1ST EDITION

THE LITTLE BOOK OF BIG SCAMS

POLICE SCOTLAND
Keeping people safe

NPCC
National Police Chiefs' Council

Scottish Business Resilience Centre
Creating a secure Scotland for business to flourish in

Royal Bank of Scotland

BIG SCAMS

Dear Customers,

At Royal Bank of Scotland we are committed to helping our customers and communities protect themselves from fraud and the fear of fraud.

We believe that prevention through education is key and so we're delighted to be working with Police Scotland to bring you this informative guide.

At Royal Bank we use sophisticated techniques to identify fraud, spot suspicious activity and help protect our customers. We work with Friends Against Scams, a National Trading Standard ScamsTeam initiative that provides our colleagues with the knowledge to help them empower communities and take a stand against scams.

On our website rbs.co.uk you'll find additional information about keeping your personal details safe. You'll also be able to download some software to help protect you online.

Our colleagues are fully trained to support customers who have been or think they might have been victims of fraud. So no matter how trivial you think your query or concern might be you should never be afraid to ask – we are here to help.

Jane Howard
Managing Director, Personal Banking

BIG SCAMS

Scottish Business Resilience Centre
Creating a secure Scotland for business to flourish in

Mandy Haeburn-Little
Chief Executive
Scottish Business Resilience Centre

We all want to be trusting and, equally, we all want to keep any money that we or our families may have, safe. In today's increasingly digital society, the reality is that strangers can become part of your inner circle with a single click of a button. More than 50% of Scottish people use platforms such as Facebook and LinkedIn to build up business and personal connections and these are vital to those of us in business as well as helping us to keep in touch with family and friends – they help us to source information, share knowledge and even find new employment.

However, the reality is that this same digital society can at times open us all up to the cyber criminal who may deliberately take advantage of your trusting nature online to log onto your account using fake profiles. In this way they can source private information that can be damaging to both you and your employer or indeed to your friends and family.

Research has revealed that an increasing number of Scottish businesses and individuals are being targeted by scammers who trawl social networking sites to steal personal data. With this data it is very easy for the cyber criminal to raid a company's personal files, sensitive data and even its finances. There's a misconception that cyber criminals use smart, developed technology to steal information. The reality is that many of them use social media in the same way as billions of other regular users. The difference is all they want to do is harvest information about you. You can change that. That is the good news.

All of us who are social media users need to ensure both personal and business accounts have strict privacy settings in place. The nature of social media is to be personable and open but remember that not everyone has good intentions. We want you to enjoy being online and we want you to be safe.

CONTENTS

PAGE

POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

Chief Superintendent John McKenzie
Safer Communities, Police Scotland.

Police Scotland together with our partners Royal Bank of Scotland and the Scottish Business Resilience Centre are pleased to bring you the latest Little Book of Big Scams reproduced with the kind permission of the Metropolitan Police Service's FALCON Protect Team. In serving an ever changing Scotland, we in Police Scotland, with community partners, seek to improve the safety and wellbeing of people, places and communities in Scotland.
Our commitment is to prevent acquisitive crime and tackle online fraud and in doing so reduce the harm it causes to our communities.

This booklet highlights the most current and popular scams and frauds committed in Scotland where often those most vulnerable are victims to malicious criminal activity. The world is changing and with the ever increasing use of technology, the individual needs to be increasingly aware of the latest scams and frauds committed in both the online "virtual" world as in the more traditional "real" world. This booklet aims to increase awareness and provide bespoke crime prevention advice to help you in not falling victim to the ever increasing variety and sophistication of scams.

We have witnessed the growth of online crime, scams and frauds. Whether by cold calls or social engineering, online shopping or insecure Wi-Fi, criminals may seek to fraudulently steal your money or obtain important information which personally identifies you and 'steal' your identity to commit fraud. All kinds of personal information can be of use to criminals including your name, address, national insurance number, credit card number or any other financial account information.

We hope that this booklet will help increase your awareness of potential scams and avoid any financial loss. Please share this information with you family and visit http://www.scotland.police.uk/keep-safe/ for further information on guarding yourself against scams.

We hope you can use the following information to identify these crimes and avoid losing money or your valuable personal information. If you are a victim of crime, please report to Police Scotland by telephoning 101 or at your nearest station.

BIG SCAMS

TAKE FIVE

Take Five to Stop Fraud is a national campaign from Financial Fraud Action UK and the UK Government, backed by the banking industry. It's about taking that moment to pause and think before you respond to any text, email or phone call asking you to share any personal or financial details.

If you suspect someone is after your money, take five and confidently challenge them with this simple phrase:

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

Follow these tips to help you protect yourself from financial fraud:

Requests to move money:

A genuine bank or organisation will never contact you out of the blue to ask for your PIN, full password or to move money to another account. Only give out your personal or financial details to use a service that you have given your consent to, that you trust and that you are expecting to be contacted by.

Clicking on links/files:

Don't be tricked into giving a fraudster access to your personal or financial details. Never automatically click on a link in an unexpected email or text.

Personal information:

Always question uninvited approaches in case it's a scam. Instead, contact the company directly using a known email or phone number.

Find out more at takefive-stopfraud.org.uk

BIG SCAMS

ONLINE CRIME

Most people now have access to the internet. We use our home computers, phones and other devices to shop or bank online, contact our friends and relatives, along with numerous other tasks. With all the convenience the internet brings, it is important to be aware of potential online risks.

Almost all frauds now use computers or technology in some way. There are many criminals who take advantage of the anonymity of the online world to deceive, hack and steal.

There are a number of ways cyber criminals can attack you and your device. They may search the internet to find insecure devices, send an email containing malicious software or even set up fake websites.

This doesn't mean we shouldn't use the internet. A few simple security measures can reduce your chances of becoming a victim. The 'Little Book of Big Scams' provides guidance on some of these crimes, further detailed information on cyber crime can be found within 'Little Book of Cyber Scams'.

Available at:
www.scotland.police.uk/keep-safe/

- ⚠ Be wary about the personal information you post online, ensure you check your privacy settings on social media sites.
- ⚠ Ensure your password is strong, using three random words eg ‘boatfishtulip’.
- ⚠ Have a strong separate password for your email account, if available set up 2 factor authentication.
- ⚠ Use anti-virus software on all devices and update regularly.
- ⚠ Back up your important data regularly using an external device or cloud storage service.
- ⚠ Secure your tablet or smartphone with a screen lock.

