HOUSE OF COMMONS LIBRARY

DEBATE PACK

Number CDP-2019-0133, 29 May 2019

Telephone and online scams

By Lorraine Conway
Grahame Allen
Maria Lalic
Sue Holland
Bess Jap

Contents

Summary

A Westminster Hall debate on Telephone and online scams is scheduled for Tuesday 4 June 2019 at 11.30am. The Member leading the debate is Chris Elmore MP.

1. Introduction

Scams come in many forms, and through different channels. Scams can operate by phone call, text message or email, post, or from an unsolicited visit to the person's home. Advances in technology have enabled scammers to become increasingly sophisticated in their methods. For example, some websites or phone numbers can look like official government sites, with the result that people pay for services that they could get cheaper or for free if they used the official government site (for instance, renewing a passport or driving licence). Phishing emails and texts try to trick the individual into giving out their personal bank details.

Although anyone can fall for a scam, vulnerable people (such as the elderly and those with mental health problems, learning difficulties or dementia) are especially susceptible and are more likely to be targeted. The annual cost of fraud against individuals – including mass marketing fraud and identity fraud – has been estimated at some £9.7 billion. Research conducted in April 2015 by Age UK suggested that 53 per cent of people aged 65+ believed they have been targeted by fraudsters.

All scams should be reported to Trading Standards (via the Citizens Advice online portal) and to Action Fraud. However, many scams go unreported due to the victim's embarrassment or shame. From time-to-time, Trading Standards teams have joined with Citizens Advice to operate 'Scam awareness' campaigns.

Since this Westminster Hall Debate is predominantly concerned with telephone and online scams, the Library's briefing paper, "Nuisance calls: unsolicited Sales and marketing, and silent calls" (CBP 6033) (dated 13 March 2019) may be of most interest. This paper provides detailed information on recent government action and regulators' enforcement action. It also provides statistics on nuisance calls. That said the following information about scams more generally should also be of interest.

2. Scams

2.1 Why people are vulnerable to scams

Scams are schemes designed to "con" people out of their money. According to the consumer body Which?, fraud is now at record levels, with more than 5 million scams costing Britain £9 billion each year.[1] There are many different types of scams and fraudsters have become increasingly sophisticated in the methods they adopt. In terms of spotting a scam, Citizens Advice suggest that a scammer may:

- contact an individual out of the blue;
- make promises that sound too good to be true;
- ask the individual to pay for something up-front (for example, they'll ask him/her to pay a fee before a prize can be claimed);
- ask the individual to make a quick decision by saying things like, 'if you don't act now you'll miss out'; this puts the individual under pressure and doesn't give them time to think;
- be over-familiar and over-friendly with the individual;
- tell the individual that an offer must be kept secret;
- ask the individual for their bank account details; and/or
- give a mobile number or PO Box number as the contact for their company (these are difficult to trace and may be a sign that the company doesn't exist or isn't legitimate).[2]

Vulnerable people are more likely to be targeted by a scam.

People of all ages can be a victim of a scam. As Citizens Advice points out, it is often thought that older people are the most likely to fall for scams, but while this does happen, other age groups can be just as likely to be taken in:

> If you're aged between 35 and 45, you can be caught out by too-good-to-be-true offers and get-rich-quick schemes, especially if you've suffered a difficult situation such as a job loss. For example, there are training scams which affect people who are hoping to improve their employment chances, but which will defraud you of all your money instead.
>
> […] People are often embarrassed to admit they have fallen for a scam or simply refuse to believe they have been conned.[3]

Although anyone can fall for a scam, vulnerable people are more likely to be targeted. Older people and people with mental health problems, learning difficulties or dementia are especially vulnerable to scams.

