UTILITIES AGAINST SCAMS A PRACTICAL GUIDE

Supporting your customers and helping employees to spot, stop and prevent a scam.

Utilities Against SCAMS

www.friendsagainstscams.org.uk

ACTION FRAUD 0300 123 2040
CITIZENS ADVICE CONSUMER HELPLINE 0345 404 0506
VISIT FRIENDSAGAINSTSCAMS.ORG.UK/UAS

CONTENTS

CREATED AND SUPPORTED BY

love every drop anglianwater

British Gas

Cadent
Your Gas Network

CONSUMER COUNCIL FOR Water

plusnet
We'll do you proud

sse

YorkshireWater

Document purpose
This guide is for utility organisations of all sizes and in all sectors including energy, water and communications. It offers guidance on how to increase employees' understanding of scams and recommends processes and practices to support utility companies in preventing, spotting and stopping individuals becoming a victim of a scam.

Title
Utilities Against Scams: A practical guide. Supporting your customers and helping employees to spot, stop and prevent a scam.

Publication date
November 2019.

Target audience
Utility companies of all sizes providing essential services to domestic homes – who through daily interactions may come across customers who are at risk of becoming or are already a victim of scams.

It is designed to help employees and interested consumer groups of utility companies wishing to improve their scam awareness and prevention within their organisation by making simple changes. These might include increasing employees' awareness of scams and improving customer experience.

Acknowledgements
With thanks to Citizens Advice and National Trading Standards Scams Team.

Authors
Ash Roberts, Charlie Weston, Ellen Wardle, Janine Shackleton, Jenny Smith.

DEFINITIONS

Communications provider

These organisations provide local, national and international telecommunications services for customers to use at home, at work and on the move. They also provide phone, broadband and TV products and services – including fixed-mobile products and services.

Distribution Network Operator (DNO)

These organisations own and operate the regional networks of cables that bring the electricity to customer homes in geographic areas. They don't sell electricity – this is done by energy suppliers.

Energy supplier

Organisations that look after customers' gas and electricity billing and metering. Customers can have different suppliers for gas and electricity, and can switch suppliers.

Water supplier

Water suppliers operate the network of pipes which provide high quality drinking water and treat the waste water for household customers. The same services are provided to businesses but their water is sold by a retailer.

Gas Distribution Network (GDN)

Similar to the DNOs, the GDNs manage a geographic area of the network of pipes that take gas to customer homes. They don't sell gas – this is done by energy suppliers.

FOREWORD FROM FRIENDS AGAINST SCAMS

Louise Baxter
Head of National Trading Standards Scams Team

As the National Trading Standards Scams Team sees on a daily basis, criminal scams do huge damage to our society. The people who are targeted are often in the most vulnerable circumstances and the impact is huge – from significant financial losses to emotional damage with victims feeling frightened and hopeless.

The aim of the Friends Against Scams campaign is simple – to reduce the number of people falling victim to criminal scams.

When my team created the Friends Against Scams campaign, it was our aim to create a social movement against scams, which is why an aspirational target of training one million people by the end of 2020 was set.

This social change can only happen if businesses, the public sector and voluntary organisations join forces and take a stand against scams together.

I am thrilled that my team has been able to work with the utilities workstream of the National Mental Capacity Forum to create Utilities Against Scams. This important project can only be a positive for consumers and the utility industry.

FOREWORD FROM CADENT

Cadent
Your Gas Network

Jo Giles
Customer Safeguarding Manager
Cadent

As the Customer Safeguarding Manager for Cadent, I focus on a wide variety of vulnerable situations that can affect our customers.

I have the privilege of being the utility lead on the National Mental Capacity Forum (NMCF) and head the utility specific work group which works to create and disseminate practical guidance to companies on the many ways that we can help embed the Mental Capacity Act (2005)[1]. The aim of the utility work group is to co-create approaches to support cross-industry consistency in providing the best support to all of our customers and to implement these in business-as-usual processes.

Scams are becoming more commonplace, more sophisticated and harder to spot than ever before; as utility companies, we are in the privileged position of entering customers' homes for planned and unplanned works.

