NCCDSW
National Centre for Cross Disciplinary Social Work
Bournemouth University

appg All-Party Parliamentary Group on Financial Crime & Scamming

Cyber Fraud and Scamming

Guidance and Advice

City of London

NATIONAL TRADING STANDARDS Scams Team

Office of the Public Guardian

cifas Leaders in fraud prevention

NATIONAL TRADING STANDARDS eCrime Team

ctsi Chartered Trading Standards Institute

Jungo

SOLLA Society of Later Life Advisers

What is Cyber Fraud?

This booklet focuses specifically on fraud and scamming; however cybercrime acts as a wider umbrella term, encompassing a range of criminal activity. Cybercrime can be simply defined as criminal activities carried out via the use of electronic devices, the internet and other forms of information and communications technology. The increasing use of computers and smartphones has facilitated a growth in the use of these systems as enablers of all types of crime, including: economic related cybercrime; organised crime; malicious and offensive communications; cyber stalking and harassment; and cyber terrorism.

Frauds committed directly against individuals are estimated at around £6.8 billion per year

Annual Fraud Indicator, 2017

Whether you use the term 'fraud' or 'scam', the goal for the perpetrators of these offenses are always the same: to gain an advantage, typically financially, over others using deceptive means. Scams come in varying forms across varying mediums but all involve deliberate deception, intending to mislead and often appealing to visceral needs and desires, in order to trick the intended target for finance gain.

Cyber Fraud can be broadly categorised into two distinct categories: **cyber-dependent fraud** and **cyber-enabled fraud.**

FRAUD ACT 2006

Fraud Act 2006 states that fraud is committed in three specific ways with different types of scams falling into each category:

(a) Fraud by false representation

(b) Fraud by failing to disclose information

(c) Fraud by abuse of position (Fraud Act, 2006, Chapter 35 (1))

THE CONSUMER PROTECTION FROM UNFAIR TRADING REGULATIONS 2008

The Consumer Protection from Unfair Trading Regulations 2008 makes misleading actions or omissions by traders a criminal offence. If a trade, business or service interaction is untruthful, likely to deceive, lead to a person engaging in a transaction they would not normally do, or hides or leaves out crucial information (Age UK, 2015). This includes unscrupulous behaviour by legitimate traders.

Cyber-Dependent Fraud

Fraudulent activity that can only be committed via the use of information communications technology, primarily targeting computers and networks. This type of cyber-crime poses the greatest threat to public services and businesses but can also affect individuals due to the collection of personal data, leading to further fraudulent activity.

The primary types of cyber-dependent crimes are:

Hacking: The unauthorised use of, or access into, computers and networks, by exploiting vulnerabilities. This access can then be used to gather personal data and information, of which the impact can be significant financial losses for larger organisations, but can also result in the personal and financial data of individuals being compromised, leading to further fraudulent activities.

Disruption of Computer Functionality: Often referred to as 'malware' and distributed by unsolicited or junk mail. Malicious software is designed to interfere with how computers and networks function, most frequently seen in the form of viruses, worms, Trojans, spyware and ransomware. Malware performs functions such as; undertaking hidden or unauthorised actions, damaging or deleting hardware, software or files, gathering sensitive and personal information or monitoring activity.

Other types of Disruption of Computer Functionality, such as Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks, most frequently aimed at organisations and businesses rather than individuals, are designed to interrupt or suspend services and systems and make web-based services unavailable to users.

Cyber -Enabled Fraud

Offenses which can be committed without the use of information communications technology but can be increased in their scale, impact and reach by the use of computers and computer networks. Cyber-enabled frauds are similar to those carried out via other mediums, such as mail, telephone and doorstep scams, but can often target individuals on mass, increasing the number of potential targets.

This section will look at the most common types of cyber-enabled fraud and provide some examples. This is by no means an exhaustive list and one type of fraud can overlap with another. Cyber-enabled frauds, as with mail and telephone frauds, are constantly evolving as the public becomes aware and as scammers adapt. Acts of fraud, however, do follow certain patterns of behaviour. This section is designed to help you spot the common identifiable signs of scams and take appropriate action.

Cyber-enabled frauds are the most common form of all cybercrime and fraud offences with over half of fraud incidents reported in the Crime Survey for England and Wales being cyber related (ONS, 2018).

The majority of cyber-enabled frauds can be aligned with the following four broad categories:

Authorised Push Payment Scams

Advance Fee Fraud

Consumer and Retail Fraud

Bank and Credit Card Fraud

Who does cyber fraud affect?

Cyber fraud can be targeted at anyone, from individuals to companies and organisations. Cyber-dependent fraud tends to be targeted at businesses and organisations where vast amounts of data can be accessed and harvested, whereas cyber-enabled fraud is more frequently targeted at individuals. However, these two types of fraud are not mutually exclusive and may interact on a practical level; for example, personal information obtained from organisations may, in turn, be used to target individuals.

1.9 million incidents of Cyber-related frauds were reported in the year ending September 2018. (ONS, 2018)

How big is the problem?

3.5 million incidents of fraud were reported in the year ending September 2018, amounting to almost a third of all reported crimes in that same year. Fraud offence data was collated by the National Fraud Intelligence Bureau (NFIB) from three reporting bodies: Action Fraud and two industry bodies, Cifas and UK Finance. Cyber-related fraud accounted for over half of reported fraud incidents during this period, a total of 1.9 million incidents.

The Crime Survey for England and Wales (ONS, 2018) reported a 33% decrease in the number of viruses being reported in the year ending September 2018, in comparison with the previous year. However, the number of incidents involving “unauthorised access to personal information” has remained relatively consistent, with 470,000 offences being reported.

Who is at risk?

Everyone! Fraudsters target different age groups depending on the type of fraud. Cifas (2018) reported that criminals target younger people to become money mules, which are individuals who allow their bank account to be used to move the proceeds of crime. Over 32,000 mule accounts were identified in 2017, which was an increase of 11% from the previous year, and 71% of which were held by males. However, individuals over the age of 60 were most likely to be victims of account takeovers, whilst individuals between the ages of 31 and 60 saw a higher occurrence of impersonation.

For further information, please see The Fraudscape (Cifas, 2018).

Fraud against older people

Factors associated with older age such as bereavement, cognitive impairment, social isolation and poverty can increase susceptibility to responding to scam approaches (Age UK, 2015). In addition, the increasing use of the internet and e-communications has provided criminals with a new way to target a global audience (Chang, 2008). Between 2016 and 2017, the top 4 types of fraud affecting the 60-99 age group were computer software service fraud, advance fee frauds, online shopping and auctions and computer virus/malware/spyware. These figures demonstrate particular vulnerabilities for this age group relating to cyber scamming.

Loneliness and social isolation have been identified as contributory factors to susceptibility to scams and fraud, with socially isolated older adults being particularly susceptible to financial scamming (Lubben et al. 2015). However, loneliness and social isolation are not exclusive to older adults, as individuals of any age who do not have a social network may have a limited awareness of scams and there may be fewer opportunities for other people to notice, identify or intercept scams.

You do not need to be socially isolated to be a target of cyber scammers. Action Fraud recorded an overall rise in computer misuse, particularly in respect to hacking via the use of social media and email, which has increased by 35%, with 9,458 offences reported over the previous 12 months.

Anyone who is online has the potential to fall victim to cyber scamming! The vast majority of us are online in one way or another and therefore a potential target.

Why people respond to scams?

Scammers appeal to basic human needs and motivations such as opportunities which lead to financial security or companionship which envoke emotional responses. The persuasive techniques used by scammers are designed to elicit visceral responses, which can encourage quick or unwise decision making, stopping individuals from thinking about the scam for long enough to consider the risks or credibility. Older people may demonstrate some additional vulnerability to cyber scams but they are not alone.