BIG SCAMS

WI-FI HOTSPOTS

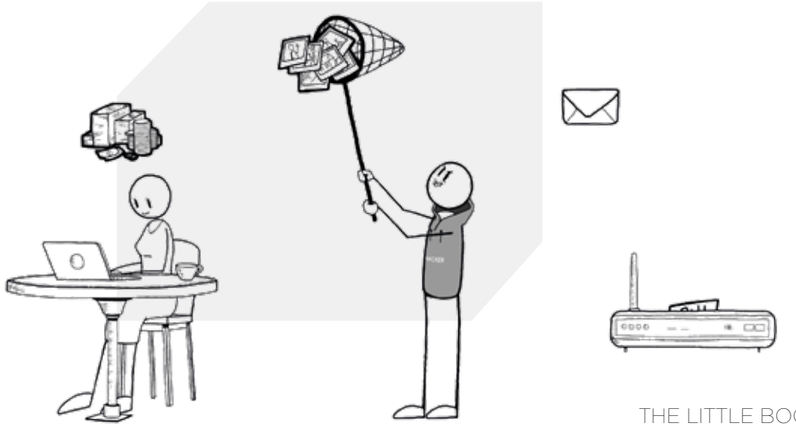
Publicly available Wi-Fi connections or ‘hot spots’ are great for accessing the internet when you are not at home or work. Not all Wi-Fi connections are secure and they can be used by cyber criminals to intercept your data. If you connect to a publicly available Wi-Fi you don’t know who else is on the network. Your data could be intercepted.

Sniffing

Be aware that even if you log into your emails using an app without typing in the password, the phone will still send your password over the Wi-Fi and could be intercepted. If you use automated passwords and do not enter your username and password manually, these details can still be intercepted.

Evil Access Points

Cyber criminals can set up their own Wi-Fi hot spots in an attempt to get you to connect to them. They broadcast a Wi-Fi connection usually calling it something like ‘free_wifi’ or ‘coffee_shop_wifi’. If you connect to this Wi-Fi the criminal can capture any data you are sending.



How to protect yourself

- ⚠ Don't use public Wi-Fi for online banking, accessing e-mails or anything involving sensitive information. When doing this in public use your 3G, 4G or 5G connection. Data passed over these connections is always encrypted.
- ⚠ Make sure you are connecting to a trusted Wi-Fi hotspot, operated by the venue you are at, ask staff if in any doubt.
- ⚠ Use a Virtual Private Network (VPN) when connecting to public Wi-Fi. All your data will be encrypted and so if it is intercepted it won't be readable. VPNs can be downloaded onto devices as an app.

REMEMBER

Not all Wi-Fi hotspots are secure.

CAUTION

Cyber criminals can capture data on an insecure Wi-Fi network.

THINK

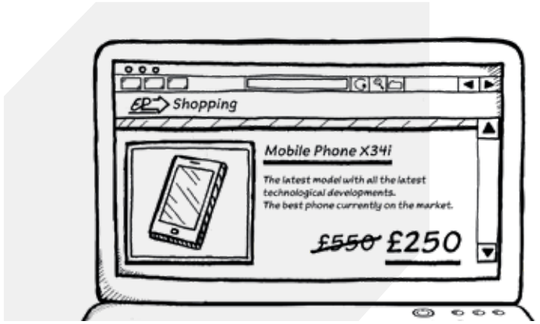
Do I need to use a VPN or switch to a 3G, 4G or 5G connection?

BIG SCAMS ONLINE SHOPPING AND AUCTION SITES

Online shopping can save you time, effort and money. Millions of people use websites such as eBay and AutoTrader, to buy new or second hand goods for competitive prices. These sites give you the opportunity to purchase a huge choice of goods from all over the world. However, amongst the genuine buyers and sellers on these sites are criminals who use the anonymity of the internet to offer goods for sale they do not have, or are fake.

In the majority of transactions, the buyer and seller never meet. Which means when making a purchase or sale on them, you are reliant on the security measures of the site.

Fraudsters will advertise an item for sale, frequently at a bargain price compared to other listings of a similar type. They may have pictures of the item so it appears to be a genuine sale.



Criminals regularly encourage buyers to move away from the website to complete the transactions and may offer a further discount for doing so. Many websites offer users the opportunity to pay via a recognised, secure 3rd party payment services e.g. Paypal, Android Pay or Apple Pay. Read the website's advice and stick to this. Fraudsters might be insistent you pay via Bank Transfer instead. By communicating and paying away from the website, contrary to their policies, you risk losing any protection you had.

Fraudsters may also email or contact you if you have 'bid' on an item but not been successful in winning the auction. They will claim that the winning bidder pulled out or didn't have the funds and offer you the chance to buy the item. Once you agree they will either provide bank details or even insist payment is made via a 3rd party payment service for mutual protection. Once you agree they 'arrange' this. You then receive a very legitimate looking email which appears to be from the website or a 3rd party payment service directing you how to make payment. Some are very sophisticated, even having 'Live Chat' functions you can use to speak to a sales advisor! Unfortunately, you are again communicating to the fraudster, so beware!

In both these scenarios, once the payment is made the 'seller' often does not send the item, either not replying to communications or making excuses as to why they haven't sent goods.

Some criminals send counterfeit goods instead of the genuine items advertised. Again, you may struggle to receive any compensation or resolution to this problem from the legitimate website, which could be against their policies.

Fraudsters also use e-commerce websites to pose as 'buyers.' If you have an item for sale, they may contact you and arrange to purchase this. It is common for criminals to confirm that payment has been made. Before posting any item login to your account via your normal method, (not a link on the email received) to check that you have received the money.

You must also be careful what address you send items to. Fraudsters may ask you to send items to a different address, maybe they need it sent to their work address or a friend or family member. If you send the item to an address other than the one registered on the user account, you may not be provided any protection from the website or payment service.