1 "Join our campaign and help us reach 150,000 signatures," Which?, [online]
2 How to spot a scam", Citizens Advice website, [online].
3 Ibid

2.2 Types of scams

Phishing emails

Often, it is not easy to identify a scam, particularly if 'phishing emails' are used. Phishing emails try to trick a person into giving out personal information (such as bank details). Examples of phishing emails identified by 'Which?' include:

- Lottery scams, which claim that the individual has won a fantastic prize (usually money) in a public ballot but to claim the prize, he/she must first pay a fee or provide their bank details. Of course, there is no prize.
- Government scams, whereby fraudsters send convincing emails that pretend to be from a trusted agency. It is not unusual for phishing emails to cite government organisations to make the email appear more convincing, such as HM Revenue and Customs. The emails ask the consumer to provide their bank details (either by email or by clicking on a link).
- Security scams, which usually involves an unsolicited phone call supposedly from a 'security expert' offering to fix a person's PC or people are deceived into believing they are speaking to their bank.

2.3 Case studies

Box 1: Fake lotteries

The vulnerable are particularly susceptible to lottery or sweepstake scams, often originating from abroad (Spanish, Canadian and Australian lottery scams are among the most common). With such scams, fraudsters usually notify the recipient by telephone, email or letter that they have won a large sum of money in an international prize draw. So that the payment can be processed, the recipient is advised to pay an 'administration fee' and/or supply personal information (such as bank details) and copies of official documents (such as their passport) as proof of identity. Of course, there is no prize and the fraudsters use this information not only to steal the victim's money but also their identity.

To prevent lottery fraud, Action Fraud provides people with the following advice:

- Never respond to any unsolicited lottery communication; if you haven't entered a lottery then you can't have won it.
- Official lotteries in other countries operate in much the same way as the UK's National Lotto; no official lotteries that we know of contact people to tell them of their win.
- We don't know of any official lottery operators who ask for fees to collect winnings. Any request for a fee payment is a good indication that someone is trying to defraud you.
- Never, ever disclose your bank details or pay fees in advance.
- If they've provided an email address to respond to, be very suspicious of addresses such as @hotmail.com or @yahoo.com or numbers beginning with 07 because these are free to get hold of.
- Genuine lotteries thrive on publicity; if they ask you to keep your win a secret it's likely to be a fraud.
- Many fraudulent lotteries have bad spelling and grammar – see this as a warning that fraudsters are at work.
- If a person (or vulnerable relative or friend) has been the victim of a lottery scam, the matter should be reported immediately to the police via the Action Fraud website.

Once an individual has fallen victim of a scam, Action Fraud provides the following advice:

- If you have responded to the email/letter, break off all contact with the fraudsters at once.

- If you have given the fraudsters your bank account details, alert your bank immediately.
- Be aware that you're now likely to be a target for other frauds. Fraudsters often share details about people they have successfully targeted or approached, using different identities to commit further frauds.

People who have already fallen victim to fraudsters are particularly vulnerable to '**recovery fraud'**. This is when fraudsters contact people who have already lost money through fraud and claim to be law enforcement officers or lawyers. They advise the victim that they can help them recover their lost money – but request a fee.

Box 1: Copycat websites

In recent years, people have complained about private companies that set up websites deliberately designed to look like official Government sites and then charge people for services that are available directly from the Government either at no cost or for a much lower fee.

Searching on the internet to apply for a European Health Card (EHIC), book a driving theory test or renew a passport, brings up websites for businesses which offer to check, review and forward applications for a fee. Advertisements for these businesses may feature prominently in search results. It is not unlawful to provide reviewing and forwarding services, but businesses should make it clear on their websites that they are not affiliated to the Government and that people will be paying for a service which they could obtain from the Government for free or at a lower cost.

Unfair and misleading practices are prohibited by the Consumer Protection from Unfair Trading Regulations 2008 (CPRs). The Regulations are enforceable by Trading Standards through the civil and criminal court. The Chartered Trading Standards Institute (CTSI) has published guidance notes for members of the public called "Wise up to the web – avoid being conned by deceptive websites".

