Shred Station's Fraud Awareness Guide

www.shredstation.co.uk

Contents

This Fraud Awareness Guide is for anyone who wants to learn a little more about fraud and the methods modern-day scammers use to exploit innocent victims out of their identities and hard-earned cash.

It will help you know how to spot a scam, learn what types of scams exist, and the tricks scammers will use. Knowing how scams work and what scams are out there is the best way to prevent a scam, especially for our most vulnerable members of society who may not have the know-how to spot scams online.

Spotting a scam

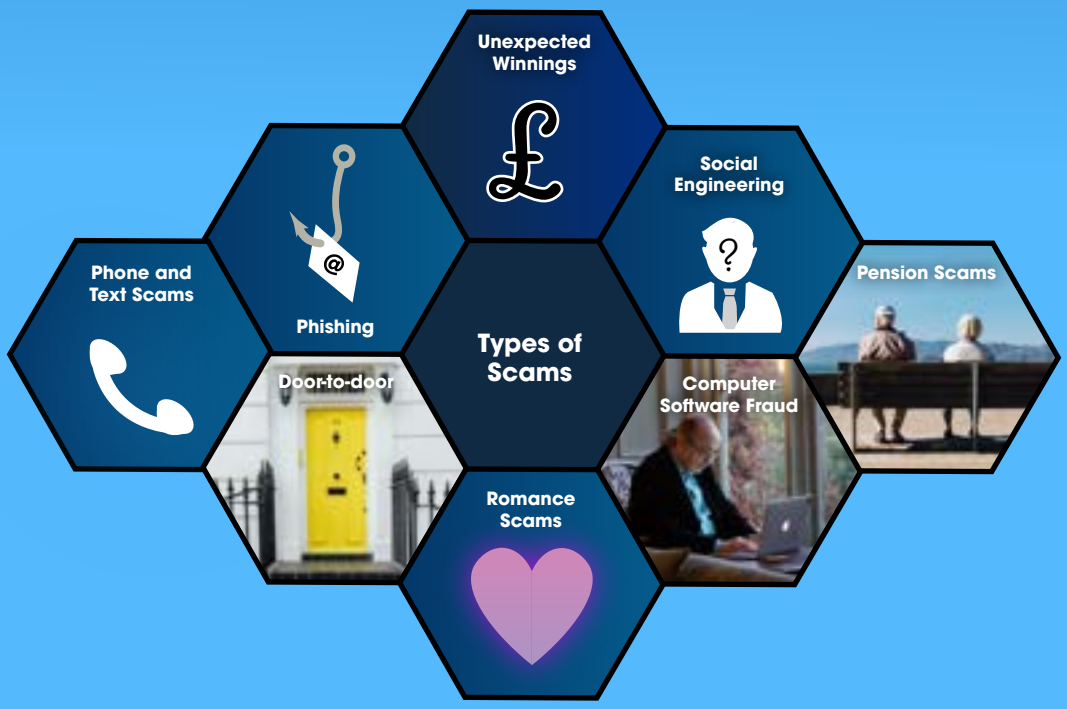
The best way to protect ourselves from scams is to be aware of the type of scams that exist. Once we are familiar with the techniques scammers use, we can start to prepare ourselves to respond to the threat of scams effectively.

There are countless types of scams, and while it isn't possible to cover every type of scam used, scams can be easy to spot once we know the signs to look for.

In this document we'll be covering:

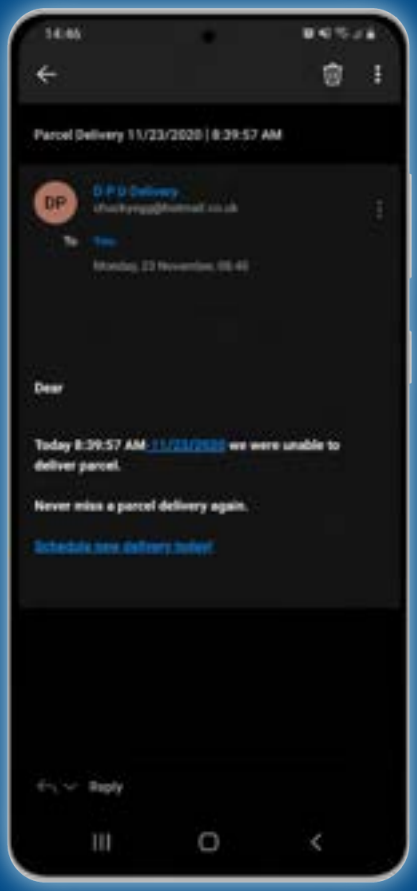
- Phishing emails
- Phone and text scams
- Door-to-door scams
- Romance scams
- Computer software fraud
- Pension scams
- Social engineering
- Unexpected money or winnings scams.

