

# How to avoid common scams and stay safe

COVENTRY Building Society

# What's inside?

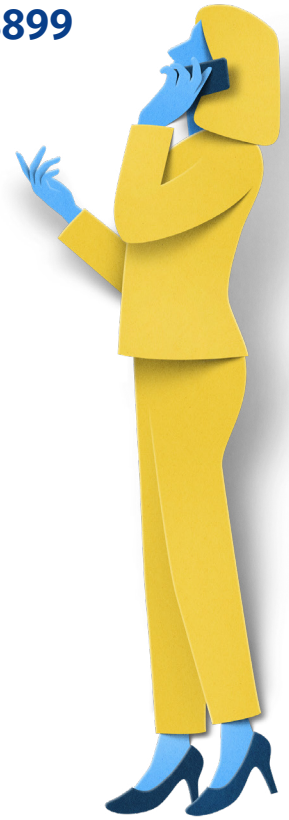

| | Page | Read<br>Tick the box once you have completed reading that section |
|---|---|---|
| Scams – stay protected | 4 | ☐ |
| Text scams | 5 | ☐ |
| WhatsApp scams | 6 | ☐ |
| Suspicious phone calls | 7 | ☐ |
| Suspicious emails | 10 | ☐ |
| Postal scams and junk mail | 12 | ☐ |
| Safe account scam | 13 | ☐ |
| Payment misdirection | 14 | ☐ |
| Fake websites and online scams | 15 | ☐ |
| Investment fraud | 16 | ☐ |
| Identity theft | 17 | ☐ |
| Holiday fraud | 18 | ☐ |
| Online dating and social media scams | 19 | ☐ |
| Remote access fraud | 20 | ☐ |
| Wi-Fi security | 21 | ☐ |
| Rogue traders | 22 | ☐ |
| Property and land fraud | 24 | ☐ |
| Cash machine fraud | 25 | ☐ |
| Follow-off theft | 27 | ☐ |
| How we help to protect you | 29 | ☐ |
| Other ways you can help to protect yourself | 30 | ☐ |
| What to do if you think you've been scammed | 33 | ☐ |
| Where to find out more | 34 | ☐ |
| Stay safe and alert to scams | 38 | ☐ |

# Making our services accessible

If you feel like you might need extra support, on a short or long term basis - for any reason - there are lots of ways we can help.

Scan the QR code or go to **www.coventrybuildingsociety.co.uk/member/supportingmembers** for more information on how we can help or to download the Making our Services Accessible leaflet.

We can also send you a copy of the Making our Services Accessible leaflet, or this leaflet, in large print, Braille or on audio CD. Call us on **0800 121 8899** and we'll be happy to help.



# Scams – stay protected

Criminals are clever. They're always developing new ways to try and catch you out and get their hands on your money and your personal information.

Scams come in all shapes and sizes. They could be online, by phone, by email, by post, through someone stealing your personal information, even on your own doorstep.

Most people think they wouldn't fall for a fraudulent email or text. But any of us can be scammed.

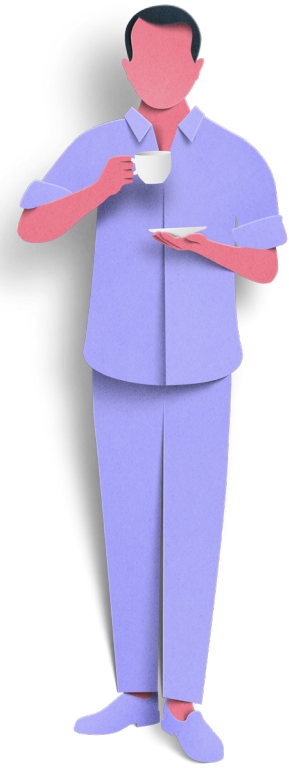
The good news is you can protect yourself as long as you know what to look out for. In this guide, we've included some common scams to help you spot threats. Try to familiarise yourself with them. If you can recognise an email that looks wrong, a phone call that doesn't sound quite right, or an offer that seems too good to be true, then you can often avoid becoming the victim of a scam.

## Take Five to Stop Fraud

If you receive a request to provide personal or financial information, take a moment to reflect and step back from the situation. Yes, even if they say they're us or another trusted organisation, you still need to take the time to stop and think about what's really going on.

TAKE FIVE TO STOP FRAUD

**www.takefive-stopfraud.org.uk**



# Text scams

Criminals send text messages (also known as an SMS) to random mobile phones. They often claim to be someone you know and trust. For example, your bank, mobile phone provider or a delivery company.

The message may try to trick you into clicking a link to a fake website or calling a phone number. It might say you need to verify or update your details or reactivate an account. The criminal will then attempt to get you to give out personal or financial information. They can then use this to access your accounts.

The messages will often tell you to act quickly or face serious consequences.