How to protect yourself

- ⚠ Stay on site!
- ⚠ Be wary of any too good to be true offers.
- ⚠ Read the consumer advice on any website you are using to make a purchase. Use the recommended payment method, or you may not be refunded for any losses to fraud.
- ⚠ Research seller/buyer and any bidding history.
- ⚠ Don't be convinced by profile pictures, they may have been taken from somewhere else on the internet. You can check photos using a reverse image search on the internet through websites like https://www.tineye.com/ or https://reverse.photos/.
- ⚠ Be suspicious of any requests to pay by bank transfer or virtual currency instead of the websites recommended payment methods.
- ⚠ Never buy a vehicle without seeing in person. Ask to see the relevant documentation for that vehicle, to ensure the seller has ownership.
- ⚠ If you are selling online be wary of any emails stating funds have been sent. Login to your account via normal route (not via link in email) to check this.

REMEMBER

Stay on site.

CAUTION

Be wary of paying by bank transfer or virtual currency.

THINK

Why is this item so cheap? Is it a scam?

BIG SCAMS

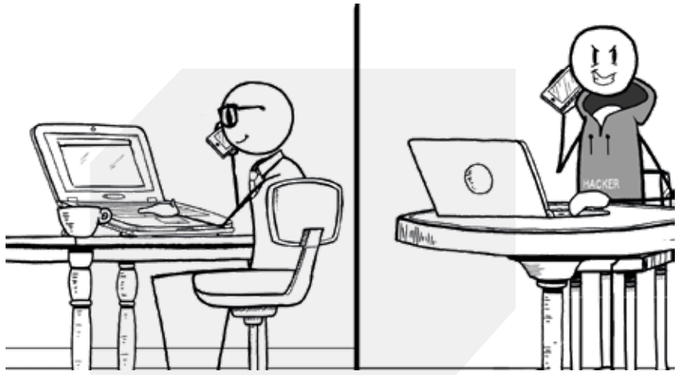
COMPUTER SOFTWARE SERVICE FRAUD

Criminals may cold call you claiming there are problems with your computer and they can help you to solve them. They often use the names of well-known companies such as Microsoft, Apple or your broadband provider to sound more legitimate.

The criminals will ask you to complete a number of actions on your computer, they may even be able to demonstrate an 'error'. They may instruct you to download what is known as a 'Remote Access Tool'. This gives the criminal access to everything on your computer. They can access and copy your data, or download malware on to your computer to monitor what you do in the future.

Fraudsters can even access your online banking, and transfer money between your accounts.

You may also be asked to pay for the 'assistance' you have been given. This could be a one-off payment or an ongoing direct debit over many months/years. If you do provide payment details these may be used to commit further fraud against you.



How to protect yourself

- ⚠ A genuine computer service company will never call you out of the blue regarding issues with your computer. If you receive a call like this hang up straight away.
- ⚠ Never allow anyone to remotely access your computer.
- ⚠ If you are having issues with your computer, contact the retailer you purchased it from regarding service and repair. If you are having issues with your internet speed or service, contact your service provider for advice or support.
- ⚠ Most broadband providers offer a free and easy test to measure the speed of your broadband service.

REMEMBER

Genuine computer service companies don't make these calls.

CAUTION

Don't let anyone remotely access your computer.

THINK

Why are they calling me, there didn't seem to be a problem? How do I know they are genuine?

BIG SCAMS

ROMANCE AND DATING FRAUD

Dating online is now one of the most popular ways for new couples to meet, with millions of people finding new relationships, romance and love this way. Unfortunately, amongst the genuine profiles are fake profiles set up by fraudsters. They are after your money, not your love. They are masters of manipulation, playing on your good nature and emotions to ultimately steal your money.

Criminals will build a relationship with online members, quickly asking to move communication off the dating website. This is so they can continue their contact with you, even if their profile is identified by the site as fraudulent and deleted.

Fraudsters are often very flattering, appearing really interested in you within a short space of time. However, they will use a range of excuses as to why they can't meet in person, such as they are stuck overseas, have a family emergency or an issue with their business. They then start asking for money to help with their problems, assuring you they will pay it back as soon as they can. The fraudster may claim to be desperate to meet you as soon as this obstacle is overcome. This is all a scam and their true intention is to take as much money from you as they can.

How to protect yourself

⚠ Stay on site, keep all communication on the dating website you are using.

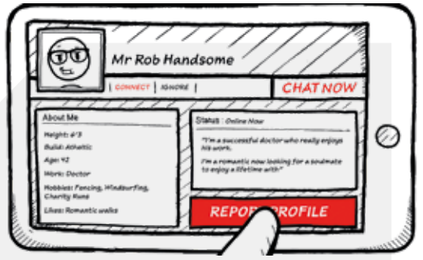
⚠ Don't be convinced by profile pictures, they may have been taken from somewhere else on the internet. You can check photos using a reverse image search on the internet through websites like https://www.tineye.com/ or https://reverse.photos/.

⚠ Do your own research on the person, are they members of any other social networking sites? Can you confirm what they are telling you about themselves, where they work or where they live?

⚠ Never send money to someone you have not met in person and be extremely wary of giving money to someone you have recently met, particularly if you have only recently started a relationship with them.

⚠ Be wary of anyone asking you to receive money on their behalf and transferring it on. They may be using you to launder money.

⚠ Talk to family and friends for advice, even if the other party is asking you to keep the relationship secret.



REMEMBER

Stay on site, never send money to someone you have not met in person, or receive/ transfer money on their behalf

CAUTION

Be wary of making contact outside of the dating website you initially made contact on.

THINK

Why are they so quick to declare their love for me? How do I know they are telling me the truth?

BIG SCAMS

RECRUITMENT FRAUD

WRITTEN WITH SAFER-JOBS AND THE DISCLOSURE BARING SERVICE (DBS)

Most people apply for a number of different jobs throughout their working lives. As technology advances, so do the techniques fraudsters use to exploit job seekers during this process.

The majority of these frauds involve the recruiter demanding some kind of payment or fee for DBS or Disclosure Scotland checks, training, certification or work permits. The job advert which has attracted applicants is often fake and the recruiter stops communication once payment is received... or asks for more!

Information provided to fraudsters by 'applicants' can also be used by criminals to open up bank accounts and loans, known as identity theft.

How to Protect Yourself

⚠ Applicants should research the company advertising the role to make sure that the job being applied for exists. You should be suspicious if asked to pay for any fees upfront for security checks, visas or training.

⚠ Never phone the company on a premium rate number for an interview, premium rate phone scams are common. You can end up paying a large amount for every minute you are kept on hold. If you are in any doubt visit www.ofcom.org.uk/phones-telecoms-and-internet/advice-for-consumers or research the number online.