Each of these types of scams can be incredibly sophisticated, and sadly are often targeted towards the more vulnerable members of society. This can include those who live alone, the elderly, teenagers and young people, and even those looking for love.



Please share this guide with those around who you may be more vulnerable or susceptible to fraudulent activities.

SHRED STATION



Phishing emails

Phishing is a crime where fraudsters try to disguise themselves as reputable organisations in order to gain information such as bank details, usernames, passwords, and more.

To the left, we see an example of phishing where the scammer is attempting to disguise themselves as DPD, the well-known parcel delivery company. When we tap on the sender (in blue), we can see that the sender is not DPD at all, but someone with a spam email address: chuckyegg@hotmail.co.uk.

If you were indeed expecting a parcel from DPD on that given day, you may be tempted to click on the link to rearrange a delivery, and this is how these scammers succeed. Phishing emails or texts are sent to the masses with the hopes of reaching a small portion of people likely to click.

Always check the sender details before taking action. We would recommend always going direct to a legitimate business before clicking links in any emails which appear suspicious. Never enter your bank details from a link directly in an email, and do not open any email attachments you were not expecting to receive.

Phone and text scams

There are many types of phone and text scams, and these scams take many different approaches. We'll go through two common phone scams below.

• **Voice of Authority** - Fraudsters will often pretend to be someone they are not, and often this is someone in a position of authority. This may include the police, HMRC, or other government departments. You may have received a phone call from what sounds like a real person, but is really a recording waiting for your response. You may also receive an unexpected phone call which sounds robotic, or even a call that sounds like somebody famous through 'deepfake' technology. If you have any doubts about the authenicity of a person's voice, or if anything sounds off, the best thing to do is hang up the phone.

• **Referrals** - Scammers may call you up saying a friend of yours gave them your contact details to offer you a discount on things like your phone bill, or a free product or service such as a home insulation check. If you ask the caller which friend it was, they'll likely refuse to disclose that information for "data protection reasons". This is a strong indicator that the person on the other end of the line is attempting to scam you, even if it seems like they are trying to do you a favour. Your friend would likely have told you themselves if they passed your details onto a third-party for a great deal. However small, if something is offered to you out of the blue, be aware this could be a ruse to gain access to your personal information.

The same techniques phone scammers use can also be sent via texts asking you to respond to the text message to claim a deal, pay an urgent bill, or enter your details on a linked website. Do not click on any SMS links if you are not expecting the messages beforehand. Also be aware that any texts you receive demanding an urgent response could be from a premium rate number. By responding to these texts, you could end up with hefty charges on your bill, all of which are going straight into the scammer's pocket.

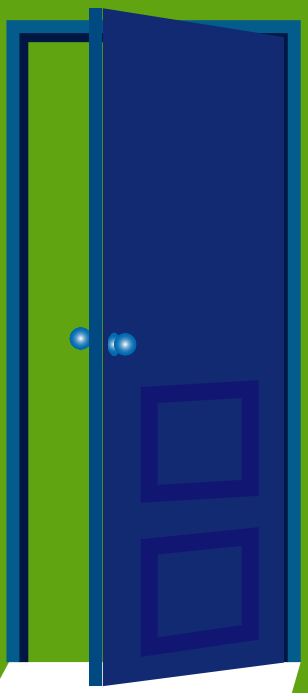
Door - to - door scams

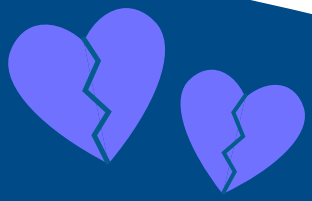
Door-to-door scammers usually operate in the daytime when older people are home. According to National Trading Standards, 85% of door-to-door scam victims are aged 65 and older, so it's important to look out for our elderly neighbours and loved ones in particular.