## Why you should report suspicious text messages

The purpose of a scam text is often to get you to click a link. This will take you to a website that could download viruses to your computer, steal passwords or other personal information. This is known as phishing.

Reporting a suspicious text is free and only takes a minute.

By reporting you can:

- Reduce the amount of scam texts you receive
- Make yourself a harder target for criminals
- Protect others from cyber crime online.



Most phone providers are part of a scheme that allows customers to report suspicious messages for free. If you forward a text to **7726** (this spells SPAM on your keyboard), this information is then shared with the police and intelligence agencies to stop scams. Alternatively, you can take a screenshot of the text message and send it to **report@phishing.gov.uk** if you prefer.

# WhatsApp scams

Criminals may pose as a member of your family and send messages out of the blue. Often, they ask you to save their new contact number.

They then claim there's an emergency and ask you for money urgently. This can seem more realistic as you have them as a saved as a known contact. The conversation might start by text and move to WhatsApp.

Another common scam is when someone claims to be a friend who gets in touch to say they've sent you a verification code by mistake. They'll ask you to help them by sending it on to them. Once a criminal has this code, they can log in to your WhatsApp account and lock you out.

These messages can be very convincing. Always stay alert and vigilant when using online platforms to talk to family and friends.



## How to protect yourself

The best way to check if someone is who they say they are, is to call them on a phone number you know to be genuine.
You'll be able to tell if it's them by their voice.

If you do receive a strange message:

- Don't reply
- Tap the chat info and scroll to the bottom of the screen – Tap Report > Report and block
- Delete the message.

**Remember! Never share one-time passcodes.**

# Suspicious phone calls

You might get a phone call from a criminal claiming to be your bank or building society. They could also pretend to be HM Revenue & Customs (HMRC), the police or other 'law enforcement agencies'.

These scams may be automated or from a real person. Their aim is to steal account security information or trick you into giving them money.

They may ask for your personal information or to tell you to transfer money.

## Here are some examples of what a criminal might say:

- "There's a problem with your account and your card has been compromised. Give me your security details and I can send you a new card."
- "We've detected fraudulent activity on your account. I can transfer funds for you, I just need your security details."
- "I need to verify your identity. Enter your full PIN on the phone keypad."
- "We've detected a virus on your computer. Download and install this software so we can remotely access your device."
- "You've won a prize! But you need to transfer money to us in order to claim it."

## How can I protect myself?

If you're called randomly by someone who says they're phoning about your Coventry Building Society account, ask for their full name, job title and department. Then end the call and call us on **0800 121 8899**.

To be sure that the line is clear, use a different phone to call us. You could call a friend before you call us to avoid reconnecting to the criminal.

Our telephone number won't show up if we do ring you. This is to stop criminals pretending to be us and trying to get your personal information.

And remember, never give out your full security details over the phone.



You can also register with the Telephone Preference Service (TPS). This is the UK's only official "Do not call" register for landline and mobile numbers.

It's a free service to opt out of sales and marketing calls. The only thing it won't stop is automated marketing calls, known as computer generated calls. This is because the law only applies to people and not computers.

**Registering with TPS is quick. You'll need your:**

- Phone number(s)
- Postcode
- Postal address.



**To register:**

- Fill in the TPS online registration form on their website **www.tpsonline.org.uk**
- Call their 24-hour automated telephone registration on **0345 070 0707**
- Text "TPS" and your email address to **85095**.

TPS will never ask you for money to register with them. If someone does ask you, it's a scam.

## If you have been scammed

If you've lost money or have been hacked as a result of responding to a call, you should report it to Action Fraud. You can do this by calling **0300 123 2040** or simply text **7726** with the word "call" followed by the scam caller's phone number.

# Suspicious emails

You might get an email that looks like it's come from a real sender. But really, it's a criminal posing as someone you trust. They could be pretending to be your bank or building society, HMRC, or a service you use – like eBay, Apple or PayPal.

These emails usually ask you to enter or update your personal or security details. This is so criminals can steal them. There's often a time limit and a link to click.

## How to spot a suspicious email

Emails that have lots of spelling mistakes are a big giveaway. The company name might not be quite right. And if you can also click on the email address of the sender, it might not look real.

When you get an email from a company that knows you, there will likely be a personal reference in the email. They may use your name, part of your postcode or an account number.

Be particularly wary of emails that have new payment details from a company.

If anything looks suspicious and you're being asked to share any information, don't click the links within the email. Links often take you to a fake but convincing webpage, where you'll be asked to enter your details. By clicking the link might even trigger the download of a virus onto your device.