Social Engineering: criminals often use social engineering tactics to trick customers into revealing their online banking security details, through scam phone calls, texts and emails. Most of us tend to want to be helpful and cooperative; fraudsters and scammers take advantage of this and will skilfully manipulate targets to divulge personal information. This is often achieved through impersonation of a legitimate organisation, such as banks, HMRC, TV licencing or a government department.

The 2018 Global Fraud and Identity Report

Device ownership

1. Smartphone (91%)
2. Laptop (83%)
3. Tablet (65%)
4. PC (62%)
5. Smartwatch (21%)
6. Smarthome device (13%)

Top Activities on Devices

1. Online shopping (90%)
2. Personal Banking (88%)
3. Play Video Games (51%)
4. Apply for Driver's License (51%)
5. Get quotes/Buy Insurance (49%)
6. Apply for Credit Cards/ Loans (48%)
7. File Taxes (45%)

Over half of the fraud incidents reported in last year's CSEW were reported to be cyber related.

The 2018 Global Fraud and Identity Report, Experian, 2018.

Social Media

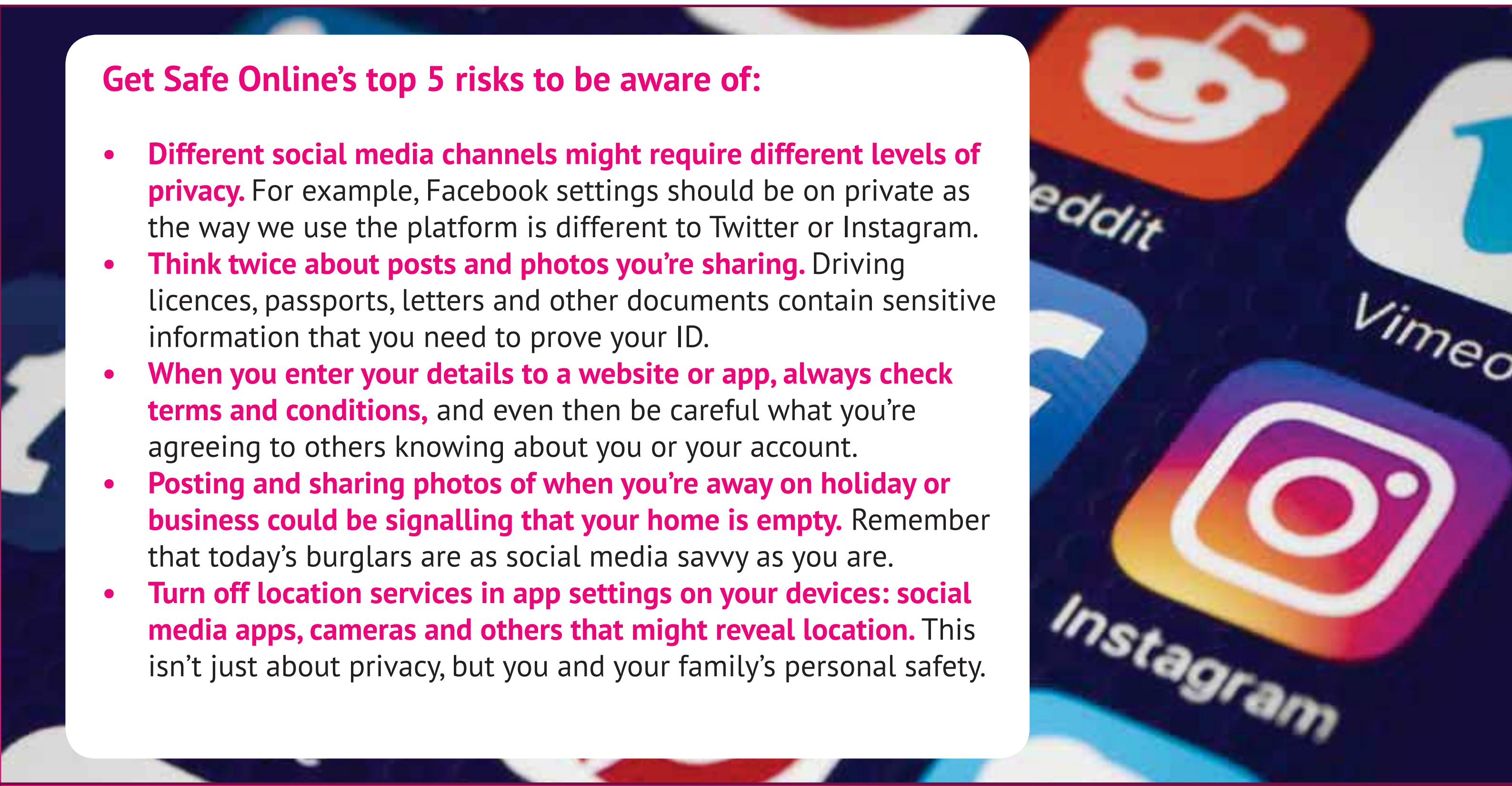
Many perpetrators aiming to commit financial fraud 'hide' behind the fact that they may not be readily identifiable by their social media accounts, which is why these methods are often used to approach targets.

It is vital that you frequently review what information exists online about you - review all the privacy and security settings on your social media pages regularly

It takes less than a second to click on a link in a tweet, or a post on your social media or in a direct message – either advertising a gift or special offer – or, ironically, warning you to take action to avoid some kind of financial loss. This could appear to be from anybody, including a trusted contact, if their social media account has been compromised or identity spoofed. The link might take you to a website requesting confidential information about you, or cause your device to be infected with malware. Alternatively, the post, tweet or message may instruct you to make a phone call to a specified number, which can either result in confidential details being requested, or be to a rate number resulting in exorbitant charges being added to your phone bill.

Some of the risks include:

- **Identity theft** – having your credentials controlled
- **Account hijacking** - having your online accounts being taken over
- **Data theft** - having your contact details obtained and used



Get Safe Online's top 5 risks to be aware of:

- **Different social media channels might require different levels of privacy.** For example, Facebook settings should be on private as the way we use the platform is different to Twitter or Instagram.
- **Think twice about posts and photos you're sharing.** Driving licences, passports, letters and other documents contain sensitive information that you need to prove your ID.
- **When you enter your details to a website or app, always check terms and conditions,** and even then be careful what you're agreeing to others knowing about you or your account.
- **Posting and sharing photos of when you're away on holiday or business could be signalling that your home is empty.** Remember that today's burglars are as social media savvy as you are.
- **Turn off location services in app settings on your devices: social media apps, cameras and others that might reveal location.** This isn't just about privacy, but you and your family's personal safety.

Most social networking sites, for example Facebook, have a means of reporting such issues. Twitter is also introducing an in-Tweet 'Report Abuse' button across all apps and its website.

Find further advice on this here:

- https://www.facebook.com/help/safety
- https://help.twitter.com/en/safety-and-security/account-security-tips
- https://myaccount.google.com/security
- https://help.instagram.com/
- https://support.snapchat.com/en-GB/a/privacy-settings2

If you are affected: gather and document as much evidence as you can and report the incident to the police and seek help and support from relevant organisations.

Written by Stevie Corbin-Clarke

Authorised Push Payment (APP) Scams

Authorised push payment scams (APP) are where a person is tricked into authorising the transfer of money into an account controlled by the fraudster. UK finance data on APP fraud show there were 43,875 cases and total losses of £236 million in 2017, increasing to £354 million in 2018.