Most door-to-door scams involve people trying to sell goods or services that you do not need or are of poor quality. Even worse, they may not actually be trying to sell anything at all. They may be trying to get information about the contents of your home, or trying to gain access to steal valuables.

Do not let anyone enter your home unless you are expecting their visit. Even if someone says they are coming to do a meter reading, it is wise to call your utility provider before letting them in. You should also double-check they are in correct uniform and have photo identification.

£18m is lost to doorstep scammers each year. Even more may be lost to crimes that go unreported.Door-to-door scams are so successful because the scammers use intimidation tactics to pressure society's most vulnerable into believing the scams are genuine and their goods or services are needed urgently - e.g. window repairs. This is usually not the case.





Romance scams

Dating fraud or romance scams are elaborate, cruel scams that prey on those seeking companionship, mostly through online dating. Criminals will pose as the "perfect person" online, gain the victim's trust, and convince them that they are in a genuine and loving relationship. Some things to look out for with romance scams are:

- The person will make excuses every time you ask to call, video call, and meet up in real life.
- They will ask a lot of personal questions about you, or try to find answers to your security questions.
- They may portray themselves as living a lavish lifestyle, but suddenly need to borrow money.
- They will put the pressure on you to transfer urgent funds or send parcels on their behalf.
- Their affections become serious very quickly, declaring strong feelings for you without having met.
- They may say they are well educated, but display limited spelling abilities and vocabulary.

Scams of this nature can be very convincing, with criminals even using videos and photos stolen from other people's social media accounts. Using the image search function on search engines, you can see if photos people use online are being used elsewhere. If their photos appear on multiple social media accounts, there's a good chance the images were stolen from someone else.

No matter how long you've been speaking to someone online, do not send them any money or provide them with copies of your personal documents such as passports or driving licences. These items can be used to open bank accounts and take out loans in your name.

Sextortion fraud is another crime to be aware of. This is done in two ways. Either the criminal will attempt to blackmail someone, commonly via email, claiming they have webcam footage of the victim accessing adult content online. These emails will demand money to keep the footage secret. These emails are sent to thousands of potential victims, hoping to scare people into transferring funds. Another way sextortion scams occur is initially through a romance scam. The scammer will solicit risque images from the victim, and then blackmail the victim to keep the images a secret. If someone online threatens to share personal images of you, contact the police immediately. This is a criminal offence and could be punishable by up to 14 years in prison.

Computer software fraud

Computer software fraud is extremely broad, and can come in the form of malicious pop-ups, ransomware, or unsolicited calls from people claiming to be from big tech companies needing to install updates on your computer.

As with door-to-door scams, a large portion of computer software fraud victims are the elderly who may not have the technological know-how to identify when someone is trying to access their files, passwords, or install harmful software on their computer.

To protect yourself from harmful computer software, make sure your computer's antivirus software is up-to-date. Never click on internet pop-ups, be aware of unsolicited calls, and, most importantly, never give anyone remote access to your computer - even if they are saying it's to fix a problem.

Big tech companies such as Microsoft or Apple will **never** phone customers to upgrade their software, so even if someone on the phone is pressuring you to take immediate action about a virus, remember that urgency is a tactic that many scammers use to get people to act on impulse.

Instead of acting on fear, take some time to consider whether the call could be from someone who is trying to access your personal details. Hang up the phone, do not allow remote access, and do not click on any pop-ups. If you are worried about a virus, run your antivirus software or take your computer to a local professional, friend, or relative who can help.

Pension scams

Since pension freedoms were introduced in 2015, retirees can access funds from their pension pots, which can amount to a substantial sum. Unfortunately, scammers have used this as a way to defraud pensioners out of their life savings through complex pension scams.