**Remember! We'll never send you an email asking you to enter your details or linking you directly to our Online Services.**

## What should you do?

If an email lands in your inbox that you're not sure about, you can report for free to: **report@phishing.gov.uk**

This email will go to the National Cyber Security Centre (NCSC), run by the government. They can take down scam emails and websites. By sending on anything you suspect, you can:

- Reduce the amount of scam emails you receive
- Make it harder for scammers to target you
- Help protect others from cyber crime.

When you report an email, the NCSC will check the suspect email and any websites it links to. If they think the activity is malicious, they can:

- Work with hosting companies to remove links to these websites
- Raise awareness of commonly reported suspicious emails and methods.



### Have you spotted a suspicious email?

If you've received an email which you're not quite sure about, forward it to the Suspicious Email Reporting Service (SERS): **report@phishing.gov.uk**

There's more information on their website: **www.ncsc.gov.uk/information/report-suspicious-emails**

# Postal scams and junk mail

Sometimes we get offers of products and services through the post. They're usually random and often just too good to be true.

Some might promise you the earth but ask you for money before they deliver. Many are supposedly time limited. They'll try and introduce a sense of urgency to get you to act quickly.

## Here are some examples of junk mail scams

- You've won cash or a prize on the lottery, but you need to pay an admin fee to claim it.
- You're asked to get involved in a chain or selling scheme and you need to send money to claim your reward. You might also be told that something bad will happen if you break the chain.
- You get a plea for funds to pay for an operation, help an orphan, or rescue someone from another county who's in danger. It's from an organisation you've never heard of.
- You get a letter saying that you can release some of your pension income before the age of 55 – if you pay a fee.

You can get your name and address removed from most direct mailing lists. To do this, you can register with the Mailing Preference Service. It's easy to set up. Just go to **www.mpsonline.org.uk**

If you're eligible to vote, you can also opt out of the 'Open Register' by visiting **www.gov.uk/register-to-vote** or contacting your electoral registration office. You can find the details of your local office on **www.gov.uk/contact-electoral-registration-office**

### Be aware

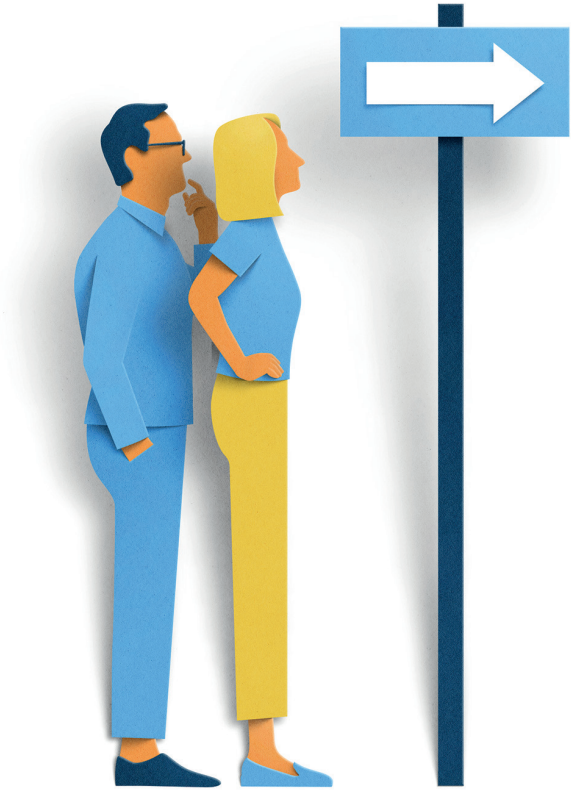
- Never send money to someone you don't know – you shouldn't have to pay anything to get a prize
- Check to see if it's from a registered charity – if you haven't heard of the organisation contacting you, check them out on the government charity register at **www.gov.uk/find-charity-information**
- **If in doubt – bin it**.

# Safe account scam

A safe account scam is where a criminal calls you or sends a text pretending to be your bank, building society or the police. They'll tell you that your bank account has been compromised and they'll convince you to transfer all your money to a 'safe account'. They'll reassure you that this will stop the scammers. You may also be told that you are 'assisting with an important investigation' and must not discuss this with anyone, including your bank or building society. You might be threatened with arrest if you don't co-operate. But as soon as you've transferred all your money to this safe account, the criminals will disappear without a trace.

## Protect yourself from safe account scams

No one other than a criminal will ever ask you to move your money. If they call, hang up. If they text, delete it. You won't be arrested, and that way you'll keep your money safe.