Individuals are convinced by the scammer to:

- **a) transfer funds to another person, but are instead deceived into transferring the funds to a different person or;**
- **b) transfer funds to another person for what they believed are legitimate purposes but which were in fact fraudulent.**

Contingent Reimbursement Model Code for Authorised Push Payment Scams

The Authorised Push Payment (APP) Scams Steering Group has agreed a voluntary code of good practice to address APP fraud.

Payment service providers that sign up to the Code will commit to:

- protecting their customers, including procedures to detect, prevent and respond to APP fraud, with a greater level of protection for customers considered to be vulnerable to this type of fraud; and
- preventing accounts from being used to launder the proceeds of APP fraud, including procedures to prevent, detect and respond to the receipt of funds from this type of fraud.

The most common type of APPs are impersonation scams, typically impersonating official bodies such as Banks, HMRC or TV licensing agency.

Confirmation of Payee (CoP): At present, only the account number and sort code need to match for payments to be successful, meaning fraudsters pose as someone legitimate to trick victims into paying them money. The proposed Confirmation of Payee system means anyone making a payment will be alerted if the name does not match the account, cutting down on the number of APP scams in which people are conned into sending money into a scammers account.

HMRC Scam

During March, April and May 2018, HMRC received nearly 250,000 reports of phishing and made over 6,000 requests to have websites shut down.

According to Ofcom Communications Market Report 2018, 95% of 16-24-year-olds owned a smartphone last year and 51% of those aged over 55+ owned a smartphone in the same period. Smartphones are often how many members of the public receive text and email scams.

The tax authority is urging anyone who knows someone that could be vulnerable to scams to warn and prepare them.

HMRC's top tips:

• **Recognise the signs -** genuine organisations like banks and HMRC will never contact you out of the blue to ask for your PIN, password or bank details.

• **Stay safe** - don't give out private information, reply to text messages, download attachments or click on links in emails you weren't expecting.

• **Take action** - forward suspicious emails and details of suspicious calls claiming to be from HMRC to phishing@hmrc.gov.uk and texts to 60599. If you have suffered financial loss contact Action Fraud on 0300 123 2040 or use their online fraud reporting tool.

• **Check GOV.UK** for information on how to avoid and report scams and recognise genuine HMRC contact.

Action Fraud, Springtime tax scams target young and vulnerable, warns HMRC, 24/04/2017

TV Licensing phishing emails

How does it work?

1 Firstly, the scammers send fake emails saying TV Licensing have been trying to get hold of you regarding a refund or an over-payment. Other versions might claim that your billing details need to be updated. However, all versions of the emails contain links to a cloned version of the official TV Licensing website that is designed to harvest your login and bank details.

The cloned site asks you to login and prompts you for your full name, phone number, date of birth, address, email address, account number, sort code, card details, and security or CVV numbers on the back of the card.

2 The second stage typically occurs a week or two later, when criminals posing as bank staff call to warn you that your account has been compromised. The criminals convince you that you must urgently move money into a so-called 'safe' account.

3 The final stage is stealing it all.

It is a convincing scam because the licensing emails appear authentic and gets victims to give criminals the details they need to appear to be from the victim's bank. For instance, at the cold calling stage, some scammers spoof caller IDs based on the victim's sort code, address and bank details to add to the illusion they really are the victim's bank.

What to look out for

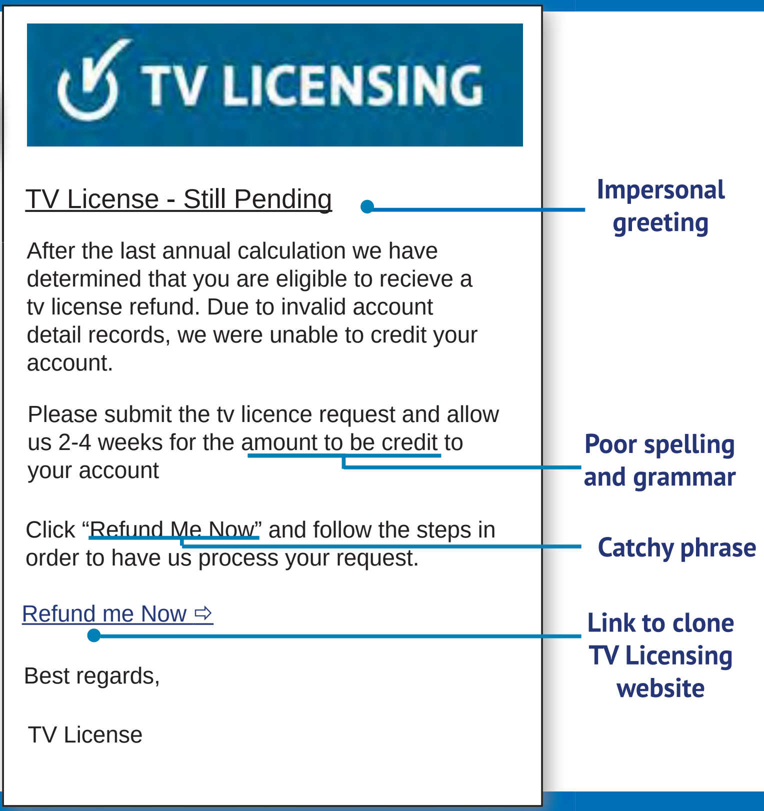
The TV Licensing agency never send refund information by email, or ask you for payment or personal details, and is investigating the scam.

The emails use catchy subject lines and phrases like 'refund', 'renew now' or 'security alert' to pressure victims into clicking through to the cloned site.

The fakes tend to begin with an impersonal greeting, rather than using the victim's real name. Genuine TV Licensing emails will include your real name.

You should always check the sender's email address, and hover over any links to check if the URL goes to the genuine TV Licensing site.

The grammar and spelling may also be poor.



TV LICENSING

TV License - Still Pending

After the last annual calculation we have determined that you are eligible to recieve a tv license refund. Due to invalid account detail records, we were unable to credit your account.

Please submit the tv licence request and allow us 2-4 weeks for the amount to be credit to your account

Click "Refund Me Now" and follow the steps in order to have us process your request.

Refund me Now ⇨

Best regards,

TV License

What to do if you get one?

In 2018, Action Fraud had over 7,000 reports of this scam. If you receive one of these emails, please delete it and do not click any of the links they contain.

Finally, if you have clicked any of the links and submitted personal or financial information, report it immediately to Action Fraud on 0300 123 2040. If you gave any bank details, you will also need to ring your bank straight away.

You can find more information from the official TV Licensing website. www.tvlicensing.co.uk

Example provided by Stephen Forster, National Communications Officer for the National Trading Standards eCrime Team

Advance Fee Fraud

Advance fee fraud (AFF) is where an individual receives a communication requesting money, often for a variety of emotive reasons. This type of fraud often involves an upfront payment being made on the basis of the prospective receipt of goods or often financial gain, such as inheritance or lottery scams. Advance fee frauds can be linked to general mass phishing campaigns, or can be highly personalised, such as in romance or clairvoyant scams. These types of scams, like many others, are underpinned by social engineering. However, are often designed to exploit the vulnerability of individuals, provoking emotional responses and often having a long term negative impact on the individual.

- **Career opportunity scams**
- **Clairvoyant or psychic scams**
- **Romance scams**
- **Fraud recovery fraud**
- **Inheritance fraud**
- **Investment Fraud**
- **Loan scams**
- **Lottery, prize draw and sweepstake scams**
- **Rental fraud**
- **West African letter or 419 fraud**
- **Work from home / business opportunity scams**
- **Vehicle matching scams**

Social Media Investment Fraud

Action Fraud has seen an increased number of investment schemes being advertised on Instagram over recent months, with young people aged between 20 and 30 the most likely to fall victim.