The Pensions Regulator suggests that the warning signs of a pension scam can include:

- Receiving an unsolicited call, letter, email, or visit from someone offering a 'free pension review', 'pension liberation', or a 'loophole' to get better returns on pension savings.

- Being approached by someone using high-pressure sales tactics insisting their time-limited offers will guarantee a large return on investment - e.g. stocks or shares that are increasing in value.

- Being asked to make unusual, high-risk, overseas or unregulated investments. While this might sound like you are getting a lucrative deal, you could actually be opting in to an investment with no consumer protections.

Action Fraud's complaint data shows that the average loss from pension scams exceeds £30,000 per instance, totalling to over £17m per year in the UK. Data also shows that pension savers could be 9x more likely to accept "advice" from someone online than they would be from a stranger in person. This makes it even more important to talk to society's older generations about online safety and how to recognise when someone online may not have their best interests at heart.

Social engineering

Social engineering is a form of scam and psychological manipulation where the scammer will pretend to be someone you know, like your boss, a colleague high up in your business, a family member, or even a close friend.

While impersonating someone you know with emotional or power influence, the scammer will ask you to make urgent payments or purchases or ask you to disclose confidential information that they can use to gain access to your online accounts and steal your identity.

An example of social engineering could be an email from someone with the same name as your company's CEO, asking you to pay an urgent invoice or purchase emergency gift cards for them. The social pressure of being asked to do an urgent task by a C-suite member of staff may be enough to make you act without questioning its authenticity or origin. Social engineering is also common on WhatsApp. If you receive a message from an unknown number claiming to be a loved one needing money, contact your loved one through the number you know first.

Always make sure, when receiving urgent requests from anyone in your life, to double-check the details the sender is using. If something seems off, check with the person who appears to be sending the message via a different route to check if the request is genuine.

Unexpected money or winnings

Unexpected money scams come in many forms, some more believable than others. These include:

• **Inheritance Scams** - This is where you will receive a message or call from someone claiming you're due an unexpected inheritance from a distant relative or wealthy benefactor. The scammer will likely pretend to be a solicitor, banker or other official, and say they just need a small fee to issue the funds.

• **Rebate Scams -** Rebate scams are attempts to convince you that you're entitled to a rebate or a reimbursement from the government or your bank, but first need to pay an admin fee. In reality, there is no rebate. HMRC will never send notifications of a tax rebate by email or text message.

• **Advance Fee Scams -** With these scams, you'll be asked to provide a smaller sum of money in exchange for a greater reward down the line. For example, you may be asked to pay £300 to cover a courier service to receive £10,000 in cash delivered to your home. The scammers will pressure you to pay these fees up front, saying if you don't pay the fee, you will lose the big prize.

These scams normally appear in the form of mass messages. If you receive a message out of the blue claiming you're due unexpected funds, be cautious. Do not send money to anyone for a bigger prize. Use search engines to search for the exact words used in any messages you receive, as these scams may have already been identified online. Also, keep your social media profiles and posts private. Scammers use social profiles to learn things about victims to make their scams more convincing.

Preventing a scam

The best way to protect yourself from a scam is to be aware of the types of scams that exist and the telltale signs that someone, or even multiple people, are trying to scam you out of your hard-earned assets or even your identity!

These five golden rules will help you to prevent most scams, and give you the tools to recognise when someone else's behaviour may be suspicious.

Five *golden* rules

1 Be suspicious - especially with urgent "problems" or prizes!

If someone is contacting you out of the blue pushing you to share your personal information, you are right to be suspicious. Likewise, if someone is contacting you with an offer or prize that seems too good to be true, it likely is. Listen to your gut feeling, and don't respond to the scammer. If the scam concerns a financial matter, such as letters demanding urgent payments for utilities, contact your provider directly on the number listed on their official website. Don't click on links or reply to the messages.

2 Don't give away personal information.

Scammers are often very good at manipulating vulnerable victims and will pull out all of the stops to get you to part with your personal information or bank details. Scammers can even pose as your friend on social media, so be extremely cautious with who you "help out" too. Personal information about yourself can be used to open bank accounts and even take out loans in your name. The best option is to keep your personal information closely guarded at all times, and that includes on social media.