# Payment misdirection

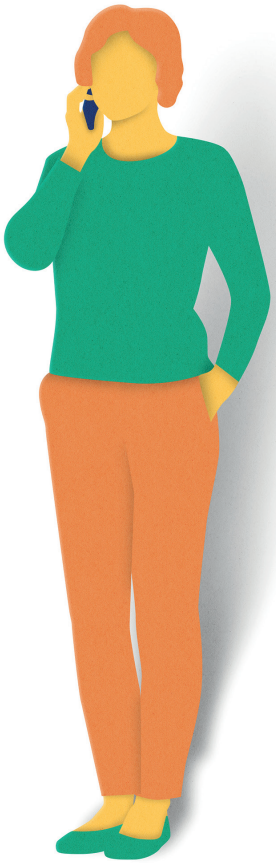
You may get an email asking you to set up a payment to a new account or to the details you have for a payee. The email might look like it's come from someone you know, like a builder or solicitor you're expecting to pay.

Emails, texts and phone numbers can be spoofed, so they're made to look genuine. Criminals can hack email accounts or change small details in an email address.

This means you could end up sending a payment to them rather than where you want to. Often you won't know that's happened until the genuine person or company contacts you to ask for payment.

## Protect yourself from payment misdirection scams

- Always confirm any instructions to make a payment to a new account or change existing account details. You should check directly with the person or business asking for the change.
- Don't reply to the email or text or use the contact details included in it. You should call the company or person on a number you've used before or look them up independently, to confirm that the change of bank details given is genuine.



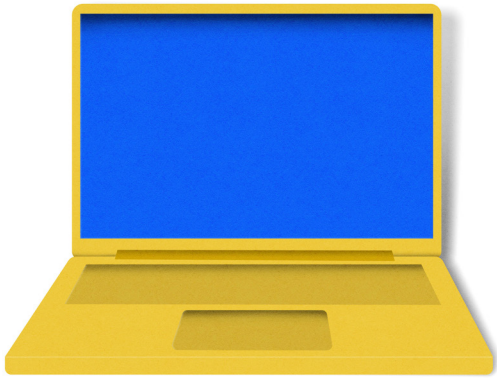
# Fake websites and online scams

A spoof website imitates a genuine website to fraudulently collect personal or sensitive data from you. They're designed to look like the real site. You can even be on a genuine listing site, such as eBay or Amazon, where people are not who they say they are. You buy goods, pay for them and nothing arrives.

## Protect yourself from fake websites and online scams

- Closely check the web address of any site you're visiting. Watch out for small clues, like spelling mistakes. Check the security certificate. A secure website would show a padlock symbol next to the address in your browser's top bar.
- Be wary when buying goods online. Goods might not arrive or are not what you ordered. Make sure you carefully check the seller's history.

Use online payment options such as PayPal that can help protect you, instead of sending money direct.



# Investment fraud

Someone encourages you to invest money in a scheme, but it turns out to be worthless or non-existent. You could lose your hard-earned savings, so always be cautious.

Investment fraud comes in many forms. But there's usually one common promise when someone is encouraging you to invest in a new scheme. They'll say you'll get a high return with little or no risk to your money. They're usually time-limited offers, and they ask you not to share with anyone else.

## How to protect yourself from investment fraud

- Even genuine investments, with the potential of high returns, carry a risk. But you should be cautious if this comes randomly from a cold call, email or letter you didn't expect.
- Don't let anyone pressure you in to making a quick decision. You might want to get independent financial advice from a professional. Especially if the type of investment isn't familiar to you.
- Check out the firm that's contacting you on the Financial Services Register online at **www.fca.org.uk/register**. You can also check the actual investment on Financial Conduct Authority (FCA) ScamSmart at **www.fca.org.uk/scamsmart**. Here you can find details of investment scams. You could also contact the FCA on **0800 111 6768**.

There's one golden rule if you're thinking about investing your money – if it seems too good to be true, then it probably is.



# Identity theft

This is when someone steals your personal details and uses them to act fraudulently in your name. They could open bank accounts or take out loans, apply for credit cards and order goods, leaving you with the debt. They'll even be able to access your accounts.

## Protect yourself against identity theft

- Keep your personal details and documents safe. Make sure you shred them when you want to throw them away.
- Be wary if anyone asks for your personal details. And remember to never write your security details down.
- Always question any uninvited approaches in case of scams. You should contact the company directly using a known email address or phone number.
- Remember to check your account statements carefully. This may help you spot unusual activity.



# Holiday fraud

Criminals may offer flights, places to stay and other travel services that just don't exist. They may have set up a fake website, or maybe list a fake advert on a genuine site.

They'll encourage you to pay directly to them for a discount. They might ask for a direct bank transfer and may even send a confirmation email to make it all look real.

## How can you protect yourself from holiday fraud

- Make sure your booking is confirmed by a consumer protection scheme. This could be ABTA (Association of British Travel Agents) and/or ATOL (Air Travel Organiser's License). Don't rely on seeing their logo. Check membership on the ABTA website **www.abta.com** or ATOL's website **www.atol.org**
- Research any property before you book. Check the reviews and look at listings on other sites. Be wary if prices differ significantly.