Fraudsters are advertising 'get rich quick' investment schemes on the app, which promise a high return within 24 hours. A £600 investment is initially requested which fraudsters claim will be multiplied within 24 hours.

Victims are then making payments via bank transfer to the fraudster's bank account. Fraudsters are then sending screenshots of thousands in profit crediting their accounts, which they claim can be released for a fee. Victims have requested to withdraw their funds while they're still in profit, and at this stage the fraudsters are stopping contact with the victim and closing the Instagram account.

Stay safe when scrolling:

- **Never respond to any requests to send money, or have money transferred into your account by someone you don't know and trust.** These types of requests should always raise a red flag. If something feels wrong then it is usually right to question it.

- **Don't immediately agree to any offer that involves an advance payment or having to sign a contract on the spot.** Always speak with a friend or family member first.

- **Always check the credentials of any financial company on the Financial Conduct Authority's (FCA) website:** – they should be on the register. Contact the preferred company directly and reject any offers made through unsolicited communications.

Action Fraud: Fraudulent investments being advertised on social media, 25-02-2019.

Every report maters – if you have been a victim of fraud or cybercrime, report it to Action Fraud online or by calling 0300 123 2040.

Romance Scams

How does it work?

1 You might think you have met your perfect partner through an online dating website and they seem interested because they are asking lots of questions about you. Fraudsters contact their targets using fake profiles in an attempt to build what feels like a loving relationship.

2 Once a fraudster is confident that they have won your trust, they will invent a reason to ask for your help. They will use the emotional attachment you have built and ask you to help them out by sending money. For example, they may attempt to invoke a visceral response by telling you a family member is ill and they need money for medical treatment. Otherwise, they may have arranged to visit you, but tell you they need money to pay for the flight or because their ticket has been stolen.

3 Once you send them money, the fraudsters will keep coming back and invent new reasons for you to send them more. They will also have all of the personal information you have told them and may use it in an attempt to blackmail you into continuing to give them money.

How do you spot one?

Scammers will generally use typical grooming techniques and might leave other clues which suggest that they have bad intentions. They will often quickly adopt pet names or terms of endearment in their messages to you and you may notice early on that they do not answer basic questions, such as where they live and work. Scammers will also prefer to switch to communications via social media, texting or email and will encourage you to chat outside of the security of the dating website. A third party is often brought into the conversation to make the scammer's lies seem more plausible.

What can you do to avoid them?

- Trust your instincts
- Avoid giving away too many personal details when online dating
- Never send money or give your bank details to someone you have only met online
- Choose a reputable dating website
- Use the site's messaging service. Fraudsters will want to quickly switch to other forms messaging so there is no evidence of them asking for money
- Reverse image search can find photos that have been taken from somewhere else - they could have been stolen from anywhere

What to do if you have come into contact with a romance scammer?

- Immediately break off all contact with the fraudster and do not send any more money
- It can be embarrassing to feel tricked into thinking you have formed a relationship online, but if you report any suspicious behaviour to the chat room operator and Action Fraud, they will take your report in confidence. Report online or call: 0300 123 2040.

Example provided by Stevie Corbin-Clarke, Bournemouth University.

Consumer and Retail Fraud

The national Crime Survey for England and Wales (CSEW) has reported a 27% increase in retail fraud in the July 2017-2018 period from the same period the previous year.

Consumer and retail fraud commonly covers deceptive business practices, where the consumer believes they are purchasing goods or services but are actually being defrauded. These frauds can relate to inaccurate claims or false promises, as well as counterfeit or non-existent products or services.

Shopping and auction fraud frequently involves purchased goods not arriving, or buyers receiving goods that are less valuable or significantly different to the original description. The most immediate problem being that the buyer is unable to return the goods or have the money refunded. Similarly, scammers take advantage of the demand for popular goods or events, where websites are set up which look genuine, using a name or web address which appears very similar to a legitimate seller. If the buyer does receive a product, it may be counterfeit, and in the case of ticketing fraud the buyer may not even be aware of this until they are refused entry to an event when the organisers recognise the ticket as fake.

Computer Software Service Fraud

If you receive a phone call, email or pop-up from your internet service provider saying your internet connection is about to be cut off, most of us would feel the need to take action. Our connection to the internet is what the majority of our devices, from Laptops to Smart TVs or streaming services, depend on. In 2017/18, Action Fraud received 22,609 reports of Computer Software Service fraud, with a total of £21,365,360 being lost to fraudsters, with the average age of victims being 63.

These types of scams are not, however, limited to internet service providers. Scammers will purport to be from well-know reputable companies, such as Microsoft or Apple, contacting you to tell you there is a problem they can help you with.

How does it work?

1 The email, pop-up or phone call will prompt you to call a number so that you can be connected with 'tech support', and these numbers may appear similar to numbers listed on legitimate websites but they will connect the caller to a call centre, often based in another country.

2 The person offering you this technical support will appear to want to help you resolve your problem; this may include one or both of the following:

- Remoting into your computer to find out what the problem is and fix it for you!
- For a 'discounted' fee, they might offer you technical support whenever you need it.

3 The final stage is stealing it all.

You give the scammer access to your PC and they can now find all your personal and account details that are stored on it!

Once the scammer has, with your permission, gained remote access to your device they are able to access all your files and personal information, install spyware or other harmful software, potentially locking you out of your own device and holding your files to ransom.

NEVER let anyone who contacts you out of the blue remote into your device or PC.

In 'purchasing' the goods, the buyer has been required to give personal and financial information to make the original payment. This information is now available to the scammers and may be used for subsequent frauds.

It is a good idea to have a separate method of payment for making online purchases and, where possible, use a digital wallet such as PayPal. Using a credit card for purchases between £100 and £30,000 is recommended to ensure the purchase is covered under Section 75 of the Consumer Credit Action 1974, making the card company jointly liable with the retailer.

- **Online shopping and auctions**
- **Computer software service fraud**
- **Ghost Brokers**
- **Ticket fraud**
- **Retail fraud**

How do you spot one?

The initial contact will often be out of the blue and may not be associated with any problems arising with the device or internet connection. The scammers will also stress the importance of taking quick action, limiting your ability to think clearly. Legitimate computer firms do not make unsolicited phone calls to help you fix your computer. Fraudsters make these phone calls to try to steal from you and/or damage your computer with malware.

What can you do to avoid a software service fraud?

The best way to avoid this type of scam is not to be rushed into making a decision. An internet service provider, such as BT, will not require access to your device to address problems related to your internet connection. Similarly, Microsoft and Apple will not require credit card information to validate software.

What to do if you have given someone access to your computer?

If you have given someone access to your computer they may have gained access to all the information, including banking details and passwords stored on that device.

Change all passwords and authentication information on all accounts that may have been accessed. Do this on a different device or PC so that the scammers do not have the new information.

Monitor your bank accounts and credit reports so you can detect any unfamiliar financial activity. Report any suspicious activity to your bank or card provider. If you have given the scammer any payment details, contact your provider to report the fraud.

Run a malware checker or antivirus program on your machine. Check the device for malware or spyware which may have been installed and still active. Do not use your device for anything confidential until you are sure the information is not still available to the scammers.

If you have let a scammer into your PC, disconnect their connection as soon as you realise; this may involve turning off the Wi-Fi on your device or physically disconnecting the device from the internet.

Report it to Action Fraud on 0300 123 2040.

Bank and Credit Card Fraud

Scammers will contact a target via email or social media pretending to be from genuine organisations, such as banks, the police or government departments and will then impersonate these organisations to extract personal or financial information from their intended target.