3 Beware of bad spellers!

Scammers often use incorrect grammar and make lots of spelling mistakes. If you are noticing glaring grammatical or spelling errors in letters, emails or texts from what appears to be a reputable business, that's a red flag. Reputable companies will almost always proofread their marketing communications before sending them, so that's one telltale sign for whether or not the communication you've received is legitimate or if it is a scam. Also be sure to double-check the address or email address the scammer is contacting you from. More often than not, it will be quite easy to tell that their contact details are bogus.

4 Take your time.

If you get a call out of the blue from someone saying you need to take urgent action, particularly in regards to a financial matter, that is a concern. Scammers will often try to hurry their victims into making a quick decision through fear. Take your time; consider if there is a possibility this could be a scam. If anything at all makes you uncomfortable, seek advice directly from your family and friends, your bank, from ActionFraud, or from your nearest Citizens Advice Bureau. It's also worth doing an internet search using the names, emails, or exact wording of any communications you receive. Scammers approach a lot of people, so bogus messages will appear on internet forums that identify scams.

5 Be aware of any unusual payment requests.

Be wary if a friend, family member, acquaintance, colleague, or unknown person approaches you asking for an unusual payment request. If someone asks you to send them money or make a purchase in preloaded cards, vouchers, bitcoin or other cryptocurrency, that is a huge red flag. Cryptocurrency is untraceable so sophisticated criminals will use these methods to steal large sums of money. Through hacking, they can also pretend to be your friends and family members, so don't believe everything you read on texts or through other online messaging platforms. Do not transfer money or goods to any person you don't completely trust. This could be a money laundering scam, and your involvement could constitute a criminal offence.

What to do if you're a victim of a scam

If you suspect you may be a victim of a fraudulent activity, here are the steps you should immediately take:

1) Write down everything you know about the scam.

Make note of who you've been in contact with. Include any names, numbers, or addresses the scammer has mentioned. Make note of any information you've shared and how you've shared it, e.g. they may have seen your online banking login over screenshare apps. Note down whether you've paid any money, and how this money was paid.

2) Call 101 and let them know all of the information you've collected.

This is especially important if the scammer is in your area and if you've transferred money to the scammer in the last 24 hours.

3) Report the scam to Citizens Advice and Action Fraud.

Your local Citizens Advice Bureau or Citizens Advice online will be able to share details of the scam with Trading Standards, who have the power to take legal action against scammers. It's also vital to contact Action Fraud. Action Fraud is the UK's national reporting centre for fraud, and they will give you a crime reference number which will be useful if you need to tell your bank you've been the victim of a scam. Action Fraud also have the power to involve the National Fraud Intelligence Bureau to investigate scams if there is sufficient evidence.

4) Call your bank.

Let your bank know if you suspect your information has been compromised. Call them on the number listed on their website or on the back of your card. You may need to cancel your cards, and change your online banking security questions and passwords. Your bank will let you know how to do this.

Talk about your experience with someone you trust.

There are, of course, secondary impacts of falling victim to a scam. Many victims feel an incredible amount of shame, anger, and even loneliness. This is especially the case with romance scams.

If you're the victim of a scam, it's important to tell someone close to you who you can trust, and talk through your feelings. Try to remember that it isn't shameful to fall for a scam. In fact, it can often be the sign of someone trusting who wants to see the best in people - two very positive traits to have.

Remember that scammers do not discriminate, and more often than not, they work at volume. The wider their web of lies, the more victims they can trap. Being targeted by scammers doesn't reflect who you are, and most of the time it isn't a personal attack. While it may feel personal, it is often just a case of bad luck, being in the wrong place at the wrong time, or putting your trust in the wrong person.

If you'd rather not talk to someone you know, you can get free, confidential help by calling Victim Support on 0808 168 9111.

Now you are aware of the types of scams that exist, you can move forward, using this knowledge to protect yourself and others around you from falling victim to a scam.

Protecting those around us

Fraudsters deliberately target older and more vulnerable people. According to a report by Age UK, 43% of people aged 65+ say they believe they have been the target of a scam. Similarly, 29% of young people aged 13-21 in England and Wales have been victims of fraud.