As a utility work group, responding to this important social issue, our ambition in launching Utilities Against Scams is to:

- Provide a way for utility companies to sign up and commit to taking a stand against scams.
- Create a clear and consistent approach in how essential services of communications, energy and water can spot, stop and prevent scams as we interact with the communities we serve.
- Provide principles based advice to allow companies to support customers, colleagues and good company practice in a way that is accessible to all within their existing resources.

We will be supporting the "one million friends by 2020" ambition by providing utility specific scams training, which has been co-created by our working group and National Trading Standards, to our colleagues and providing these numbers back to Friends Against Scams.

SCAM STATISTICS

SCAMS COST THE UK ECONOMY £5-10 BILLION[2] A YEAR IN COMPARISON TO DOMESTIC BURGLARY COSTING APPROX. £4.1 BILLION[3] A YEAR

THE AVERAGE AGE OF VICTIMS OF MASS MARKETING POSTAL FRAUD IS 75[4]

ONLY 5% OF SCAMS ARE REPORTED[5] AND 7 OUT OF 10 PEOPLE TARGETED DO NOT TELL ANYONE ABOUT IT, INCLUDING FRIENDS, FAMILY OR THE ORGANISATION BEING IMPERSONATED, AS WELL AS THE RELEVANT AUTHORITIES[6]

UNAUTHORISED FINANCIAL FRAUD LOSSES ACROSS PAYMENT CARDS, REMOTE BANKING AND CHEQUES TOTALLED £844.8 MILLION IN 2018, AN INCREASE OF 16% COMPARED TO 2017[7].

PEOPLE HAVE LOST AN ESTIMATED £43 MILLION TO PENSION SCAMMERS SINCE APRIL 2014[8]

THE AVERAGE SCAM VICTIM HAS LOST OVER £3000[9] – OVER 5 TIMES THE AVERAGE WEEKLY HOUSEHOLD SPEND. AVERAGE WEEKLY SPEND IN THE UK WAS £572.60 IN 2018[10]

SCAM STATISTICS

ALMOST 5 MILLION OLDER PEOPLE (65+) BELIEVE THEY HAVE BEEN TARGETED BY SCAMMERS[11]. WHILE ONLY 12% OF THOSE TARGETED RESPONDED TO A SCAM, THIS MEANS AROUND HALF A MILLION OLDER PEOPLE COULD HAVE FALLEN VICTIM[12]

THERE WERE 3.4 MILLION INCIDENTS OF FRAUD IN THE YEAR TO MARCH 2017. OVER HALF OF THESE (57%) WERE CYBER-RELATED[13]

PEOPLE DEFRAUDED IN THEIR OWN HOMES ARE 2.5 TIMES MORE LIKELY TO EITHER DIE OR GO INTO RESIDENTIAL CARE WITHIN A YEAR[14]

53% OF PEOPLE OVER 65 HAVE BEEN TARGETED BY SCAMS[15] – OVERALL ESTIMATED POPULATION FOR OVER 65S IS 12.5 MILLION[16] = 6.6 MILLION TARGETED

23% OF OVER 75S ARE NOT CONFIDENT IN THEIR ABILITY TO SPOT A SCAM[17]

ACTION FRAUD RECEIVES AROUND 7 ROMANCE FRAUD REPORTS EVERY DAY. A QUARTER OF VICTIMS ARE IN THEIR 50S, LOSING £10,000 ON AVERAGE[18]

SINGLE OLDER PEOPLE ARE MORE LIKELY TO RESPOND THAN MARRIED PEOPLE, AND HALF OF ALL PEOPLE AGED 75+ LIVE ALONE[19]

IN 2018 THERE WERE:

3,312 PERSONAL INVESTMENT SCAMS WITH LOSSES VALUING £48.5M[20]

51,208 PERSONAL PURCHASE SCAM CASES WITH LOSSES TOTALLING £42.4M[21]

1,400 CASES OF ROMANCE SCAMS WITH A TOTAL LOSS OF £12.6M[22]

5,112 PERSONAL POLICE AND BANK STAFF IMPERSONATION SCAMS WITH LOSSES OF £49.8M[23]

4,910 CASES OF OTHER IMPERSONATION SCAMS WITH £30.3M LOSSES[24]

3,750,000 OVERALL THEFT OFFENCES[25]

WHY DO UTILITY COMPANIES MATTER?

Utilities standing together against scams.