⚠ Never provide personal details such as your bank account, National Insurance number, date of birth, driving licence or utility bill information during an application process or on your CV.

⚠ Do not conduct the whole process online. At some point a job application should lead to a telephone call or face to face interview. Be wary of hiring agents who keep solely to email.

⚠ Do some research, find out about the company that the job is with. Check landline telephone numbers to confirm the job is real. Use social media and similar sources to dig deeper into the organisation to check their reputation.

⚠ If in doubt about a job advert visit www.safer-jobs.com for free advice.

REMEMBER

Your personal information is valuable, protect it.

CAUTION

Do some research to check if the company exists and if they are really advertising the role.

THINK

Why am I being asked to make upfront payments?

BIG SCAMS

HOLIDAY FRAUD

Millions of people book their holiday online. Whilst you can get some fantastic deals fraudsters take advantage of this. They advertise flights, accommodation and other travel services that are not provided or don't exist.

Often, you will only become aware you have been scammed when you arrive at an airport or even worse your destination and find no booking has been made!

The false advertising can be either an entirely fraudulent website or a fraudulent advert posted on a genuine website. Images of the holiday maybe used to make the offer appear authentic, however these could have been copied from anywhere on the internet.

Criminals will often ask you to complete the booking away from the site, even offering a further discount for doing so. They may encourage payment by direct bank transfer rather than third party payment services (e.g. Paypal) as this makes it much harder for you to recover your funds.

Fraudsters may even send 'confirmation' emails to convince you the booking has been made.

How to protect yourself

⚠ Where possible pay for holidays and travel using either a credit card or the third party payment service advised by the website. These can provide you additional financial protection.

⚠ Ensure your booking is covered by a consumer protection scheme such as ABTA (Association of British Travel Agents) and/or ATOL (Air Travel Organiser's Licence). However, their logos can be copied by fraudsters to add credibility to their adverts. Look for the membership number and contact the scheme to confirm if the company you are using is really a member.

⚠ Research any property before you book, look if it is advertised elsewhere or has its own website. Be extremely cautious if the prices are significantly different.

⚠ Don't be convinced by photos, they may have been taken from somewhere else on the internet. You can check photos using a reverse image search on the internet through websites like https://www.tineye.com/ or https://reverse.photos/.

REMEMBER

Always pay by credit card or the third party payment service advised by the website.

CAUTION

Be suspicious of any discount offered for paying by bank transfer, or request to complete the booking offsite.

THINK

Can I trust the advert? How do I know the booking exists?

BIG SCAMS

TICKETING FRAUD

Getting tickets to see your favourite band, football team or theatre production can be extremely difficult as tickets sell out quickly. Fraudsters take advantage of this by offering tickets for sale that do not exist or are fake.

Most event tickets are sold via reputable websites operated by promoters, the event venue or other official agents. Many tickets are also offered for sale on secondary resale sites. Fraudsters set up fake ticket sales websites, place adverts on secondary resale sites or use social media to sell tickets they do not have.

Once you make payments you will either will not receive the tickets, or the tickets you receive are fake or non-transferrable. When you arrive at the venue you will not get in.

Some tickets are not transferable and can only be used by the person who initially purchased them. In many cases unauthorised resale of these tickets is illegal.

How to protect yourself

- ⚠ Buy tickets from the event promoter, venue box office, official agent or a reputable ticket exchange site.
- ⚠ Where possible, pay for tickets using a credit card as this offers additional financial protection.
- ⚠ Be suspicious of requests to pay by bank transfer
- ⚠ Be wary of paying for tickets where you are told someone will meet you at the event with your tickets, they may not arrive.
- ⚠ If the retailer is a member of the Society of Ticket Agents and Retailers (STAR) you are offered additional protection if something goes wrong. If a website shows their logo you can check they are really a member on www.star.org.uk.
- ⚠ For further information on buying tickets safely visit the STAR website.

REMEMBER

The site you are using could be fake.

CAUTION

Use your credit card to pay, this could offer you additional protection.

THINK

How can I check the tickets are real?

BIG SCAMS

ONLINE BANKING AND CARD FRAUD

ONLINE BANKING

The use of online banking or people using banking apps on smartphones and tablets has grown. People use them at home or when they are out and about. To stay safe while banking online you must protect your password and personal details to stop criminals from accessing your accounts. See the following information about using contactless payments and cash machines.

How to protect yourself

- ⚠ Choose, use and protect passwords and memorable words with great care. Watch http://news.met.police.uk/videos/video-clip-passwords-29571 or see https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0 for further advice.
- ⚠ Keep online banking software and banking apps up to date. Always download updates when prompted.
- ⚠ Always log out of your online banking account or banking app when you have finished using it. Closing the app or web page or turning off your device may not be sufficient.
- ⚠ Do not use publicly available Wi-Fi networks for banking. It is very difficult to tell if a hotspot is secure or not, so it is always best not to use it.

For further advice please visit www.sbrcentre.co.uk/ and www.scotland.police.uk/keep-safe/

CONTACTLESS PAYMENT

Contactless payment is an increasingly popular method of payment, with at least one in three card payments in the UK made using contactless technology. There are many myths that exist relating to the security of this payment system. The information below explains this process, which should ease any concerns you have over this payment method and how it works, whilst giving advice on how to use it safely.

Contactless payment uses a wireless chip containing the user's payment card details which is embedded in a mobile phone or on a bank payment card. This enables users to make payments of up to £30 at stores, cafes and other outlets simply by passing their smartphone or contactless card a few centimetres from a suitable card reader.

Some of the security features on this method of payment include the following:

- ⚠ Every contactless card has an in-built security check, which means occasionally you have to enter your PIN number to confirm payment.
- ⚠ You have to be very close to someone for them to illegally scan your card, even then they wouldn't be able to access details such as your security code, or your personal details.

This is the icon for contactless payment

How to protect yourself

- Look through all your bank cards to identify which are contactless.
- Protect your contactless payment cards by investing in special sleeves or wallets. These wallets are lined with an electromagnetic shield, so the data cannot be intercepted by others, or so you accidentally pay for purchases.
- Always monitor your bank statements regularly, to ensure that payments have not been taken from your account without your knowledge or permission.
- If your contactless payment card or contactless enabled smart phone is lost or stolen, report this to your bank immediately and you should be covered for any subsequent losses.