# Online dating and social media scams

This is when you're tricked to pay a person you've never met, with whom you believe to be in a relationship with, or you trust. It often takes place through online dating websites. But criminals may also use social media such as Facebook, TikTok, Instagram or email to make contact.

When they know you trust them, they'll ask (either subtly or directly) for money. They could also ask for gifts or your bank/credit card details. They often pretend to need the money for an emergency. It could be for a family member who's ill and needs medical attention. Or they could claim they're struggling with money due to bad luck, like a failed business or a mugging.

## But are they who they say they are?

Never send money or your account details to someone you haven't met in person. Be alert to spelling and grammar mistakes or gaps in their stories. There could be other signs too, like their camera never working when you want to video call each other. Don't rush into an online relationship. You should get to know the person, not the profile and ask lots of questions.

Analyse their profile and check the person is genuine. You can put their name, profile pictures, things they always say plus the term 'dating scam' into your search engine. Also, do an image search of your admirer to help find out if they are who they say they are. You can use image search services such as Google or TinEye.

Talk to your friends and family about your dating choices. Be wary of anyone who tells you not to tell others about them. Stay on the dating site messenger service until you're confident the person is who they say they are. If you do decide to meet in person, make sure the first meeting is in a public place and let someone else know where you're going to be.

Some dating scams can end with a lot of money changing hands – and no relationship at the end of it.

# Remote access fraud

Someone accesses your computer using software they've asked you to install.

Be wary of anyone who calls you telling you they need to 'fix a problem' on your machine. They might claim to be from your broadband provider and tell you they need to correct an issue with the router. They'll tell you the only way they can do this is by accessing your computer.

The caller might even offer to pay you to do this work. Then they'll claim they've overpaid you and ask you to log in to your online banking to return the money. Before you know it, they have your account details.

## How to protect yourself from remote access scams

- Don't let anyone remote access to your computer and never log in to your online banking accounts while you're on the phone to someone.
- Don't share your security details or one-time passcode (OTP) with anyone. Even if you have a joint account, your login information should be unique to you.
- Never agree to anything hastily. If you're in any doubt, say you need time to think and end the call.



# Wi-Fi security

Not all Wi-Fi you can access in public is secure. This means criminals could use this to steal your data. Even if you access an app without typing in your password, your phone or tablet will still be able to send your passwords over the Wi-Fi.

## Protect yourself

- Make sure the Wi-Fi you connect to is secure.
- Don't use public Wi-Fi for doing anything you wouldn't want a criminal to see. Think online banking, accessing emails, or anything that requires a username or password.
- Use your mobile data connection if you're not sure that the Wi-Fi is secure. Data passed via your own mobile data connection is encrypted and more secure.
- Use a Virtual Private Network (VPN) when connecting to public Wi-Fi. This will encrypt information you send. You can download a VPN from your app store.



# Rogue traders

A trader turns up on your doorstep unannounced to get business from you. They usually give you a quote for work you may not even need doing and often at a higher price than you should pay.

Rogue traders can be unpleasant and use threatening, high pressure tactics to get you to commit to buying their goods and services. Some will demand payment before they start, or before they've finished the work and never come back. They may not even be properly qualified to do the work.



## Protect yourself from rogue traders

- Never agree to work being done on the spot. If someone knocks on your door and tells you, 'you need work doing' – roof tiling, exterior painting, gutter repair – just say no. Be firm, they may not want to take 'no' for an answer.
- If you know you need some work carried out, shop around – contact them yourself and get a minimum of three quotes from reputable local traders.
- Ask friends for recommendations – it's the best way to get someone you can trust to do the job.
- Don't take money out for them – if they offer to go with you to get cash out, refuse!
- If you feel like you're in danger, call the police.

### Approached by a rogue trader?

Then contact Trading Standards. Call their Citizens Advice consumer helpline on **0808 223 1133**.

# Property and land fraud

Property and land fraud is where criminals try to 'steal' your property and/or land, most commonly by pretending to be you and they could attempt to sell your house or take out a mortgage on your property without your knowledge.

**You're more at risk if:**

- Your identity's been stolen
- You rent out your property
- You live overseas
- The property is empty
- The property is not mortgaged.

## Protecting yourself from property and land fraud

You can take steps to protect your property from being fraudulently sold or mortgaged. Your property will already be registered if you bought it or it has been mortgaged since 1998. Please check with HM Land Registry if you're unsure.

For more information visit **www.gov.uk/guidance/property-alert** or by calling **0300 006 0478**. It's free to register your property to receive alerts, such as if someone applies to change the register of your property. For example, if someone tries to use your property for a mortgage. This won't automatically block changes to the register but will alert you when something changes so that you can take action. You can get alerts for up to 10 properties and there's no fee.



# Cash machine fraud

Criminals continue to find new ways to take your money – but the outcome is still the same. You get distracted at a cash machine, you lose sight of your card and you have your money stolen.