Utility companies understand the importance of raising awareness around scams as it is a growing issue affecting people globally.

Utility companies interact with customers on a daily basis, whether having a telephone conversation, communicating digitally or face to face when carrying out work in the community or in a customer's home.

With the digital age, it is becoming easier for criminals to pose as legitimate companies and scam people out of large sums of money. This not only impacts customers both financially and emotionally, but also creates reputational risk for businesses and the wider industry.

Utilities have well known and trusted branding and this could be copied by others to look official either on the doorstep, over the phone or via email/ post. As utilities, we can take a stand to help stop this and this guidance provides a number of examples how we can do this in a consistent way.

Also, isolation and loneliness is a growing issue in our society - it doesn't matter where you live, and it's not always age related. However, recent figures show that 200,000 older people have not had a conversation with friends or family for an entire month[6].

Scammers may play upon this to gain trust and become a 'friend' as they might be the only person that customer has seen or spoken to for a number of days or weeks.

We have an opportunity to help spot, stop and prevent scams to support customers to stay safe, warm and independent in their homes. This can be achieved by training our colleagues to understand the signs and what to do if they come across a situation that is linked to a scam or scams.

Why is it important that we focus on this work?

It's important for many reasons. Not least the fact that only 5% of scams are reported[7], and more than 50% of people aged 65+ have been targeted by criminals[3].

There are now 11.8 million people aged 65 or over in the UK. The number of people aged 65+ is projected to rise by 40.77% in the next 17 years to over 16 million. By 2033 the number of people aged 85 and over is projected to more than double again to reach 3.2 million, and to account for 5% of the total population[26].

BENEFITS OF BECOMING A UTILITIES AGAINST SCAMS ORGANISATION

As essential service providers, and as employers, we have a responsibility to help people ensure they are safeguarded from scams and feel confident in communicating with us as a business.

We are well positioned to make a positive difference in helping to eliminate scams. Combined with our community presence, we know our customers well and can play a crucial part in spotting signs of scams in order to signpost support services.

Becoming a Utilities Against Scams organisation instils positivity and confidence, which not only helps customer growth and retention, but also staff morale. The prevalence of scams is growing and almost everyone has been targeted by a scam, whether this be via email or through the post. By becoming involved in such a relatable and emotive issue it keeps customers and our people engaged.

We can also have a positive effect on our customers through scam education and empowerment. The more advice and information we provide people with, the less daunting the thought of going online and interacting with organisations digitally becomes for customers.

Finally, becoming a Utilities Against Scams organisation enables us to collaborate with other utilities and learn from each other and provide examples of good practice.

All of these allow us to make positive steps in raising awareness and preventing the number of those who fall victim to scams, whilst also meaning we positively impact this important social issue.

PEOPLE DEFRAUDED IN THEIR OWN HOMES ARE 2.5 TIMES MORE LIKELY TO EITHER DIE OR GO INTO RESIDENTIAL CARE WITHIN A YEAR[14]

WHAT IS A SCAM?

A scam is a deception, trick or persuasion done to make a person part with something, usually money. Scams come in many forms including fake emails (phishing), romance scams, winning a fictitious lottery or fake prize, selling of fake music venue tickets, or someone knocking on the doorstep pretending to be a professional tradesperson or utility employee.

The reality is that the police would classify these things as fraud. The reason they can happen is that the people committing these acts become very skilled at what they do. They may invest time and money and will be very adept at persuading people to trust them. Documents will be created or websites made to look like the real thing.

Scams don't just affect individuals – businesses and charities can be targeted too and are often exploited by the same criminals.

It's not uncommon for people to be targeted by scam artists repeatedly, if they haven't realised what has happened to them and becoming victims of multiple frauds.

IMPACT OF SCAMS ON OUR SOCIETY

Scams affect the lives of millions of people across the UK on a daily basis. The National Trading Standards Scams Team estimates that the detriment to UK consumers as a result of these scams is between £5 billion and £10 billion a year.

Research shows that being scammed causes 'detriment to the economic and personal health and well-being of individuals and the wider society' (Lonsdale et al, 2016). This research also suggests that victims of scams vary in terms of their awareness of the fraud committed against them, the extent to which they may have unwittingly facilitated the fraud, and the financial detriment they experience.