In March 2014, the National Trading Standard Board (NTSB) received additional funding of £120,000 to investigate copycat websites. In the March 2015 Budget, George Osborne, then Chancellor of the Exchequer, said the government would give the National Trading Standards Board an extra £250,000 to help it crack down on copycat websites masquerading as legitimate government services.

In certain circumstances, the Advertising Standards Authority (ASA) will investigate misleading websites. The ASA enforces the Advertising Codes; the Codes' overarching principle is that all advertisements are "legal, decent, honest and truthful". The ASA has received complaints about firms that pose as official websites. Typical concerns are:

- It's unclear from the website whether they're an official service
- The company has appeared above the official body on Google search results
- Copycat sites charge fees for services that could have otherwise been free or cheaper
- The consumer did not realise until after the transaction that they would have to pay a handling fee in addition to paying for the service.

The ASA can act against misleading advertisements and has various sanctions at its disposal, including:

- a name and shame section on its website,
- 'ad alerts' advising CAP members to withhold advertising space, and
- methods for seeking the removal of a company's paid for search advertisements

In respect of wider trading practices, for example, where a company is charging people extortionate prices for false services, complaints should be made directly to Trading Standards or Action Fraud.

Box 2: Nuisance phone calls and texts

- Although not scams, nuisance phone calls (i.e. unsolicited and unwanted marketing messages, silent or abandoned calls) and spam texts cause widespread harm and inconvenience especially to the vulnerable, as acknowledged by the relevant regulators – Ofcom (the communications regulator) and the Information Commissioner's Office (ICO).
- Ofcom deals with silent calls while the ICO deals with marketing calls. As well as Ofcom and the ICO, the Telephone Preference Service (TPS) and Silent CallGuard offer advice and assistance. If a person is concerned about unwanted marketing calls, he/she can register their phone number with the TPS. There are also other options, including call-blocking technology, available.

2.4 What people can do to protect themselves?

Report a scam

To report a scam, victims should call the Citizens Advice Consumer Helpline on 08454 040506 or they can use the online enquiry form. If appropriate, Citizens Advice may refer the case on to Trading Standards and action may be taken against a rogue trader. If a person suspects that a fraud has been committed, they can report the matter to Action Fraud via its online reporting tool.

If a consumer suspects that a website may be selling counterfeit goods, they can report the matter to Brand-i. This alert will be forwarded on to the brand-holder's protection department. Brand-i is a directory website in partnership with the Chartered Trading Standards Institute, which provides a list of all the online shops selling genuine branded products.

Register with a preference service

If a person is concerned about unwanted marketing calls, he/she can register their phone number with the Telephone Preference Service (TPS). There are also other options available to deal with scams, including call-blocking technology.

Telephone and mailing preference services

The three main mailing preferences are as follows:

- the Mailing Preference Service (MPS) stops addressed mail; and
- 'Your Choice' preference service stops unaddressed mail.
- Royal Mail also runs its own door-to-door 'opt-out' scheme to stop unaddressed mailings delivered by Royal Mail.

Individuals are protected from unsolicited spam emails through the Privacy and Electronic Communications (EC Directive) Regulations 2003 (the 'PECR'), which came into force on 11 December 2003. The Regulations sit alongside the new Data Protection Act 2018 and the General Data Protection Regulation (GDPR). They give people privacy rights in relation to electronic communications, there are rules on:

Protection against spam emails

- marketing calls, emails, texts and faxes;
- cookies (and similar technologies);
- keeping communications services secure; and

- customer privacy (i.e. traffic and location data, itemised billing, line identification, and directory listings).

The Information Commissioner's Office is responsible for taking enforcement action against organisations that persistently ignore their obligations. Further information is available on the ICO website.

It should be noted that the PECR have been amended several times. The most recent changes were made in 2018, to ban cold-calling of claims management services and to introduce director liability for serious breaches of the marketing rules; and in 2019 to ban cold-calling of pensions schemes in certain circumstances.