## How it could happen to you

You insert your card into a cash machine and enter your PIN. In the queue behind, a criminal is looking over your shoulder and sees your PIN. This is known as shoulder surfing. Some of the scenarios that could follow are:

- A 'passer-by' distracts you while you're using the cash machine by pointing to a dropped wallet or money on the ground and asking if it's yours. As you look away from the screen, an accomplice leans in to swipe your cash or card. If they take your card, they can use it with the PIN they've seen while shoulder surfing and will take money from your account elsewhere.
- Your card won't eject from the cash machine, you think it's been swallowed. A 'passer-by' offers to help. They suggest you try your PIN again – which you do – and they watch to see which numbers you enter. When your card still won't come out, they suggest you go into the branch to ask for help. In your absence, they then eject your card and use it elsewhere.
- A criminal distracts you at a cash machine. They steal your card and replace it with an almost identical one so you don't realise yours is gone until it's too late.

## How to protect yourself from cash machine fraud



- Always look closely at the slot on a cash machine. Never use it if it looks as though it's been tampered with. And if something doesn't look right, please let the branch employees know too.
- You never know who's behind you at a cash machine, so make sure you always shield the keypad when entering your PIN.
- Never let anyone distract you at a cash machine. If you hear an 'excuse me' or 'is this yours?', stay focused and only respond when you've finished.
- If your card won't eject from the cash machine, call your bank or card issuers helpline while you're still standing by the machine. If you have an app, use it to temporarily freeze your card. Don't walk off. Don't accept help from a stranger or go into the bank to talk to them this can allow a criminal to move in and steal your card.

**If you're ever distracted at a cash machine, check the details on your card to make sure nobody has switched it with a similar one.**

# Follow-off theft

Criminals often use cunning tactics to steal from people who've just taken money out. Here are some of the common tactics they use and how you can protect yourself:

## Surveillance and targeting

Criminals watch for people taking out lots of money from a cash machine. Then they follow their targets to a less secure location.

## Distraction and deception

A criminal might approach you with what seems like an innocent question or request. They're distracting you while an accomplice steals your money. They might also stage a fake accident or spill something to grab your attention.

## Bag switching

Criminals may switch your bag or envelope containing money with an identical one while you're not looking. They often do this in busy or crowded places where you may not notice.



## Vehicle break-ins

Criminals follow you to your car. They then wait for a chance to break in and steal your money when you leave it unattended, even for a short period.

## Direct confrontation

In some cases, criminals might confront you directly. They can use intimidation or threats to steal your money.

## Protect yourself from follow-off theft

Stay alert, be aware and be conscious of your surroundings, especially after making large withdrawals.

Avoid displaying cash in public. Conceal it, place it securely in your bag or pocket immediately.

Keep your bag or purse close to you at all times. Don't leave your things in your car or in your shopping trolley after making large withdrawals.

If you feel like you're being followed, trust your instincts. Go to a crowded place, go back into the branch to seek help, or call the police.

If possible, take someone with you when you plan to withdraw a large sum of money.

Stay vigilant and protect yourself from follow-off theft.



# How we help to protect you

- We'll never ask you for your full PIN or Telephone Password. We'll only ever ask you for some characters when you call us.
- We'll never ask you to transfer money or offer to do it for you. If someone suggests this to you, it's not a genuine call.
- A Coventry Building Society employee will never come to your home, unless we have an appointment and you're expecting us.
- We'll never ask you to give us any of your online security details over the phone. You'll only be asked to do that when you log in to Online Services.
- We'll never send you a link to a login page. If you get an email asking you to update your security details, don't click on anything.
- All our branches have digital CCTV systems in place. These are monitored by our Security Operations Centre 24 hours a day, 365 days a year.
- We have security fog in our branches and a range of sophisticated alarm systems. They detect and monitor our branches. Our alarms link to the police who provide around the clock response.
- Our branch colleagues do security training and are kept up to date with the latest developments in scams and frauds to help protect you.
- We work closely with the police, National Police Chief Council, other banks and building societies, as well as other agencies to share information and work together to combat crime.

# Other ways you can help to protect yourself

## Credit reports

Checking your credit report is part of good credit hygiene. It can help you spot identity theft or fraud early. If you see an address that is unfamiliar, credit you didn't apply for, or activity on credit cards you've not used recently, a credit report can give you the heads up.

You can check your credit files online or via an app at Experian, Equifax, TransUnion, Credit Karma and Clear Score.



## Devices

Criminals may also try to attack your devices. This can compromise both your data and your privacy. It can also expose you to hacking and identity fraud.

Devices like smartphones, tablets and PCs are getting more secure. But hackers are getting better at attacking them too.