Scammers use a variety of tactics to elicit a response from targets, often specifically impersonating organisations which will provoke an emotional response from targets. For example, they might indicate that there has been an issue in regards to payment, their account security or a refund or rebate is due to them.

Personal and financial information can be obtained by allowing someone remote access to a computer or by a third party data breach. Therefore, this does not depend on the target handing over their details to the scammer and they may not be aware that the scammers have obtained them.

The ultimate goal of many different types of cyber-enabled and cyber-dependent fraud is to obtain an individual's personal details to access their financial facilities. This allows the scammer maximum access to available funds, in addition to identity theft and dishonestly retaining wrongful credit.

Shopping coupon scams

If you saw a supermarket coupon for £75, £150 or £250, it would get your attention... Right? Of course it would, and that's exactly what coupon scammers rely on. This is because what appears to be a harmless, low level scam is really a cynical ploy to steal your money, your identity or banish you to a life on suckers' lists.

If you have not seen a fake coupon yet, you may see one soon because it is only a matter of time before someone shares one with you on Facebook, Twitter or WhatsApp, or before the scammers find another way to dangle one under your nose.

How does it work?

1 You might see a social media post, or receive a WhatsApp message or text from a friend saying something like: "Asda is giving free £100 vouchers to EVERYONE for their wedding anniversary".

Sometimes they are referred to as 'vouchers', other times they are called 'gift vouchers' and latterly they have become 'prizes'. They may come or appear to come from a friend, and encourage you to pass them on to make them seem more believable.

2 There is always a link... **BUT DON'T CLICK IT.** The link leads to an online customer survey asking for your name, address, phone number, and date of birth in return for the voucher.

This seems reasonable for the amount of money they are giving away, doesn't it? In reality, it is enough information to take out a loan in your name, and you will never receive the promised vouchers anyway.

3 **But wait, there is even more!**

They will also sell your details to other criminals to use, abuse and bombard you with more scams.

So what can you do to avoid a coupon scam?

The best way to avoid coupon scams is simply to ignore them. You should never click the links because you risk downloading malicious software to your computer or device. Whatever you do, you should never, ever give over any personal details. Finally, do NOT spread the scam by sharing any of the posts or messages with family and friends.

If scammers can obtain individual's card and bank details, they can utilise them in a variety of ways:

- By gaining direct access to bank accounts, credit cards and online banking facilities.
- Applying for credit by impersonating the target

- **Cheque, plastic card and online bank accounts**
- **Remote purchase fraud**
- **Application fraud**
- **Mortgage related fraud**
- **Mandate fraud**
- **Dishonestly retaining a wrongful credit**

In 2016, £432.3 million was lost to remote purchase fraud, a 9% increase on the previous year. The vast majority of this type of fraud involves the use of card details that have been fraudulently obtained through methods such as unsolicited emails or telephone calls or digital attacks such as malware and data hacks. The card details are then used to undertake fraudulent purchases over the internet, phone or by mail order. It is also known as 'card-not-present' (CNP) fraud.

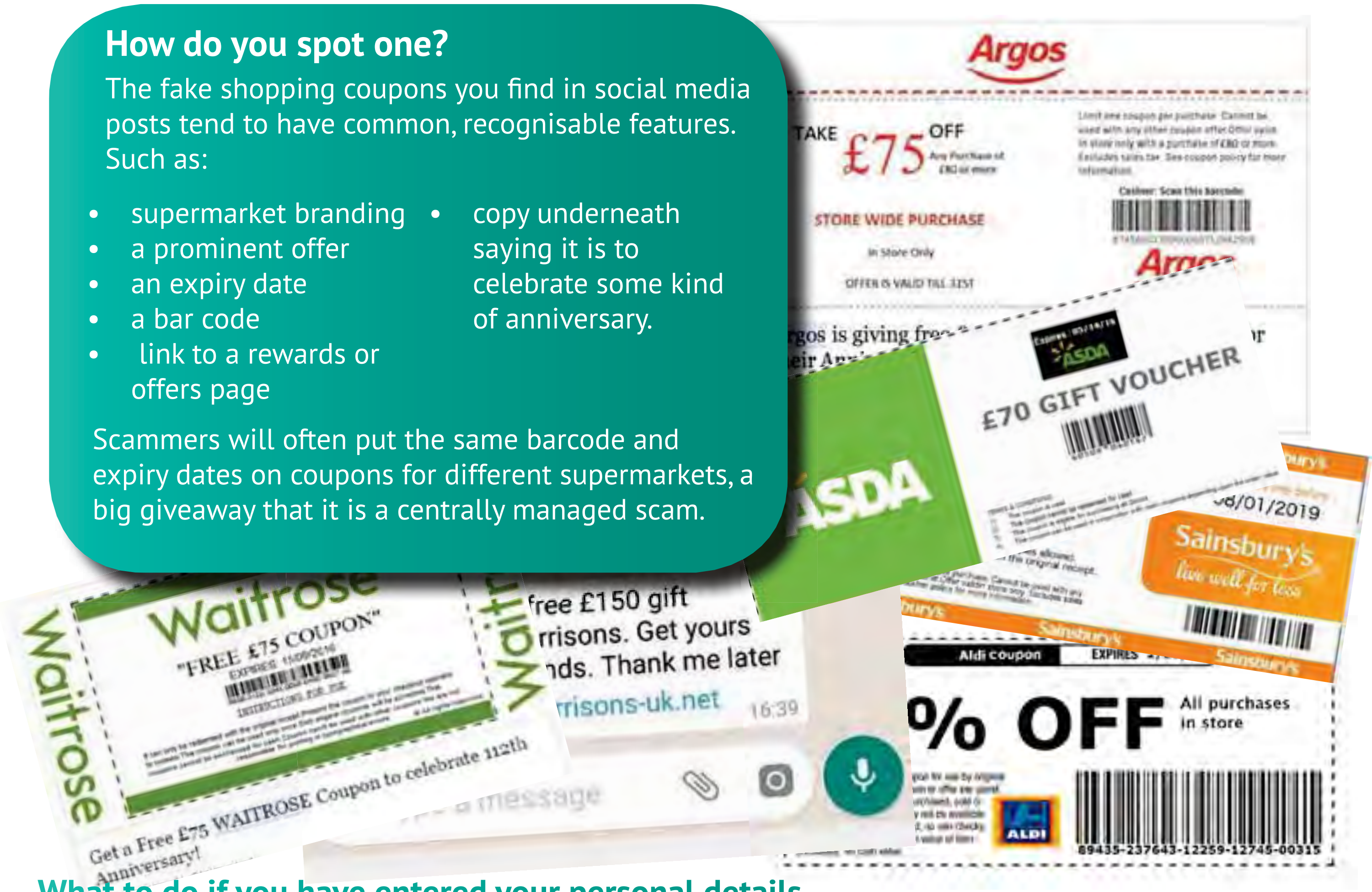
Fraud the Facts 2017, Financial Fraud Action UK (FFA UK)

How do you spot one?

The fake shopping coupons you find in social media posts tend to have common, recognisable features. Such as:

- supermarket branding
- a prominent offer
- an expiry date
- a bar code
- link to a rewards or offers page
- copy underneath saying it is to celebrate some kind of anniversary.

Scammers will often put the same barcode and expiry dates on coupons for different supermarkets, a big giveaway that it is a centrally managed scam.



What to do if you have entered your personal details

Start monitoring your bank accounts and credit rating using a credit report. This is necessary in case the scammers have used your details to open other accounts or taken out loans in your name.

If you have clicked the link, you might also want to run a malware checker or antivirus program on your device, in case the link was malicious.