CASH MACHINES

People are targeted at cash machines by criminals who distract users and steal their card or cash. Fraudsters also fit devices to the machines that trap bank cards, copy the card details and record the PIN number. You must be vigilant when taking money out of a cash machine, don't let anyone distract you.

Criminals may try to see your PIN number as you enter it; they may use a hidden camera or stand nearby. They then attempt to get your card.

They might try and make conversation with you when you are withdrawing money to distract you while they or their accomplice takes your card or cash. Criminals have also been known to drop cash on the floor to ask you if it is yours, diverting your attention. They may have fitted a device on the cash machine which clones your card. They could have a device fitted which retains your card. If your card is trapped in a cash machine by a criminal device, you may leave it unattended to report inside the bank or leave. The criminal will then retrieve the device and your card.

Now the criminal has your card (or a copy) and your PIN.

How to protect yourself

- Be wary of anyone approaching you when you are trying to withdraw cash.
- Shield your PIN from criminal cameras or prying eyes. Stand close to the cash machine and cover the keypad with your purse, wallet or spare hand.
- If there appears to be anything unusual about a cash machine, such as signs of tampering do not use it and report your concerns.
- If your card is retained by a cash machine report this immediately to your card issuer while still at or near the machine. Store your card issuer's 24-hour contact number in your mobile phone.

BIG SCAMS

IDENTITY FRAUD

Identity fraud involves the misuse of an individual's personal details to commit crime. Your details are valuable to criminals and can be misused by them, or sold on to others. If your data is obtained by criminals it may be used to obtain credit cards or bank accounts in your name, as well as numerous other financial products.

Criminals can also use your stolen information to gain access to the funds in your bank accounts, savings accounts or pension. Your details can be obtained in a number of ways, from letters or bank statements you throw away, to information stolen from your computer or mobile device.

If you become a victim of identity fraud it may severely affect your credit rating and it can take a significant amount of time to rectify this.

How to protect yourself

- Sign up to a reputable credit rating agency. After doing so you will be notified when a credit check is completed using your details. This can identify if someone is using your details without your knowledge.
- If you start to receive post from a company or organisation you don't know find out why it is being sent to you.
- Be extremely wary of unsolicited phone calls, emails or text messages purporting to be from your bank or your phone provider. Particularly if they are requesting personal information such as dates of birth or passwords.

- Review your bank and credit statements for any suspicious activity.
- Have security software installed on your computer and mobile devices to prevent malicious software being downloaded. Make sure the software is kept up to date as prompted.
- Don't open attachments or click on links in unexpected emails. This can lead to malicious software being downloaded on to your device or your information being harvested from fraudulent websites you are directed to.

REMEMBER

Your personal information is valuable, protect it.

CAUTION

Be wary of anyone asking you for your private information.

THINK

Why am I being asked to give this information? Is it necessary?

BIG SCAMS

COURIER FRAUD

Fraudsters cold call you pretending to be from your bank or from the police. They claim there is an issue with your bank account or request your assistance with an ongoing bank or police investigation. The ultimate aim of this call is to trick you into parting with your money either in person, online, via a money service bureau or in a bank. They may even ask you to buy high value goods, foreign currency or gift cards such as iTunes.

Criminals call you claiming to be from the police or fraud department of your bank. They claim they are conducting an investigation, often saying it involves corrupt bank employees or police and ask for your help or say your account is at risk.

If they manage to convince you, they instruct you to carry out a task which effectively involves you handing over your money. These include:

- ⚠ Asking you to attend your bank branch, withdraw a large sum of money which they will then collect from you for evidence. They may claim the money may be counterfeit, or that it is going to be sent off for forensic or fingerprint analysis.
- ⚠ Asking you to withdraw large amounts of foreign currency, which will similarly be collected by a courier from your home address.
- ⚠ Asking you to provide details over the phone, including typing in your PIN number. Then handing over your cards to a courier sent to your address (often after you have cut them up as instructed).
- ⚠ Asking you to purchase high value items, such as expensive watches to 'clear criminal funds' which will again be collected by a courier.

In all of these cases they will assure you that you will soon be reimbursed.

Fraudsters want to avoid detection, and may give you instructions to achieve this such as:

- ⚠ Informing you it is an undercover operation involving bank/police corruption, so you must not tell bank staff or police anything about the phone call. They may even threaten that you could be arrested if you do!
- ⚠ Give you a cover story to tell bank staff or police, e.g. the money/item is for building works, a holiday or a gift for a relative.

Criminals have now developed their methods to include ones that no longer involve the courier. They may now claim that as a result of the fraud they are investigating **your** bank account, so ask you to transfer your money into a 'safe account'. They will provide you with the account details and may even say this is set up in your name.

How to protect yourself

- Be extremely wary of unsolicited phone calls from your bank or the police. Particularly if they are requesting personal information.
- End the call, call back on a different phone line or on a mobile. If this is not possible, wait at least one minute before calling back. Use either the telephone number on your bank card, go to the bank's website or for the police dial '101'.
- Speak to friends or family before carrying out any actions. Don't trust claims made by cold callers.
- Never hand over your money, bank cards or make purchases following an unexpected call.
- Never share your PIN with anyone.

REMEMBER

Your bank or the police will never ask you for your PIN, bank card, or ask you to withdraw money or buy items on their behalf.

CAUTION

If you receive an unexpected call, hang up, use another phone to call back and confirm identity.

THINK

How do I know they are who they say they are?

BIG SCAMS

DOOR-TO-DOOR FRAUD

Door-to-door scams involve criminals knocking on your door unexpectedly offering products or services. Fraudsters convince you to pay for goods or work which is overpriced, poor quality or is not even carried out! In many cases, this work is not necessary. They may use intimidation and pressure you to make quick decisions, so you agree to their demands.

Criminals may try to convince you that work is urgently required and the price they are charging is fair. They will put pressure on you to have the work done immediately and may ask for payment upfront. Often the work is not completed or if it is, the work is to a poor standard. You may also be overcharged for any work done.

They can use deception to convince you:

- claiming they were working on a neighbours' address and noticed you need work completed and they have left over materials.
- they may inspect areas you can't access e.g. loft or roof and show you photos or videos claiming they are evidence that you need the urgent repairs. Beware of these tactics, these images may not even be your property!
- they may throw water down when you are not looking to indicate you have 'damp'.

