unknown person or company.

## Delivery and Shipping Scams

This scam takes on a few slight variations. Although you may not have ordered anything, you are advised that delivery cannot proceed without payment of customs clearance or delivery charges. If you are really expecting a delivery, there should be no extra charges. When an item is ordered, any delivery charges are added, so no additional payments should be necessary.

## Website Design and Services Scams

This takes on two forms. If you have ever had a website or used an uncommon email address, it will be assumed that you have a website, and you will receive an email offering specialist website service. The other type of message or phone call you will receive is an offer to build you a new website. Such requests should be rejected, as many companies offer free website design services. They get their payments from the website host company.

# Test Your Scam Knowledge

**Complete the** Stop Fraud's Scam Savvy Quiz: http: **Are you scam-savvy? - Take Five** (https://quiz.takefive-stopfraud.org.uk).