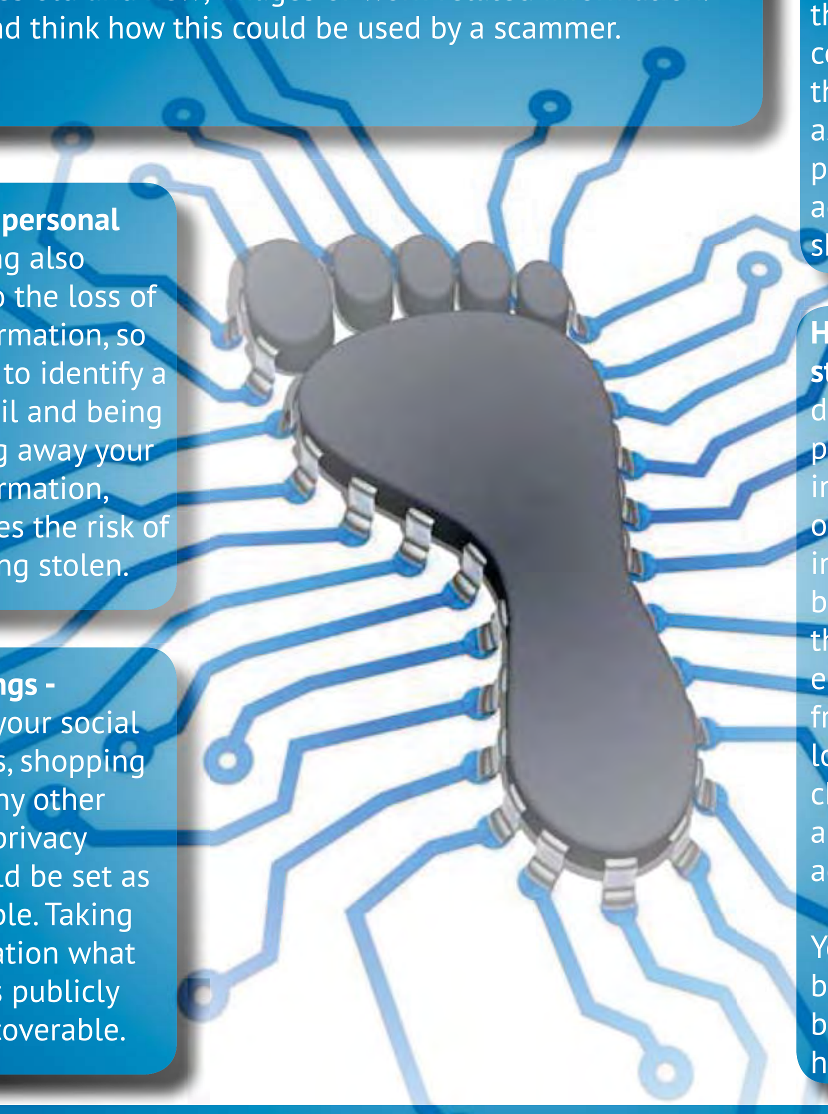
Report it to Action Fraud on 0300 123 2040.

Example provided by Stephen Forster, National Communications Officer for the National Trading Standards eCrime Team

Your digital footprint and identity

It is important to understand the extent of your digital footprint, or, in other words, the information about you that is publicly available on the internet. Your name, address, family and key details that all of us regularly publish about ourselves on social media provide a wealth of information for people looking to use your identity.

The following provides some key advice to help secure your digital footprint and reduce the risk around your identity:



Search for yourself - a good starting point when looking into your digital footprint is to type your name into several search engines such as Google or Bing. Take a good look at what information may be publicly available about you. This could be news articles; social media profiles old and new; images or work-related information. Take note and think how this could be used by a scammer.

Clean up - review your online presence, whether that be on social media or online accounts, delete unused ones and take down information that is unnecessary. Also, consider the information that you have found such as dates of birth (or images posted about your birthday), addresses or check-ins showing your location.

Phishing and personal data - phishing also contributes to the loss of personal information, so learning how to identify a phishing email and being wary of giving away your personal information, further reduces the risk of your data being stolen.

Security settings - whether it is your social media profiles, shopping accounts or any other online login, privacy settings should be set as high as possible. Taking into consideration what information is publicly shared or discoverable.

Has your data been lost or stolen? - more and more data breaches are being publicised where personal information has been lost or stolen. This personal information is often sold on both the surface web and the dark web. Take note of emails you have received from companies that have lost your data and, if needed, change your security settings and password if there is an account.

You can also see if you have been subject to large-scale breaches by visiting: www.haveibeenpwned.com

Know your rights - as of May 2018, the General Data Protection Regulations (GDPR) brought about increased rights for you and your personal data. Knowing these will help you to understand how you can go about reducing the amount of personal data out there about you but also how companies utilise your data. You have the right of access, to be informed, to delete and five other important rights. Visit www.ico.org.uk and look for individual rights for more information.

Passwords

The most common complaint when it comes to securing online accounts and technology is the use of passwords. They can also be the most annoying part of our relationship with computers and the internet, as trying to remember unique and strong passwords is very difficult for most people to do. There is so much conflicting messaging and expectations that it becomes overwhelming in what to do with your passwords. Ultimately, it is about finding something that works for you but also keeps you secure.

Cyber aware and the national cyber security centre (NCSC) understand that there must be a balance between security and people. The following are some considerations around how to go about protecting yourself and using better passwords.

Securing your email - using a strong and unique password for your email is crucial. If you think about it, your email is where you reset all your other security settings for your accounts and a major part of your online presence.

Three random words - although complexity is useful in creating a strong password, it's not particularly useful when you can't remember it. A good way to create a strong and memorable password is to use three random words such as 'carbookelephant' or 'blueshedtable'. Use words are memorable to you and adding numbers and special characters such as '?' or '!' to make it even more secure such '4!carbookelephant?3'.

Do not be personal - combined with your digital footprint, a lot of your personal information can be out there publicly. It's important when choosing your password to not use personal information such as child or partner's name, place of birth or a favourite holiday. All of this could be potentially found online and easily guessed.