They may be insistent you pay in cash immediately or put down a deposit, even offering to take you to the bank to get the money. If you do this, they may continue to find reasons for you to pay more money.

Some callers will be legitimate. Gas, electricity and water companies may visit to read your meters. Charities may visit to ask for donations, council officials may contact you regarding local issues. Always ask for identification, tell them to wait outside whilst you check this by calling the company or speaking to a relative or friend. (Don't use the phone number on the ID card).

How to protect yourself

- ⚠ Always check their identity. If you are not happy about a person's identity, do not let them into your house under any circumstances.
- ⚠ Take time to consider your options and research costs from other providers, if in doubt contact your local Trading Standards.
- ⚠ If you feel pressured by any cold caller, have the confidence to be firm and say no.

REMEMBER

Take time to consider your options. Don't be pressured into making a quick decision.

CAUTION

Never pay upfront for goods or services you have not received.

THINK

Are they a legitimate company? Why haven't they given you a written quote?

BIG SCAMS INVESTMENT FRAUD

Investing in stocks and shares or any other commodity can be a successful way of making money. However, it can also lead to people losing their entire life savings. Fraudsters will persuade you to invest in all kinds of products, offering high rates of return, particularly over longer periods of time, which often do not exist.

Common products that will be offered include binary options, virtual currency, carbon credits, wine, rare metals, gemstones, land and alternative energy. Often, initial investments will yield small returns as an incentive to invest further funds. However, larger investments or cashing out will be met with excuses or a penalty charge. Eventually contact with the fraudster will be impossible and all funds and bogus returns lost.

Fraudsters are organised they may have details of previous investments you have made or shares you have purchased. Knowing this information does not mean they are genuine.

Criminals may direct you to well-presented websites or send you glossy marketing material. These resources do not prove they are a genuine company. Many fraudulent companies have a polished customer image to cover their illegal activities.

It is relatively easy to register a company with Companies House. This does not confirm or endorse they can provide genuine investments. Indeed, emerging investment markets maybe unregulated, making these open to abuse.

Companies may be registered at prestigious addresses, for example Canary Wharf or Mayfair. This does not mean they operate from there. It is an accepted business practice to rent such a virtual office to enhance a business's status. However, fraudsters are also aware this and exploit it.

The fraudster may put pressure on you offering a 'once in a lifetime opportunity' or claim the deal has to be done quickly to maximise profit.

Be wary of companies who offer to 'recover' any funds you have lost to any sort of investment scam. They may be linked to the company who initially defrauded you in the first place and may be targeting you again. This is known as 'recovery fraud'.

How to protect yourself

- ⚠ There are no get rich quick schemes. If it sounds too good to be true, it probably is.
- ⚠ Genuine investment companies will not cold call you. Be extremely wary of anyone who does.
- ⚠ Research what you have been offered and the investment company, speak to Trading Standards if you have concerns.

REMEMBER

Don't be pressured into making a quick decision.

CAUTION

Seek independent financial advice before committing to any investment.

THINK

Why would a legitimate investment company call me out of the blue.

BIG SCAMS SCAM MAIL

Many victims of scam mail, also known as mass market fraud, are drawn in by the thrill of a guaranteed win. You will part with money in order to claim a prize that does not exist. Often, victims of this type of crime are elderly or vulnerable. They are targeted because they may live alone or have access to significant savings or pension funds.

There are numerous types of scam mail, some more obvious than others. Be wary of what you reply to, particularly if you are asked to send money or provide personal information.

The letters may claim you have won a prize draw; competition or lottery you have not even entered. The letters will be personally addressed to you, giving the illusion that you have been specially selected. Your name may appear numerous times within the letter, using words like 'guaranteed winner'.

They will request a fee to small claim your prize. This fee may be advertised as a delivery or administration cost. Fraudsters may also try to obtain your personal details such as bank account or date of birth.

Be wary of letters offering discounted goods or samples. Always check the small print and make sure you are not agreeing to a direct debit without realising.

It only takes a single response to scam mail, to be inundated with more. After this response your details will be added to a 'victim's list' that other fraudsters have access to.

How to protect yourself

- ⚠ You cannot win a competition or lottery you have not entered! If you are asked to pay an upfront fee for such a 'win' do not pay!
- ⚠ If purchase goods in response to a mail offer, make sure you review your bank or credit card statements.
- ⚠ Any doubts, speak to a friend or relative.

REMEMBER

You cannot win a prize if you haven't entered.

CAUTION

Be wary of anyone asking you for your private information.

THINK

Why am I being asked to make upfront payments?

BIG SCAMS

WHAT TO DO IF YOU GET SCAMMED

GET HELP AND REPORT A SCAM

If you think you have uncovered a scam, have been targeted by a scam or fallen victim, there are many authorities you can contact for advice or to make a report.

Reporting crime, including fraud, is important. If you don't tell the authorities, how do they know it has happened and how can they do anything about it? Remember that if you are a victim of a scam or an attempted scam, however minor, there may be hundreds or thousands of others in a similar position. Your information may form part of one big jigsaw and may be vital to completing the picture.

Reporting fraud in Scotland

Report all fraud and cybercrime allegations to Police Scotland by telephone on 101 or to your local police station.

Unless

- ⚠ A crime is in progress or about to be committed.

If this is the case you should contact police directly either by dialing 999 in an emergency, dialing 101 in a non-emergency or visiting your local police station.

If you have any information on any crime and you would prefer not to speak to police, you can call Crimestoppers anonymously on 0800 555 111 or visit www.crimestoppers-uk.org. Crimestoppers is an independent charity.

OTHER CONTACTS

Action on Elder Abuse

Action on Elder Abuse work to protect and prevent the abuse of vulnerable older adults. Their services include a confidential freephone helpline, which provides information, advice and support to victims and others who are concerned about or have witnessed abuse, neglect of financial exploitation and a Peer Support Volunteer Programme to bring older people together to support each other.

Confidential hotline: 080 8808 8141 or visit www.elderabuse.co.uk

Age UK

Age UK is the country's largest charity dedicated to helping everyone make the most of later life. They offer companionship, advice and support to older people who need it most.

Call 0800 169 8787 or visit their website at www.ageuk.org.uk

Alzheimer's Society

A National charity providing advice and support for people affected by dementia.