Some internet service providers (ISPs) also offer a free filtering service where emails are re-directed to a dedicated inbox folder. The subscriber can then either check this folder for any emails they do not want to receive or choose not to check the folder in which case the filtered emails will usually be deleted automatically after a certain period. Alternatively, an individual could purchase an email filtering product.

2.5 Getting their money back

Individuals who have been scammed do not always get their money back, especially if they have parted with cash or made a bank transfer or if the company is based abroad.

If an individual has responded to an email from a fraudster and sent money, there is no automatic mechanism to get their money back if it's a transaction they have authorised. Proper legal advice should be sought from Citizens Advice or Trading Standards.

If the individual has used a credit or debit card they may (depending on the circumstances) be able to pursue the following options:

- Under section 75 of the Consumer Credit Act 1974 (as amended), a credit card company is jointly and severally liable for any breach of contract or misrepresentation by the trader. However, for section 75 to apply the good or service bought must have cost over £100 and not more than £30,000. Section 75 might be useful where goods or services never materialise, and the trader has disappeared.
- Chargeback – if an individual has bought a good or service with a debit card, they may be able to ask their card provider to reverse the transaction using chargeback. The chargeback scheme applies to all debit card transactions including goods costing less than £100, although exact rules may vary between the various networks. It is important to note that chargeback is not enshrined in law but is part of Scheme Rules, which participating banks subscribe to.
- Unauthorised transactions – if an unauthorised transaction has been made on a person's card then they may be able to recover the money from their bank. The Payment Services Regulations 2009 and the Banking Conduct of Business rules place obligations on banks and building societies to provide a refund in certain circumstances.

- On 28 May 2019, a new voluntary banking industry code came into force to help blameless scam victims who are tricked by "authorised push payment" (APP) scams obtain reimbursement. (see section 2.7 below). Previously, banks only tended to reimburse people if there was an obvious fault in the way the payment was handled by the bank.

2.6 What action is being taken by consumer groups & regulators?

From time-to-time, Trading Standards teams have joined with Citizens Advice Bureaus to operate "Scam awareness" campaigns. The aim being to increase awareness of scams and to provide people with practical advice on how to avoid being scammed. The Action Fraud website highlights the latest scams based on reports from the public.

Scams involving false investment opportunities.

Age UK has also published a guidance note on avoiding scams, "Smart ways to protect yourself", and the consumer body Which? has an online petition to urge the government to take further action to ensure companies safeguard all people from scams.

Scams involving false investment opportunities are common and devastating when they involve the life savings of elderly individuals. The main regulator, the Financial Conduct Authority (FCA), has a statutory objective of "Securing an appropriate degree of protection for consumers". It seeks to do this in many ways; through consumer information/education programmes such as the ScamSmart scheme and the active investigation and prosecution of suspect activity. In 2015, the FCA received over 8,500 reports about potential unauthorised activity, it froze over £2.7 million of assets and returned nearly £1.9 million to victims.

Changes in the law in April 2015 gave people aged 55 and over more flexibility over when and how to draw their defined contribution pension savings. The Government said it recognised that people would need help navigating the expanded range of options and therefore introduced a guidance service – Pension Wise. Nonetheless, concerns have been raised about whether the increase in flexibility might make people more vulnerable to scams. In its report on "Pension freedom guidance and advice" published in October 2015, the Work and Pensions Select Committee recommended that the Government **"**urgently redouble its publicity efforts around pension scams." In its response in December 2015, the Government explained that it worked with the National Crime Agency, regulators and the industry to tackle scams and understand emerging threats. Its anti-scam strategy was also focussed on "improving consumer awareness, to prevent people falling victim to scams in the first place." It would also work with other bodies to consider how to ensure "reported data on pension scams is clearer, and how best to drive forward this agenda, ensuring that there is an ongoing focus on the pension freedoms in 2016."