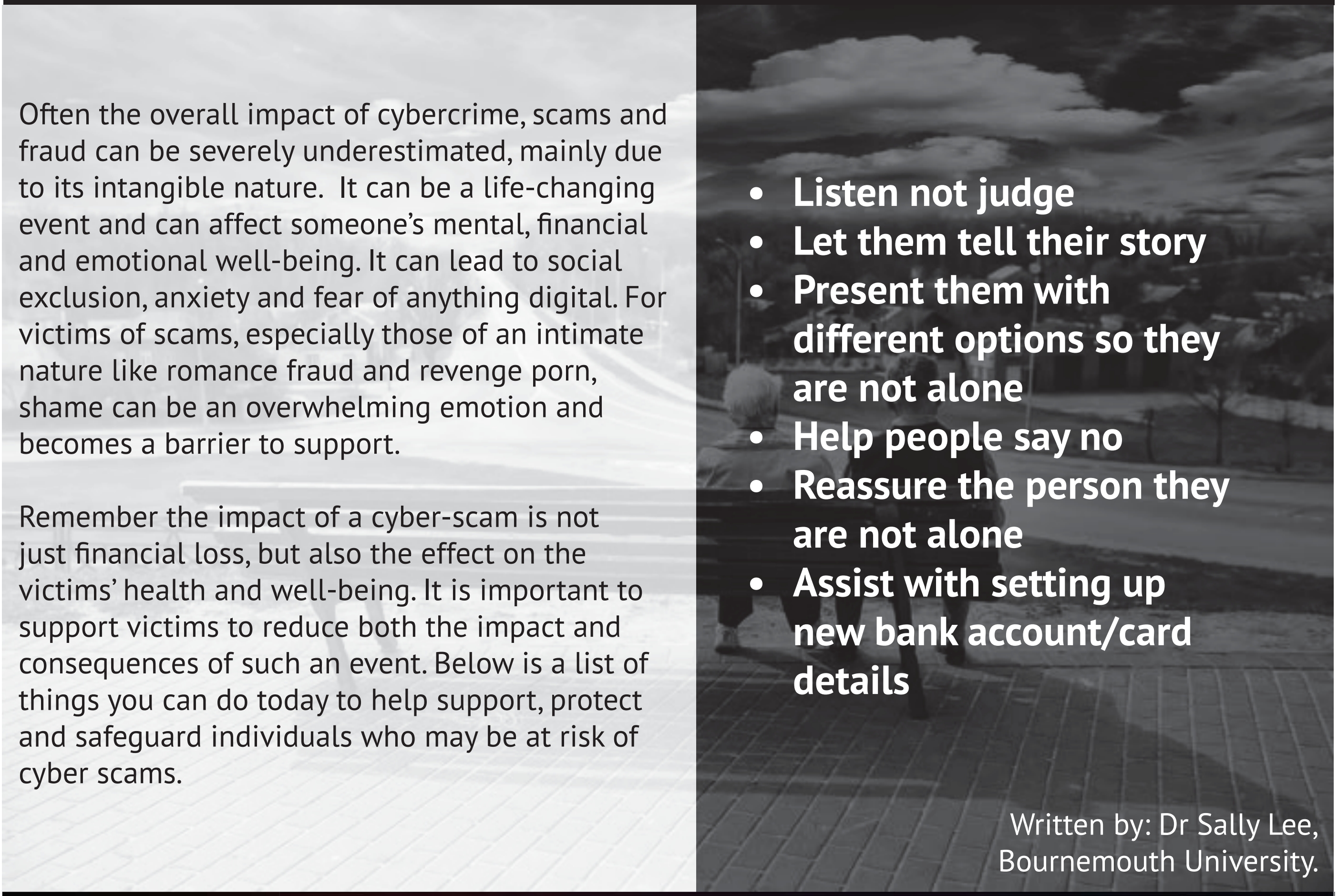
Be unique - although hard remember sometimes, it is important to use a unique password for all of your accounts and logins. The reason behind this is that when one password is discovered, whether that's through a data breach or phishing attempt, the criminal then tries to use that password across the internet and multiple accounts. If you have used the same password then the impact on your privacy and security is much greater.

Password managers - a really good way of managing your passwords is through the use of a password manager. These useful pieces of software come in the form of an application, either built into your browser or your computer. This then creates a really secure and unique password for every login and account for you. Password managers are incredibly convenient. However, you must ensure that the password and security for getting into it is a very strong password.

Two factor authentication - most of your online logins are only as secure as your username and password. But the use of two factor authentication provides an added level of security. If you have done online banking, you will have come across this method where you are asked to provide a code or a number through either your smart phone or a small token. Identifying key accounts that you use regularly such as email and social media and turning on this feature is a really good way to secure it.

Written by: Paul Maskall, Cyber Security and Privacy Consultant, Jungo

How to support victims of cyber scams



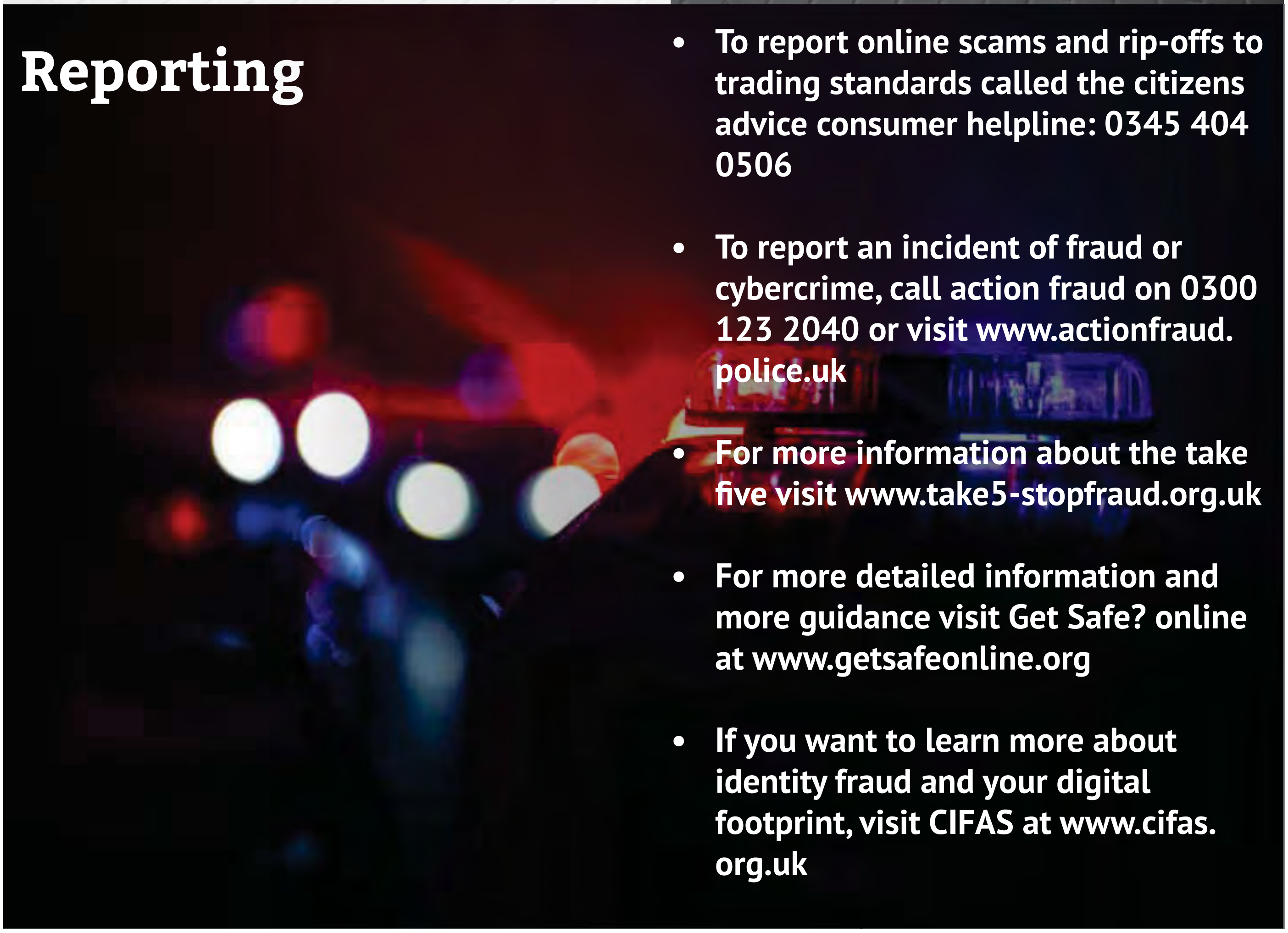
Often the overall impact of cybercrime, scams and fraud can be severely underestimated, mainly due to its intangible nature. It can be a life-changing event and can affect someone's mental, financial and emotional well-being. It can lead to social exclusion, anxiety and fear of anything digital. For victims of scams, especially those of an intimate nature like romance fraud and revenge porn, shame can be an overwhelming emotion and becomes a barrier to support.

Remember the impact of a cyber-scam is not just financial loss, but also the effect on the victims' health and well-being. It is important to support victims to reduce both the impact and consequences of such an event. Below is a list of things you can do today to help support, protect and safeguard individuals who may be at risk of cyber scams.