Relatively inexpensive forms of mass communications, such as the internet, telephone and direct mail, have turned mass marketing fraud activities into a global issue. Many of these scams campaigns target UK consumers but the criminals running them are based outside of the UK. These scams often use the names and logos of legitimate businesses, like utility companies, to convince consumers to hand over money or personal financial details.

Research also shows that mass marketing fraud affects all members of society, regardless of their age, class, occupation, socio-economic background, race or gender.

It is also suggested, however, that certain types of scams appeal more to particular victim profiles, for example older people are particularly susceptible to doorstep salesmen (RAND Corporation, Jack Melling, 2016).

Scams can cause untold distress and damage, particularly for people made vulnerable by their circumstances, such as those living with dementia. The harm done by scams is not limited to financial losses but also includes people feeling threatened, worried about being in their own home and helpless to stop the scams they receive.

The Friends Against Scams project helps tackle the lack of scams awareness by providing information about scams. This information enables communities and businesses to understand scams, talk about scams and cascade messages throughout those communities.

Utilities Against Scams was created to encourage utility companies and their employees to get involved and take a stand against scams together with the National Trading Standards Scams Team.

Friends Against Scams training is available for you to promote to your customers at **friendsagainstscams.org.uk/elearning/UAS**

WHO IS TARGETED AND WHAT ARE THE IMPACTS?

Everyone can be a target. It can be easy for anyone to miss the signs of a scam even if you think you wouldn't fall for it. Criminals look for new ways to trick people and trends such as shopping online, contactless payments and evolving technology mean it's difficult for anyone to confidently say they would never be a victim of a scam.

Scams can have a significant effect on people at an emotional level and the sad truth is that people often feel shame at being scammed and won't tell anyone. Only 5% of scams[5] are reported but we do know that 55% of people over 65 have been targeted[15]. People can feel embarrassed, stop trusting people which can leave them isolated or depressed, and suffer from severe worry about managing their debts. Some people may fall victim to further frauds in an attempt to make up their lost money.

For those targeted, the immediate impact is often losing the money which has been taken by the criminals. The average fraud victim loses over £3,000[9]. For many people even losing a small amount of money can affect their ability to heat their house and pay their bills. Between October 2017 to March 2018, fraud victims lost over £706 million alone[27]. The Annual Fraud Indicator estimates that scams cost the UK economy £190 billion a year[28].

CHALLENGES FACED BY FRIENDS AND FAMILY

Scammers are cunning; they create situations (with their scam offers) that increase the likelihood of poor decision-making. They befriend their target, showering them with promises and leading them into a false sense of security.

Citizens Advice estimates up to 4 million people each year are exploited by scammers.

Often, people who have been the target of a scam cannot admit it to themselves and do not tell anyone through fear of embarrassment and judgement. They even keep it from their family or friends.

Whilst those who are subjected to scams can be left feeling confused, manipulated and ashamed, their friends and family members also suffer when a scam occurs. They are left feeling frustrated and powerless to help their relative, facing the challenges of:

- Identifying a scam is in process or has occurred.
- Approaching the conversation and trying to reveal the true motive of the scammer.
- Refraining from getting frustrated.
- Not forcing the issue, encouraging their family member to make their own choices - regardless of their own personal emotions.
- Maintaining regular contact and supporting them.

Scammers use various communication methods including postal scams, telephone scams, online scams and doorstep scams to draw in their targets.

Family and friends can look out for these tell-tale signs that a scam might be taking place:

- Getting more mail than usual – the letters will often have foreign post marks as many scams come from abroad.
- Receiving many phone calls a day, from unknown numbers.
- Talking about a new partner they met online – mention of sending money to them.
- Receiving repeat visits from strangers, insisting unnecessary work needs to be carried out in their homes (often this is poor quality work for extortionate fees).
- The mention of financial struggles – after spending their money (sometimes their entire life savings) on responding to scams.
- Witnessing self-neglect and living off low quality food – due to financial hardship as a result of the scam.
- Someone falling into a cycle of isolation and distancing themselves from society.

If they think a friend or relative is being targeted, they should raise the subject with them sensitively. They could approach the conversation by asking them about the amount of letters and/or calls received. Remember, always tell them what options available to them, in the form of locally sourced support groups as well as reporting the fraud to Action Fraud.