Call 0300 222 1122 or visit www.alzheimers.org.uk

Association of British Travel Agents (ABTA)

ABTA is the largest travel trade association in the UK with over 1200 members. All ABTA members must follow ABTA's strict code of conduct and if they breach the code they can be fined or have their membership withdrawn. Consumers who book holidays through ABTA members are financially protected in the event of a company failure.

Visit www.abta.com

Citizens Advice Bureau (CAB)

Citizens Advice provides free, confidential and independent advice to help people overcome their problems. They can help with many issues, from money concerns to problems at work, housing to consumer rights.

Call 03444 111444 or visit www.citizensadvice.org.uk

Cifas

UK fraud prevention service CIFAS offers Protective Registration to people who have fallen victim to, or are at risk of, identity theft. This service flags your personal file, so that when Cifas member companies receive an application in your name, they'll conduct extra checks to ensure that the application is genuine.

Visit www.cifas.org.uk

Crimestoppers

Crimestoppers is an independent charity. If you have information on any crime and you would prefer not to speak to police, you can call Crimestoppers on 0800 555 111 or visit www.crimestoppers-uk.org

Companies House

Online, you can obtain details about a company for free, including:

- Company information, eg registered address and date of incorporation
- Current and resigned officers
- Document images
- Mortgage charge data
- Previous company names
- Insolvency information

Visit www.gov.uk/government/organisations/companies-house

Cyber Aware

Cyber Aware provides cyber security advice for small businesses and individuals, such as using strong passwords made up of 'three random words' and always downloading the latest software and app updates, that can help you protect your devices from cyber criminals.

Visit www.cyberaware.gov.uk

Financial Conduct Authority (FCA)

The FCA's aim is to make financial markets work well so that consumers get a fair deal. To do this they regulate the conduct of more than 56,000 businesses who operate within the financial sector. Their work to protect consumers covers a wide range of activities including ensuring that a firm has its customers at the heart of how it does business, giving them appropriate products and services, and putting the customer's financial protection above the company's profits or remuneration.

Call 0800 111 6768 or visit www.fca.org.uk

Get Safe Online

Get Safe Online is the premier source of online safety advice for the general public and small businesses. The advice it provides can help safeguard against fraud and online threats helping to provide a positive experience of the internet. Get Safe Online works closely with Police Scotland, other UK Police forces and law enforcement agencies and industry regulators to provide up to date crime prevention advice and alerts.

Visit www.getsafeonline.org

Disclosure Scotland

Some jobs require standard or enhanced checks, essentially a criminal record check, and it is up to an employer to assess whether a role is suitable for this type of check.

Visit www.mygov.scot/organisations/disclosure-scotland/

Insolvency Service

The Insolvency Service is an executive agency of the Department of Business Innovation and Skills (BIS). They have the power to investigate Limited companies where they have received information that suggests serious corporate abuse. This may include allegations of serious misconduct, fraud, scams or sharp practice.

To complain about a limited company that is still trading call 0300 678 0015 or visit www.gov.uk/government/organisations/insolvency-service

National Cyber Security Centre (NCSC)

The National Cyber Security Centre is part of GCHQ, it provides advice and intends to make the UK the safest place to live and do business online.

Visit www.ncsc.gov.uk

Mail Preference Service

This is a free service enabling UK consumers to stop receiving unsolicited mail by having their home addresses removed from mailing lists. It is actively supported by Royal Mail, trade associations and the Information Commissioner's Office.

To register for the Mail Preference Service call 020 7291 3310 or visit www.mpsonline.org.uk

Online Dating Association (ODA)

The Online Dating Association was set up maintain standards across the industry and reassure users that each member website was working to achieve the highest standards of security for its users. ODA members are required to adhere to the membership codes of practice and are committed to providing users with advice, guidance and support in the event of any problems they may encounter when using members websites.

Visit www.datingagencyassociation.org.uk

Royal Mail Opt Out Service

Opting out from Royal Mail Door to Door stops all unaddressed items from being delivered by the Royal Mail to your address. Opting out means no one at the address will receive unaddressed mail items via Royal Mail deliveries. If you wish to opt out of receiving Door to Door mail items send your name and address details to the address to Freepost ROYAL MAIL CUSTOMER SERVICES or email your name and address to: optout@royalmail.com You will then be sent an opt-out form to your address, which you must sign and return.

Visit https://personal.help.royalmail.com/app/answers/detail/a_id/293

Royal Mail Scam Mail

If you think you or a family member is receiving scam mail you can report it to the Royal Mail. Write to Royal Mail at Freepost Scam Mail or call on 03456 113 413 or email at scam.mail@royalmail.com

SAFERjobs

SAFERjobs is a charity originally set up by the Metropolitan Police in 2008 with the objective to protect job seekers. It offers free advice to jobseekers and agency workers to ensure people do not fall foul of fraud or illegal practice. Jobseekers are advised to look for recruiters who partner with SAFERjobs for a safer job search.

Visit www.safer-jobs.com

Police Scotland

All reports of cybercrime, fraud and any other financial crime should be reported to police via 101 without delay. The Police Scotland website also contains up-to-date information on numerous types of fraud and cybercrime and details how to protect yourself when online.

Visit www.scotland.police.uk/keep-safe/

The Scottish Business Resilience Centre

The Scottish Business Resilience Centre also contains up-to-date information and informative preventative videos on numerous types of fraud and cybercrime, and details how to protect yourself when online. These are relevant to the business community but also very useful for the individual.

Visit www.sbrcentre.co.uk/

Secure Tickets from Authorised Retailers (STAR)

STAR is the leading self-regulatory body for the entertainment ticketing industry across the United Kingdom. STAR members include major UK ticket agencies as well as numerous venues and box offices in London and across the country. STAR offers general advice and information on ticket buying and provides a dispute resolution service for customers who have an unresolved problem with their purchase from a STAR member.

Visit www.star.org.uk

Stay Safe Online

Powered by the National Cyber Security Alliance, Stay Safe Online builds strong public/private partnerships to create and implement broad-reaching education and awareness efforts. To empower users at home, work and school with the information they need to keep themselves, their organisations, their systems and their sensitive information safe and secure online and encourage a culture of cybersecurity.