Pension scams

2.7 What action is being taken by the banks?

On 28 May 2019, a new voluntary industry code came into force to help blameless scam victims who are tricked by "authorised push payment" (APP) scams. This is where people are tricked into transferring money, perhaps because they think they are paying a bank, a business or HM Revenue and Customs (HMRC). This voluntary code sets a new criterion to judge whether customers caught by "authorised push payments" should be reimbursed. In effect, a victim who is a customer of a signatory firm will be fully refunded, if they meet the standards expected of them. However, a victim who has been "grossly negligent" will not be reimbursed. The Payment Systems Regulator has ruled that the code should be voluntary, rather than mandatory. Payment providers (primarily banks) who have signed-up to the code include: Barclays, Lloyds Banking Group, HSBC, Metro Bank, Royal Bank of Scotland, NatWest, Santander and Nationwide.

According to the trade association UK Finance, initial funding provided by the banks is intended to give enough time for the industry to work with the regulators and government to deliver sustainable long-term funding for a reimbursement fund by January 2020. The consumer group Which?, which previously made a "super-complaint" to regulators about bank transfer fraud, also wants banks to publish victim and reimbursement figures on a regular basis.

A separate name-checking service, called "confirmation of payee", works by making sure the name of the account someone is sending money to matches the name they have entered. The Payment Systems Regulator (PSR) has proposed that the UK's six biggest banking groups, which are involved in about 90 per cent of bank transfers, fully put the confirmation of payee measures in place by 31 March 2020.

2.8 APPG on Financial Crime and Scamming

The All-Party Parliamentary Group (APPG) on Financial Crime and Scamming was launched in October 2017. The stated aim of the APPG is to challenge the response to fraud from law enforcement, government, and the public, private and charity sectors. It is also intended to act as a channel for expert briefings on financial crime and scamming to parliamentarians.

On 14 December 2018, the APPG published its report "Young Victims of Financial Crime Inquiry". This followed an inquiry earlier in 2018 which heard and received evidence from law enforcement, financial services, education providers and wider industry. According to this report, young people are at risk of being a victim of fraud and of being drawn into financial crime as a perpetrator. Evidence submitted to the APPG inquiry showed that 41% of money mule accounts are linked to young people aged 25 or under and there was a 24% increase in young people under 21 being involved in fraud either as a victim or perpetrator from 2015 to 2017. The report calls on schools, law enforcement, social media companies, industry and government to do more to tackle this problem.

2.9 Statistics

Statistics on "scams" are not collected. However, this may be a matter of definition – most "scams" will appear in statistics as crimes of "fraud". For example charity fraud is defined as "When fake charity collectors prey on your sympathy by asking you to make a donation to a worthy cause" (Source: Action Fraud) which could start with a "scam" but leads to a crime being committed and it is only at this point would it be recorded as a crime.

Statistics on fraud can be found in the ONS publication: Crime in England and Wales: Additional tables on fraud and cybercrime: year ending December 2018 (published 25 April 2019) – as you will see there are some types of fraud, such as credit card fraud, which may or may not include some "scams".

There is very little information available on the age of victims of "scams". However, there is a 2018 report from the Centre for Counter Fraud Studies at the University of Portsmouth and elderly helpline Reassure: Tackling the Taboo': Talking about fraud and scams to reduce the risk of becoming a victim.

3. Media

3.1 Press releases

Authorised Push Payments Scams Steering Group

New voluntary Code on authorised push payment scams launches today
28 May 2019

GOV.UK

Press release: HMRC warns of landline scams threatening households
2 March 2019

Authorised Push Payments Scams Steering Group

APP Scams Steering Group Agrees Voluntary Code

28 Feb 2019

Pensions Regulator

Scam victims lose more than £1m each to fraudsters
28 January 2019

GOV.UK

Press release: Record number of fake HMRC websites deactivated
30 June 2018

3.2 Articles and blogs

BBC

Scam victims to be refunded by banks

28 May 2019

Which?