WHAT DOES BECOMING A UAS ORGANISATION INVOLVE?

CUSTOMER GUIDANCE

COLLEAGUE TOOLS

COMPANY GOOD PRACTICE

For the industry, becoming a Utilities Against Scams (UAS) organisation means:

- Understanding the impact of scams and how they affect customers.
- Considering how a company's processes and services can help customers affected by scams.
- Using this guide to make changes to these processes – this could include training, raising employee awareness of scams and the support available.
- Supporting people who may be showing signs of being targeted by a scammer or have been a victim already, whether they are customers or employees.
- Understanding the support already available for people affected by scams and how to help customers access this support.

It doesn't mean that businesses are expected to:

- Become a Utilities Against Scams organisation immediately.
- Tackle scammers directly or enforce prosecution.
- Ask customers difficult or intrusive questions.
- Breach existing legislation such as the Data Protection Act 2018 and the Mental Capacity Act 2005.
- Ignore normal security processes and procedures.

CUSTOMER GUIDANCE

UAS notebook.

The purpose of this section is to provide details about different types of scams that can impact customers. It is written so companies can copy and share the words directly with customers as a consistent approach to advice.

Scams come in a variety of formats whether it is someone knocking on the door to gain entry, or an email offering a prize in return for money or personal information. As a utility organisation we have recognised three interaction types that are more likely to be targeted by scammers, which are doorstep, telephone and written communication. Further details on scam types can be found later on in this guide.

A customer potentially at risk of becoming a target can be identified in various ways, whether it be an organisation representative on-site or a pro-active identification of risk using the Priority Services Register (PSR) data available. It is also our intent to target high risk areas using data mapping tools and carrying out localised events to offer the products we have created.

We have created customer giveaways to provide tips on preventing scams and these will be sent to customers that are identified as at risk of being a victim of scams. These products include an internal door sticker providing top tips for preventing doorstep scams, which also has an external message warning the scammer that they will be asked to prove their identity. A notebook has also been created for use by the telephone. It details main contacts on the inside page and gives tips on each page.

UAS internal door sticker.

COLLEAGUE TOOLS

Providing quality training to our employees is a key factor in achieving our ambition to prevent, spot and stop scams for both our customers and employees.

We have worked collaboratively across the utility sector with the valued support of Friends Against Scams to create a utility specific training package to highlight how scammers not only target their victim but also how they can impact the individual's mental and physical health.

The training package has been created as computer-based training initially with a view to review this over time to ensure the most effective method is delivered. It encompasses scenario based learning to provide examples of how a contact centre employee can spot the signs of a scam victim. Examples of this could be 'I am waiting for my lottery winnings to arrive' or 'I need to go now as a lovely gentleman contacts me daily at this time'.

Employees attending people's homes are in a unique situation and therefore can have the ability to identify scams visually. They will be given the skills to identify visual and verbal signs that indicate a scam has occurred and how to signpost the victim to their support services.

Employees will be trained in how to prevent, spot and stop a scam. It is also crucial that they understand how we as utility companies are impersonated by scammers. As a representative of a utility company, employees need to ensure that they provide relevant identification and clarification to customers to reassure them of our authenticity and do not apply pressure to gain entry or make a snap decision.

Each organisation should have their own reporting process for scam notifications, which should be communicated out to all employees. Support and guidance should be readily accessible for those impacted by a scam whether it be a customer or an employee.

COMPANY GOOD PRACTICE

Education and awareness around scams is the key to prevention. Utility companies should identify the types of scams which may affect more of their customers perhaps because of the type of utility, the types of customer communication used and from what their customers are telling them.

Helping customers to understand more about spotting a scam and recognising when a communication or engagement is genuine is critical. This can be achieved by creating environments in which people are comfortable talking about scams and confident in identifying them. In order for this to work, focus should be put on raising awareness, providing training and working with external partners who can help spread scam prevention education.

Organisations should offer bespoke scam training for different departments which should be driven by how they come into contact with customers. For example, when educating a call centre agent, particular emphasis should be put on how to spot the signs of a scam over the phone. Equipping them with the tools to identify scams and those at risk is crucial in providing safe environments for customers to talk and report scam activity.