We do so much on our devices. From online banking and shopping, to email and social media, you should take steps to stop cyber criminals getting hold of your data. Think about your devices much the same way as you would your purse or your debit card. You need to keep them protected from criminals.

## How you can protect yourself

If you've just bought a new or second-hand device or haven't looked at the security for a while, take some time to make sure you're protected against the latest threats. Most companies have easy to use guides on how to secure your devices.

You can also look on the Which? website where you can find more information on how the check the security on your device. To do this visit **www.which.co.uk** and search mobile phone security. These companies also have more detailed information on their websites:



- Apple
- Google (Android)
- Samsung
- Microsoft.

## Antivirus software

Antivirus can detect and remove viruses and other kinds of malicious software from your devices. This is known as malware.

Malware are codes that cause harm to your devices and the data that's on them. Common types of malware are:

- **Trojans** – this can download onto a computer disguised as a real program to gain user systems access with their software.
- **Adware** – this makes pop-up ads show up on your computer or mobile device. Adware can slow your device down, hijack your browser and install viruses and/or spyware.
- **Spyware** – gathers data from your device and sends it to third parties without your consent.
- **Ransomware** – is designed to block access to a computer system until a sum of money is paid.

Microsoft devices are often targeted by malicious snooper – a program or malware designed to secretly watch, collect or steal data. Because of this, it's a good idea to install robust antivirus protection on these types of devices. Without this, hackers can exploit devices and online accounts.

## How does antivirus work?

Antivirus makes it harder for criminals to get your data. You can run scans regularly to see if your device has been infected.

Modern antivirus products update automatically. This helps keep you safe.

You may want to do your research to find which antivirus is right for you. For more guidance, visit National Cyber Security Centre **www.ncsc.gov.uk**



# What to do if you think you've been scammed

First, contact the organisation who provides your account. To do this, use details from their website, original paperwork or the FCA register.

Under current regulations, if you lose money as a result of a scam, you should be able to claim your money back. This is subject to conditions and limits from where you sent the money from.

If you think you've been a victim of fraud, make sure you report it to the police. You should let them know if you believe your account details or personal information have been stolen.

Remember, criminals are experts at impersonating people, organisations and the police. They spend hours researching you for their scams, hoping you'll let your guard down for just a moment.

- **Stop**: Taking a moment to stop and think before parting with your money or information could keep you safe.
- **Challenge**: Could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.
- **Protect**: If you think you've fallen for a scam, contact us immediately and report to the police on **101** or alternatively contact Action Fraud on **0300 123 2040** or **www.actionfraud.police.uk**.

**My money? My info? I don't think so!**

For more advice, visit:

**www.takefive-stopfraud.org.uk**

TAKE FIVE TO STOP FRAUD™

# Where to find out more

This leaflet doesn't include all scams and criminals on on how to protect yourself, visit the websites below:

| | | |
|---|---|---|
| Action Fraud<br>**0300 123 2040** | ActionFraud<br>National Fraud & Cyber Crime Reporting Centre<br>0300 123 2040 | **www.actionfraud.police.uk** |
| Citizens Advice Bureau (CAB)<br>**0808 223 1133** | citizens advice bureau | **www.citizensadvice.org.uk** |
| Crimestoppers<br>**0800 555 111** | CrimeStoppers. | **www.crimestoppers-uk.org** |
| FCA ScamSmart | FCA ScamSmart | **www.fca.org.uk/scamsmart** |
| Financial Services Register | FCA | **www.fca.org.uk/register** |
| Get Safe Online | GET SAFE ONLINE | **www.getsafeonline.org** |
| HM Land Registry – Property alert<br>**0300 006 0478** | HM Land Registry | **www.gov.uk/guidance/property-alert** |
| Mailing Preference Service<br>**0207 291 3310** | mps | **www.mpsonline.org.uk** |
| National Cyber Security Centre | National Cyber Security Centre<br>a part of GCHQ | **www.ncsc.gov.uk** |

The UK's national reporting centre for fraud and cybercrime. Here you can report fraud if you have been scammed, defrauded or experienced cybercrime in England, Wales and Northern Ireland.

This national charity and network of local charities offers confidential advice online, over the phone, and in person, for free.

An independent charity that gives you the power to speak up and stop crime – 100% anonymous. Open 24/7, 365 days a year.

Enables a fair and thriving financial services market for the good of consumers and the economy.

A public record of firms, individuals and other bodies that are, or have been, authorised by the Financial Conduct Authority (FCA) or the Prudential Regulation Authority (PRA).

The UK's leading internet safety website who provide unbiased, factual and easy-to-understand information on online safety.

Enables you to monitor a property if it's already registered with HM Land Registry, monitor the property of a relative; you don't have to own a property to set up an alert.

A free service funded by the direct mail industry to enable you to have your name and home address in the UK removed from lists used by the industry.