Visit www.staysafeonline.org

UK Finance

UK Finance is responsible for leading the collective fight against financial fraud on behalf on the UK payments industry. Their membership includes banks, credit, debit and charge card issuers, and card payment acquirers in the UK. Their website offers information about the various types of payment fraud, as well as helpful tips and advice on how to minimise your chances of becoming a victim, and what to do if you become a victim.

Visit www.ukfinance.org.uk

The Silver Line

The Silver Line operates the only confidential, free helpline for older people across the UK that's open 24 hours a day, seven days a week. They also offer telephone and letter friendship schemes where volunteers are matched with older people based on their interests; facilitated group calls; and help to connect people with local services in their area.

To contact the Silver Line call 0800 4 70 80 90 or visit www.thesilverline.org.uk

Telephone Preference Service (TPS)

TPS is a central opt out register allowing individuals to register their wish not to receive unsolicited sales and marketing telephone calls. It is a legal requirement that companies do not make such calls to numbers registered on the TPS.

To register call 0345 070 0707 or visit www.tpsonline.org.uk

Think Jessica

Think Jessica is a charity set up to protect elderly & vulnerable people from scams which come through the postal system and criminals who contact them by telephone. They offer advice and support to victims of mass marketing fraud as well as assistance to friends and relatives of those that have been scammed.

Visit www.thinkjessica.com

REDUCING THE DAMAGE

Although it may be hard to recover any money that you have lost to a scam, there are steps you can take to reduce the damage and avoid becoming a target again.

The quicker you act, the more chance you have of reducing your losses.

Report a scam

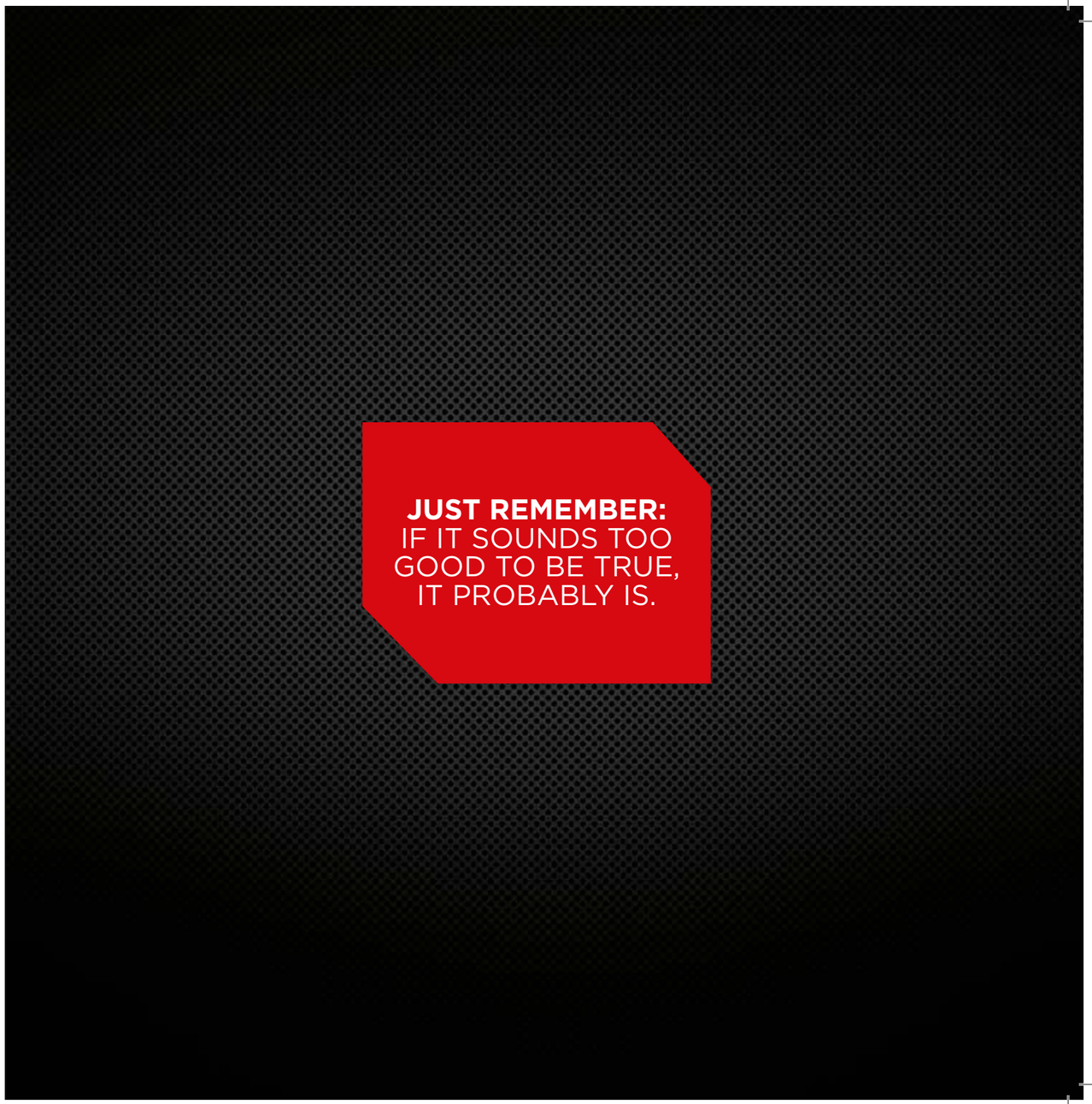
By reporting the scam to Police Scotland or Trading Standards, we will be able to warn other people about the scam and minimise the chances of the scam spreading further. You should also warn your friends and family of any scams that you come across.

Scammers are quick to identify new ways of conning people out of their money. Be aware that any new scheme or initiative will quickly be targeted.

Finally, remember that this booklet does not contain all the answers but to avoid being a victim you need to be aware that someone who is not suspicious and has a trusting nature is a prime target for a scammer.

Be suspicious and remember if it sounds too good to be true it probably is!

BIG SCAMS



BIG SCAMS

NOTES

Royal Bank of Scotland, Police Scotland and the Scottish Business Resilience Centre would like to thank the Metropolitan Police Service for their assistance in the publication of this booklet.

BIG SCAMS

POLICE SCOTLAND
Keeping people safe

NPCC
National Police Chiefs' Council

Scottish Business Resilience Centre
Creating a secure Scotland for business to flourish in

Royal Bank of Scotland