To protect those around us, it's important to have discussions about the different types of scams that exist and how to avoid falling victim to these scams. People can often feel shame after being scammed, and may even try to hide it from their loved ones. Here are some warning signs to look out for:

- They seem shorter of money than usual or their spending habits have changed.
- They are receiving a lot of phone calls or "urgent" letters.
- They seem sad, anxious or irritable for no obvious reason.
- They seem to be extra cautious when opening the door.
- There is evidence that they made large cash withdrawals but there doesn't seem to be evidence of any large purchases.

If you suspect someone in your life is the victim of a scam, it can be difficult to approach the situation. They may believe the scam is genuine and they are helping a friend or are making a wise investment. Try to get them to see the situation from another viewpoint, for instance, how they would feel if you or their best friend were approached by a stranger trying to access their funds.

If the person you believe may be a victim of a scam is receiving care from their local authority, whether that's a care visit once a week or permanent assistance, it's also worth reporting your concerns to their local Safeguarding team. Social workers can investigate situations where a person may be at risk of financial abuse, including scams. You can find your local authority's website by visiting gov.uk.

Another place to access free guides and fact sheets is the Action Fraud website: actionfraud.police.uk.

Conversations with victims of fraud

It takes a lot of courage to speak out about being the victim of any crime, but doing so can help raise awareness of these crimes and the warning signs to look out for. We spoke with three people willing to share their stories in hopes of preventing others from becoming victims.

Please note, the names of these victims have been changed to protect their privacy.

Ellen's story, aged 26.

"I received a message from a work friend on social media. They said they were having trouble transferring money between their bank accounts and asked if they could transfer the money to me, and I'd transfer the money back out to their other account. I agreed, thinking I was helping a friend. It was a large sum of money, so they asked me to prove I was sending it by installing a screen sharing app on my phone. I didn't think that was unreasonable, and they seemed desperate for the money. Before I received the funds, they asked me to take a picture on my phone of my driving licence for further proof it was me. Shortly afterwards, the money appeared in my account. Little did I know, they had used my ID and online banking details to take out loans in my name for £32,000. The money I'd received was technically mine. Instead of transferring the money to another account, they pressured me to log into a bitcoin wallet and use the money to buy bitcoin instead. Then they went quiet. Later that afternoon, I saw the friend post that they'd been hacked. I immediately had a horrible sinking feeling when I realised what had happened. I called my bank, the police, and Action Fraud. It was terrifying and horrible and left me feeling low for months. I was very lucky that I did eventually have those loans voided by the bank, but I couldn't access my bank account for a month afterwards, having to rely on my parents and boyfriend for everything. It has really impacted my self-esteem."

Bill's story, aged 81.

"A young man knocked on the door one day, looking very smart in a suit and tie. He told me that quite a few houses in the area had poorly insulated roofs, and it could be costing us a lot of money in heating bills. He seemed nice and offered a free survey of the roof. A week or so after, two men went into the loft for half an hour or so, and they told me the roof was leaking a lot of heat. They said they could improve insulation using spray foam, and it would cost £600. They didn't pressure us into getting the job done and seemed like they were trustworthy. We did book the work in. We can't get into the loft ourselves these days, but they showed us pictures and it looked like they had done a good job, but when our son went up to look in the loft months later, he said there was foam all over our things, and it looked like some of our boxes had been opened and gone through. We aren't sure if anything was taken but it has made us very wary of people knocking."

Lily's story, aged 24.

"A friend I met on a childhood family holiday sent me a message just after I graduated from university, asking if I'd be interested in a job. He owned an investment company and was always posting photos of himself in nice cars, wearing nice watches, eating at fancy restaurants etc. He said a new office was opening, and because it was a long way from home, he would sort me out with a nice flat and company car. He said I'd be earning £40k plus commission - a huge amount for a new graduate. All I would have to do is prove I could get investors. If I could get £1000 ready by the next week, the job was mine. I found some people willing to invest, but something just felt too good to be true. Thankfully I listened to my gut, and secretly visited the "office" he had in London. It didn't exist. I read the contracts he sent across and they were full of spelling mistakes. I hadn't taken any money from people who had agreed to invest, thankfully. I don't want to think about what situation I'd be in if I had. I confronted him, and was met with a torrent of verbal abuse. A couple of years later I googled his name and he was serving time for fraud. He'd been scamming dozens of young women, his fake online lifestyle a big factor in his success. Just shows you can't believe everything you see online."