Once a victim of an attempted scam is identified, organisations should have a clear and consistent procedure for reporting scams and empower their people to feel confident in using this. Organisations should leverage their existing external relationships to help signpost customers who have been victims of scams to additional help when needed.

The following case studies highlight some examples of how customers could be scammed.

CASE STUDIES
WHAT GOOD PRACTICE LOOKS LIKE

Employee doorstep unplanned visit

Jenna, Customer Liaison for a water supplier, is attending an incident where the water main has burst causing loss of supply to 350 properties. Jenna's role is to attend properties where vulnerability is identified, using data from the Priority Service Register (PSR), to ensure additional support is provided where needed.

Jenna is wearing a hi-vis jacket with the water supplier's logo on and an ID badge on her lanyard. She visits Mrs White who is registered on the PSR as having a chronic serious illness. Mrs White answers the door with her safety chain applied. She wasn't aware of any issues with the water supply and seemed cautious of allowing Jenna in to the property.

Jenna displays her ID badge stating that she is from the water supplier and there to help. She passes her ID badge to Mrs White and offers Mrs White to close the door and call the water supplier using the number off a recent bill whilst she waits outside. Mrs White accepts this offer and closes the door to contact the water supplier. Jenna waits patiently outside the property until Mrs White returns.

Jenna remains polite and patient throughout her time at the property and provides Mrs White with bottled water.

Good practice to help Mrs White:

- **Wear appropriate ID and uniform.**
- **Offer the customer the chance to clarify ID with organisation.**
- **Remain polite and patient.**

Postal lottery scam

Mark, an emergency gas engineer, is dispatched to Mr Johnson's house following a report of a smell of gas in the kitchen. Mr Johnson is a 71-year-old male living alone. Upon entering the property Mark notices a large pile of mail on the sideboard in Mr Johnson's hallway. Mark immediately thinks this is a large amount of post for an individual person to receive.

Mr Johnson is very happy to see Mark and feels at ease that his gas leak will be made safe. Mark carries out his checks and identifies that the boiler is leaking and has to be isolated for safety reasons. Mr Johnson is advised to contact a Gas Safe Registered engineer (GSR) to get the boiler repaired however upon being told this Mr Johnson states that he doesn't have the money to pay for the repairs until he receives his lottery winnings.

Mark, being even more concerned, shows an interest in Mr Johnson's upcoming fortune and asks which lottery he had played and when did this win happen. Mr Johnson advises it was a postal lottery and he had been randomly selected as a winner. Mark continued to show positivity for Mr Johnson's fortune and asks if he can see the letter he had received.

Mr Johnson, keen to share his great news, locates the letter. Mark immediately spots concerns within the letter where money is requested in order to release the prize. Mr Johnson states he has sent the money off and should receive his prize any day now.

Mark sits down with Mr Johnson, expresses his concerns around the legitimacy of the prize and provides Mr Johnson the contact information for the local Citizens Advice centre to enable Mr Johnson to get the letter checked. Mr Johnson accepts the information and advises he will contact them later in the day.

Mark provides Mr Johnson with alternative heating facilities to ensure he has adequate heat whilst his boiler is awaiting repairs, and leaves the property wishing Mr Johnson well.

Good practice to help Mr Johnson:

- **Don't ignore the signs.**
- **Be considerate of others and show sincere concern for their wellbeing.**
- **Offer support services.**
- **Don't be judgemental.**

Betrayal of trust

Merryn was concerned about the large balance on her aunt's account with an energy supplier. Mrs O'Connor was 78 and had been relying on help from one of her neighbours to look after her bills.

Merryn informed the energy supplier that her aunt had been moved out of her property by social services after it was discovered that her neighbour had been accessing her money and pension, but not paying any bills.

The energy supplier liaised with local police who confirmed the crime reference number provided by the customer's niece was genuine. Given the circumstances, senior manager authorisation was provided to clear the customer's balance.

It is important to understand the circumstances associated with the customer behind every bill and assess each scenario on an individual basis.

Good practice to help Merryn:

- **Listen to the concerns of the customer.**
- **Obtain evidence to substantiate the concern/allegation.**
- **Offer empathy and support when appropriate.**

Clairvoyant scam

Donald had been contacting psychic lines on a daily basis. It's unclear if he was invited to contact them or if Donald sought out the psychic lines himself. Donald is socially isolated and lives alone after his wife, Susan, passed away, so contacted the psychic lines for someone to talk to.