Scam victims to be reimbursed under new code: has your bank signed up to protect you?

28 May 2019

Independent

Banking code to protect victims tricked into transferring money to fraudsters

28 May 2019

Observer

I replied to a genuine bank tweet and lost £9,200 to a fraudster

28 May 2019

Times

Beware of cloned ISAs: scammers are pushing fake savings plans online

12 May 2019

BBC

TSB pledges to refund fraud victims

15 April 2019

Guardian

Beware caller ID: it may not be your bank, it could be a fraudster

30 March 2019

Times

The latest scams and ways to avoid them

30 March 2019

BBC

Payment scam victims more likely to be reimbursed

1 March 2019

Financial Times

Scams cost UK investors £197m in 2018

6 February 2019

Guardian

I got a phishing email that tried to blackmail me – what should I do?

17 January 2019

Financial Times

Push payment scams — or modern-day bank 'robbery'

12 October 2018

Guardian

Will victims of bank fraud now get a better chance of justice?

25 August 2018

Financial Times

How one 'push' from bank fraudsters can lose you thousands of pounds

10 August 2018

Financial Times

Time to slam the phone down on nuisance callers

June 2018

Times

For sale: your Netflix account details — and the key to a successful identity scam

4 March 2018

Guardian

Think you can spot scammers? Just 9% of Britons really can

22 January 2018

4. Parliamentary Business

4.1 Debates

Scamming: Vulnerable Individuals,

HC Deb, 8 September 2016, cc507-530

Unsolicited Calls (Prevention)
HC Deb 24 April 2018 c775-7

4.2 Parliamentary Questions

Telecommunications: Fraud
To ask the Secretary of State for Digital, Culture, Media and Sport, pursuant to the Answer of 18 October 2018 to Question 178225 on Nuisance calls, what steps the Government is taking to reduce levels of phishing.

29 Nov 2018 | Written questions | Answered | House of Commons | 194052

Asked by: McCabe, Steve | **Answered by:** Margot James | **Department:** Department for Digital, Culture, Media and Sport

Internet: Fraud
To ask the Secretary of State for Business, Energy and Industrial Strategy, what guidance his Department issues to (a) retailers and (b) consumers to raise awareness of the threat of online scams.

13 Jun 2018 | Written questions | Answered | House of Commons | 149987

Asked by: Simpson, David | **Answered by:** Andrew Griffiths | **Department:** Department for Business, Energy and Industrial Strategy

Internet: Fraud

To ask the Minister for the Home Department, what steps the Government is taking to improve awareness among older people of internet scams

7 Feb 2018 | Written questions| Answered | House of Commons | 127198

Asked by: Andrew Percy | **Answered by:** Ben Wallace

Department: Home Office

Cybercrime

To ask the Secretary of State for the Home Department, what steps her Department is taking to reduce the incidence of cyber-fraud; and by what means she plans to advise the public of the steps to take to protect themselves against such fraud.

8 November 2016 | Written questions | Answered | House of Commons | 52208

Asked by: Amanda Solloway | **Answered by:** Ben Wallace

Department: Home Office

Nuisance Calls

To ask Her Majesty's Government what action they are planning to take to prevent cold calling for pension scams.

10 October 2016 | Written questions | Answered | House of Lords | HL2156

Asked by: Baroness Altmann | **Answered by:** Lord Ashton of Hyde

Department: Department for Culture, Media and Sport

Fraud

To ask Her Majesty's Government what assessment they have made of the adequacy of the law to protect vulnerable people from phone phishing and other communication scams.