Handling data securely

In addition to the scams we've already mentioned, physical information is also a huge area of risk when it comes to fraud and identity theft. Personal documentation in the wrong hands could expose enough of your details to create false identities. Once a false identity is made, it can be used to take out loans, sign up for direct debits, acquire medicines in your name, take out insurance policies, and much more. The best way to ensure your physical documents aren't exposing you to the risks of identity theft is to destroy anything you no longer need. This goes for letters, bank statements, old documents, diaries, bank cards, ID cards, hard drives, USB devices, and anything else that stores personal information.

Here are some quick tips on how to avoid your confidential materials getting into the wrong hands.

- **Be cautious about what paperwork you put in the recycling bin.**

Bin raiding is a common practice fraudsters use whereby they take documents out of bins, using these documents to commit identity theft. Make sure any documents you put in your general waste bin or recycling bin do not contain any personal information, including your full name and address or bank details. Ripping these documents into smaller pieces is not a deterrent for these criminals, so it's best to be highly cautious when disposing of any paperwork.

- **Keep confidential paperwork and electronic storage devices locked away and out of sight from any windows or doors.**

Criminals often stake out properties for days before burglaries, considering things like when people come and go from an address, when the home is empty, and what valuables they can see through the windows of the home to see if the risk is worth the reward. You can protect yourself by installing home security, keeping all doors and windows locked at night and when the house is empty, and by keeping paperwork and valuables out of sight of windows and doors.

- **Do not share confidential information with anyone unless essential or for the purposes of destruction.**

There is no reason anyone should ask you for confidential information such as proof of ID or financial information unexpectedly.

You should never share your PIN number with anyone - not even your bank. Never log into any accounts or online banking where someone could see your password. This includes in person and online, for instance while sharing your screen or receiving remote support on your PC.

Destroying data securely

When you no longer need your confidential materials, you should destroy them to avoid them falling into the wrong hands. Using a fully-accredited shredding service is the best way to do this and is much more secure than using a home office shredder. Home office shredders often shred documents into long strips, which are easy to reassemble. With home shredding, your fragments may also just end up outside in an unlocked bin, ready for the taking.

When you use a shredding service, your documents will be cross-cut in industrial shredders operated by security-vetted personnel. This method tears the documents into small pieces. Not only that, the fragments of your documents will be mixed in with the fragments of hundreds of thousands of other documents, never accessible to the public.

At Shred Station, we want our customers to feel confident about data destruction. We give our customers this confidence by having high security measures in place every step of the way. We also do our best to minimise our environmental impacts, cause minimal interruption to our customers, provide industry-leading customer service, and continuously innovate. All of this combined means we can offer a service to suit everyone.

1

Schedule Collection

Lockable bins or bags are supplied for regular collections, or alternatively we offer a one-off collection of bagged, boxed or palletised material.

Our Journey Begins

You'll receive an email containing a live service tracking link. You can track our driver's route position throughout the day. You'll also receive a second email when you are the next job on our driver's route.

2

Security Vetted Staff

Our uniformed and BS7858 security-vetted staff will transfer your documents and material into a secure vehicle.

3

4

Off-site Shredding

Secure vehicle is sealed for transportation and material is shredded on arrival at our secure depot.

OR

On-Site Shredding

Once behind secure doors, our operatives place the data directly into the shredder located on board.

5

Certificate of Destruction & WTN

A certificate of destruction and **waste transfer note** are issued, confirming the safe destruction of your data in compliance with European standards.

Recycling

Shredded paper is baled and sent to UK mills for recycling. Other material is recycled where possible and non-recycleables are sent to Energy from Waste. Nothing we shred goes to landfill.

6