The psychics understood that Donald was vulnerable due to his loneliness and claimed that they could guide him towards a better future if he continued to contact them. Donald also believed that he could contact his wife via the psychic lines and would regularly seek comfort and assurance that Susan was often 'thinking about him'. Donald since became addicted to phoning the psychic lines as these were the only 'friends' he had. He contacted them at all times of the day, including late at night and the early hours of the morning. Calls to the psychic lines are premium rate numbers and cost in the region of £1.50 per minute.

Donald contacted the psychic lines so much that he incurred a telephone bill which amounted to over £6,000, which he could not afford to pay. Donald was at risk of being disconnected from his telephone service due to the high call charges he couldn't afford to pay and all because the 'psychics' played on his vulnerable circumstances in a bid to get him to contact them frequently.

Good practice to help Donald:

- **Proactively identify irregular or unusually high telephone bills.**
- **Contact the customer when they reach a spend threshold to advise of the high calls charges and to prevent further bill shock.**
- **Understand the underlying causes for high telephone expenditure.**
- **Signpost to Bereavement and Addiction Helplines.**
- **Signpost to Action Fraud or the Police if a scam is suspected.**
- **Restrict calls (with the customer's permission) to prevent the temptation to call.**
- **Work with the customer to prevent financial vulnerability – where appropriate, reduce or write off the bill and implement flexible repayment plans.**
- **Set credit limits to prevent bill shock.**

OUR COMMITMENTS

Anglian Water are committed to being proactive when it comes to raising awareness of scams. All of our employees have easy access to a dedicated page on our intranet sites which includes information on scams, appropriate escalation points and signposting as well as training materials accessible via our online learning library.

British Gas commit to continuing to raise awareness of scams and educating our customers, employees and external partners on how to protect themselves. With the support of our internal communications team, we will launch an online scams training module for our staff by the end of 2019. Our frontline staff will strive to identify and respond to customers who may be scam victims and offer guidance on the best ways in which these customers can seek support. We will offer all our people the opportunity to join Friends Against Scams and we are focusing on our customers and staff who are Carers, and the risks associated with looking after a loved one and how you can protect them to live safely at home.

All customer facing staff will complete the UAS training to help them to spot and stop scams where possible through reporting to the relevant agencies. Cadent will proactively identify hot spots of potential scam victims through data tools available to us and to support a greater awareness of scams across our networks. We will deliver 10,000 aids (such as anti-scam door stickers and notepads) to support key guidance to prevent scams as detailed in the UAS guidance.

Consumer Council for Water commit to raising awareness of scams and educating their employees and consumers on how to protect themselves. With interest within the water industry turning towards how water companies can also add social value, we will be challenging water companies to do the same.

Every new employee will complete the Utilities Against Scams training. We are also looking in to incorporating the training in to our existing employees' development plans.

SSE Scam Champions will be working closely with our specialist teams who help our most vulnerable customers. We are also updating our online resources for front line staff, so they can easily access training material and information about the support available to those affected by scams.

Yorkshire Water commit to train 400 of our front line colleagues to ensure we can help identify when our customers may be at risk, on top of reviewing our processes.

TYPES OF SCAMS

PLEASE COPY AND SHARE THE FOLLOWING OVERVIEWS WITH YOUR CUSTOMERS.

DOORSTEP SCAMS

Bogus callers - Distraction burglary
Doorstep callers - Rogue traders

Bogus callers - Distraction burglary

Distraction burglars sometimes work in pairs, where one will distract you on your doorstep, wearing what appears to be a uniform, while the other enters your property elsewhere to steal personal belongings or other personal information.

On other occasions the distraction burglar will pretend to be from a reputable company and distracts you by asking you to perform a task to assist them and while you're doing this they steal your personal belongings or information.

How to protect yourself:

- Don't answer the door to anyone you're not expecting.
- Always ask for an identity badge.
- Ask the caller to wait while you contact the company they are representing (using the telephone number off your bill or the company's official website). If they're genuine they'll be happy to wait outside while you do this.
- Contact a friend or relative to come and check out the doorstep caller for you.