- **Listen not judge**
- **Let them tell their story**
- **Present them with different options so they are not alone**
- **Help people say no**
- **Reassure the person they are not alone**
- **Assist with setting up new bank account/card details**

Written by: Dr Sally Lee,
Bournemouth University.

Reporting



- **To report online scams and rip-offs to trading standards called the citizens advice consumer helpline: 0345 404 0506**

- **To report an incident of fraud or cybercrime, call action fraud on 0300 123 2040 or visit www.actionfraud.police.uk**

- **For more information about the take five visit www.take5-stopfraud.org.uk**

- **For more detailed information and more guidance visit Get Safe? online at www.getsafeonline.org**

- **If you want to learn more about identity fraud and your digital footprint, visit CIFAS at www.cifas.org.uk**

TAKE FIVE TO STOP FRAUD™

THINGS YOU CAN DO TO PREVENT FRAUD

If you receive a request to provide personal or financial information always take a moment to reflect and step back from the situation. Here are some general tips to keep in mind:

1. NEVER DISCLOSE SECURITY DETAILS A genuine bank or organisation will never ask you for details such as your PIN or card number over the phone or in writing. Before you share anything with anyone, stop and think. Unless you're 100% sure who you're talking to, don't disclose any personal or financial details. Instead, hang up and contact the organisation yourself using the number on the back of your bank card or on their website.

2. DON'T ASSUME AN EMAIL OR PHONE CALL IS AUTHENTIC Just because someone knows your basic details (such as your name and address or even your mother's maiden name), it doesn't mean they are genuine. Criminals will use a range of techniques to get your details and may even say you've been a victim of fraud to scare you into action.

3. DON'T BE RUSHED OR PRESSURED Under no circumstances would a genuine bank or another trusted organisation force you to make a financial transaction on the spot; they would never ask you to transfer money into another account, even if they say it is for fraud reasons. They will always let you call them back on a number you know is real – if they try and stop you doing this, it's a fraudster and you should hang up.

4. LISTEN TO YOUR INSTINCTS If something feels wrong then it is usually right to question it. Criminals may lull you into a false sense of security when you're out and about or rely on your defences being down when you're in the comfort of your own home. If your gut-feeling is telling you something is wrong, take the time to make choices and keep your details safe.

5. STAY IN CONTROL Have the confidence to refuse unusual requests for personal or financial information. It's easy to feel overwhelmed when faced with unexpected or complex conversations. Remember that it's ok to stop the discussion if you don't feel in control of it. If you've taken all these steps and still feel unsure about what you're being asked, never hesitate to contact your bank or financial service provider on a number you trust, such as the one listed on their website or on the back of your payment card.

For more information and resources please visit the Take Five website at: https://takefive-stopfraud.org.uk.

Take Five is a national campaign that offers advice to help consumers prevent financial fraud. This includes email deception and phone-based scams as well as online fraud– particularly where criminals impersonate trusted organisations. Take Five is backed by Financial Fraud Action UK (FFA UK) part of UK Finance, HMG via the Home Office and a range of partners including banks, building societies, law enforcement agencies, commercial, public and Third Sector organisations.

By working together banks, the financial industry, Government and consumers can help to stop fraud.

References and more information:

Action Fraud (2019) Fraudulent investments being advertised on social media, 25/02/2019. Available at: https://www.actionfraud.police.uk/news/instasham-fraudulent-investments-being-advertised-on-social-media. Accessed: April 2019.

Action Fraud (2019) Action Fraud, Springtime tax scams target young and vulnerable, warns HMRC, 24/04/2017. Available at: https://www.actionfraud.police.uk/news/springtime-tax-scams-target-young-and-vulnerable-warns-hmrc

Cifas (2018) The Fraudscape. Available at: https://www.cifas.org.uk/insight/reports-trends/fraudscape-report-2018. Accessed: January 2019.

Experian (2017) Annual Fraud Indicator 2017: Identifying the cost of fraud to the UK economy. Available at: https://www.experian.co.uk/assets/identity-and-fraud/annual-fraud-indicator-report-2017.pdf. Accessed: January 2019.

Experian (2018) UK&I Fraud Report: Analysis of UK Fraud. Available at: https://www.experian.co.uk/assets/identity-and-fraud/uki-fraud-report-2018.pdf?SP_MID=17887-g&SP_RID=8109411-g. Accessed: January, 2019.

FFA UK (2017) Fraud the Facts 2017: The definitive overview of payment industry fraud. Available at: https://www.financialfraudaction.org.uk/fraudfacts17/assets/fraud_the_facts.pdf. Accessed: April 2019.

Home Office (2018) Serious and organised crime strategy. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752850/SOC-2018-web.pdf Accessed: January 2019.

Home Office (2013) Cyber Crime: A review of the evidence. Available at: https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence. Accessed: January 2019.

Maskell, P (2019) Jungo. Cybercrime, Fraud and Scams. https://www.dorset.police.uk/help-advice-crime-prevention/scams-fraud-cyber-crime/

The Metropolitan Police (2017) The Little Book of Cyber Scam. Available at: https://nbcc.police.uk/attachments/The%20Little%20Book%20of%20Cyber%20Scams.pdf. Accessed: April 2019.

National Cyber Security Centre (2018) Annual Review 2018: Making the UK the safest place to live and work online. Available at: https://www.ncsc.gov.uk/news/annual-review-2018. Accessed: April 2018.

ONS (2018) Crime in England and Wales: year ending September 2018. Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingseptember2018. Accessed: January 2019.

PwC (2018) PwC's Global Economic Crime Survey 2018 UK findings: pulling fraud out of the shadow. Available at: https://www.pwc.co.uk/forensic-services/assets/pwc-global-economic-crime-survey-2018-uk.pdf. Accessed: March 2019.

Take Five (2017). Stop and Think. Available at: https://takefive-stopfraud.org.uk/. Accessed: April 2019.

Top10VPN 2019, accessed February 2019, <https://www.top10vpn.com/news/privacy/dark-web-market-price-index-2019-uk-edition/>

UK Finance (2018) Fraud the Facts 2018: The definitive overview of payment industry fraud. Available at: https://www.ukfinance.org.uk/system/files/Fraud%20the%20facts-Digital%20version%20August%202018.pdf. Accessed: January 2019.

UK Finance (2018) 2018 half year fraud update: Unauthorised payment card, remote banking and cheque fraud and authorised push payment scams. Available at: https://www.ukfinance.org.uk/system/files/2018-half-year-fraud-update-FINAL.pdf. Accessed: January 2019.

NCCDSW
National Centre for Cross
Disciplinary Social Work
Bournemouth University

Contact details

We are able to offer a single point of contact for all questions and enquiries regarding all our research Our contact details are below:

NCCDSW Research Team
National Centre for Cross Disciplinary Social Work
Bournemouth University,
Bournemouth Gateway Building
St Pauls Lane
Bournemouth
BH8 8AJ

Email: nccdsw@bournemouth.ac.uk
Website: www.nccdsw.com
Twitter: @nccdsw

This publication had been produced by the Research Team at the National Centre for Cross Disciplinary Social Work, Bournemouth University.

Written and Designed by: Emily Rosenorn-Lanng, Research Project Officer, Bournemouth University.
Additional Content provided by: Stevie Corbin-Clarke, Research Assistant, Bournemouth University.
Dr Sally Lee, Post-Doctoral Researcher, Bournemouth University.
Stephen Forster, National Communications Officer for the National Trading Standards eCrime Team
Paul Maskall, Cyber Security and Privacy Consultant, Jungo