Helps businesses, the public sector and individuals protect the online services and devices that we all depend on.

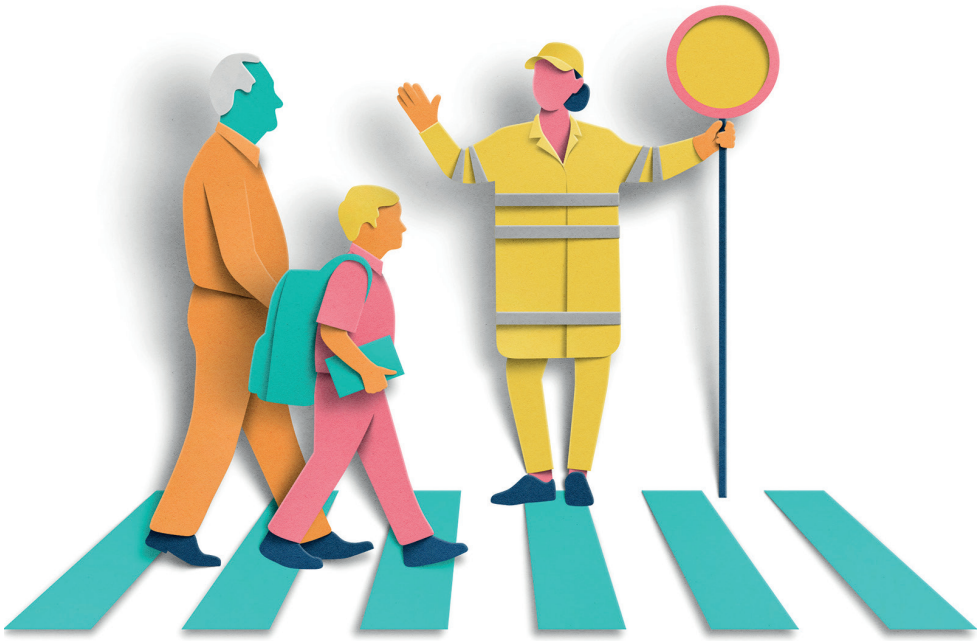
| | | |
|---|---|---|
| Telephone Preference Service **0345 070 0707** | | **www.tpsonline.org.uk** |
| Trading Standards | | **www.gov.uk/find-local-trading-standards-office** |
| UK Finance – Take Five to Stop Fraud | | **www.takefive-stopfraud.org.uk/advice/general-advice** |
| Victim support | | **www.gov.uk/get-support-as-a-victim-of-crime** |

Opt out of unsolicited live sales and marketing calls. It's free and quick to register a telephone number.

Report a business to Trading Standards if you think they have broken the law, acted unfairly or if you have been sold something that is unsafe or dangerous.

A national campaign that empowers individuals and businesses across the UK to protect themselves against financial fraud.

Get free support and advice if you've been a victim of crime.



# Stay safe and alert to scams

**Remember:**

- No one should ever ask for your PIN, password or other security details in full.
- No one will ever collect your bank card.
- Legitimate computer firms won't call you to help you fix your computer, unless you've asked them to.
- If it sounds too good to be true, it probably is.
- You shouldn't have to pay anything to claim a prize. If you haven't bought a ticket, you can't win.
- If in doubt, don't reply. Bin it, delete it, or hang up.
- Pushy trader? Just say 'no thank you'.
- Contacted out of the blue? Be suspicious.
- Don't respond to job advertisements that ask for money in advance.
- Don't respond to offers of commission for allowing your account to be used for moving money.
- Good investments aren't secret so you shouldn't be asked to keep quiet about it.
- The police, your bank or your building society will never contact you to tell you that you're part of a fraud investigation. And they won't ask you to move your money to a safe account.

**Don't be embarrassed or suffer in silence – tell others about scams.**





## Contact us

**At a branch**
For details of our opening hours, visit **thecoventry.co.uk**

**Online**
**thecoventry.co.uk**

**By phone**
**0800 121 8899**

**By post**
Oakfield House, PO Box 600, Binley, Coventry CV3 9YR.

Coventry Building Society is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority (www.fca.org.uk) and the Prudential Regulation Authority (firm reference number 150892).

For more information, visit our website **thecoventry.co.uk**, call us on **0800 121 8899** Monday to Friday 8am-7pm or Saturday 9am-2pm, or pop into a branch. Calls to 0800 numbers are free from the UK. You may be charged for calls to all other numbers, please contact your service provider for further details. Calls may be monitored or recorded to help improve our service and as a record of our conversation.

Information correct at time of going to print (September 2025).

07512 09/25

Coventry Building Society.
Principal Office: Coventry House, Harry Weston Road, Binley, Coventry, West Midlands CV3 2TQ.

recycle
When you have finished with this booklet please recycle it