23 December 2015 | Written questions | Answered | House of Lords | HL4466

Asked by: Baroness Kennedy of Cradle | **Answered by:** Baroness Neville-Rolfe

Department: Department for Culture, Media and Sport

4.3 Early Day Motions

AUTHORISED FRAUD COMPENSATION

That this House welcomes the publication of the Authorised Push Payment (APP) Scams Voluntary Code due to come into effect on 28 May 2019 to protect customers from APP fraud; notes that during the first half of 2018 consumers lost £92.9 million due to APP scams; further notes that this has caused significant loss and financial instability for individuals and families; commends the banks that have signed up to the code including Barclays, HSBC, Lloyds Banking Group - which includes Bank of Scotland, Halifax, and Lloyds Bank - Nationwide, RBS - which includes NatWest and Royal Bank of Scotland - and Santander; further commends TSB for going further for their customers by promising to refund those who have been victims of APP fraud; urges all other banks to follow their example; further challenges all banks to backdate the compensation to historic cases of APP fraud; calls on the Government to make the Authorised Push Payment Scams code mandatory for all banks; and further calls on the Government to demand banks provide compensation for customers who have fallen victim to APP fraud in the past and pledge to compensate those who will in the future.

20 May 2019 | Early day motions | Open | House of Commons | 2401 (session 2017-19): Primary sponsor**:** Farron, Tim

FRIENDS AGAINST SCAMS

That this House supports National Trading Standards' campaign, Friends Against Scams, which seeks to protect and prevent people from becoming victims of scams; understands that scams affect the lives of millions of people across the UK and that postal, telephone and doorstep scams are often targeted specifically at disadvantaged consumers or those in periods of vulnerability; further supports National Trading Standards' aim to achieve 1 million Friends Against Scams by 2020 in order to tackle the lack of scams awareness by providing information about scams and those who fall victim to them in our communities, as well as highlighting the impact of scams and helping people recognise the signs that someone might be at risk in their community; is deeply concerned by the National Trading Standards Scams Team estimate that such scams cost UK consumers between £5 billion and £10 billion annually; recognises that 98 per cent of those who participated in Friends Against Scams training would recommend the awareness session to other people; and applauds the excellent work of National Trading Standards' Friends Against Scams campaign to ensure that UK consumers are better protected against scams

23 Jan 2018 | Early day motions | Open | House of Commons | 841 (session 2017-19): Primary sponsor: Gibson, Patricia

5. Organisations and Further Reading

Action Fraud

Over £27 million reported lost to crypto and forex investment scams

21 May 2019

Which?

£27 million lost to Bitcoin and other investment scams

21 May 2019

House of Commons Library, *Nuisance Calls: Unsolicited sales and marketing, and silent calls*, 15.03.2019

Age UK, *Avoiding scams Smart ways to protect yourself,* June 2018

Bournemouth University, "Security Minister joins forces with BU to fight financial scamming", 12 June 2018

Bournemouth University, "How loneliness in older people makes them more vulnerable to scams", 24 July 2017

Bournemouth University, "Reality of financial scamming in the UK highlighted during Parliament event", 11 March 2016

Europol, Take control of your digital life. Don't be a victim of cyber scams!

Take Five to Stop Fraud website

The Money Advice Service, Types of Scam

Which?, Phone scams

Which?, Internet Scams

Action Fraud website

Get Safe Online

All-Party Parliamentary Group (APPG) on Financial Crime and Scamming

DEBATE PACK
CDP-2019-0133
23 May 2019

About the Library

The House of Commons Library research service provides MPs and their staff with the impartial briefing and evidence base they need to do their work in scrutinising Government, proposing legislation, and supporting constituents.

As well as providing MPs with a confidential service we publish open briefing papers, which are available on the Parliament website.

Every effort is made to ensure that the information contained in these publicly available research briefings is correct at the time of publication. Readers should be aware however that briefings are not necessarily updated or otherwise amended to reflect subsequent changes.

If you have any comments on our briefings please email papers@parliament.uk. Authors are available to discuss the content of this briefing only with Members and their staff.

If you have any general questions about the work of the House of Commons you can email hcinfo@parliament.uk.

Disclaimer