Doorstep callers – Rogue traders

Rogue traders try to scam you by offering to sell you sub-standard products or by offering you overpriced services, such as home improvement work. If you take the scammer up on any of these products or services, the chances are they will come back and ask for more money, or claim that more work needs to be completed. The amount you pay will always be more than the products or services are worth.

How to protect yourself:

- If in doubt, don't open the door. Ask a family member or friend to make some enquiries about the business on your behalf.
- Never agree to any work being done before obtaining quotes from reputable businesses which have been recommended.
- Be wary of callers who wear 'corporate' clothing with logos and lanyards etc. as this doesn't necessarily mean they are genuine.
- If you are not expecting the call and suspect the caller may be a rogue trader call 101, and in an emergency, or if the caller refuses to leave the property call 999.

POSTAL SCAMS

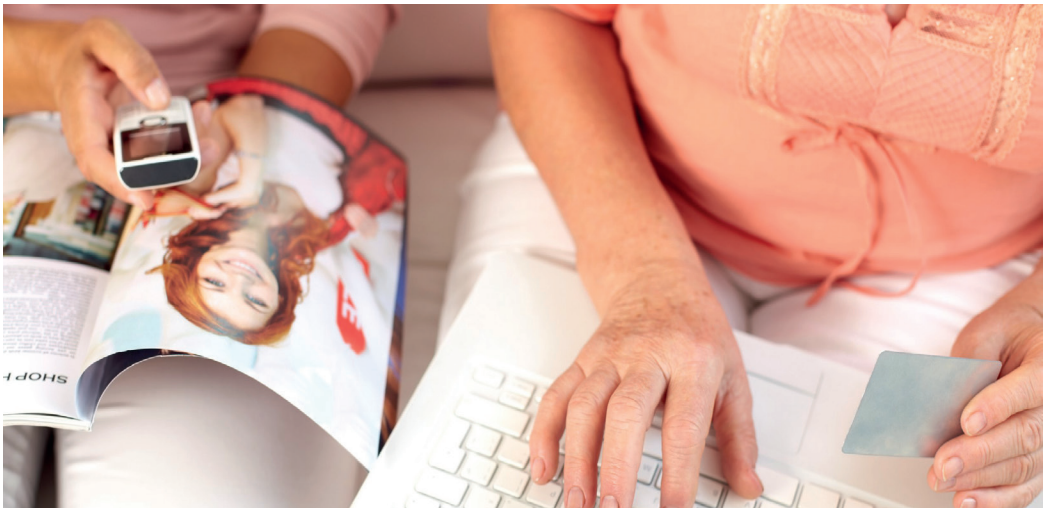
Lottery or prize draw scam
Catalogue scam
Clairvoyant scam
Inheritance scam

Lottery or prize draw scam

The mail you receive will claim that you've won a huge sum of money in a lottery or prize draw. To claim the money you need to pay certain administrative or legal fees to unlock the winnings. You may also be asked to send personal details to verify your identity, such as copies of official documents. These documents are then used to steal your identity. The lottery or prize draw is either fake or sometimes scammers will use the name of legitimate lotteries or prize draws to make them seem genuine and the scams usually come from overseas.

How to protect yourself:

- Don't respond to unexpected mail with claims of lottery or prize draw wins.
- You can't win a lottery or prize draw you haven't entered.
- If you've been asked to keep the win a secret, it's highly likely to be fraudulent.
- Official lotteries won't ask you to pay any fees to be sent the winnings.



Catalogue scams

You'll receive mail asking you to buy home, beauty or fashion products in exchange for a guaranteed prize if you do so. Although you've bought the goods, the prize never arrives. Instead you receive further mail or phone calls asking for purchases of other products in exchange for bigger and better prizes. If you do receive the products, they are either of little or no value.

How to protect yourself:

- Don't respond to mail or catalogues you're not expecting.
- Don't buy products on the promise of a guaranteed prize. Legitimate organisations won't ask you to do this.

Clairvoyant scam

'Psychics' may contact you via email, telephone or post claiming that they can predict your future in return for payment. Often scammers claim that something bad will happen in your future and that the psychic can protect you from this if you continue to pay them. Some may ask that you purchase expensive items, such as jewellery, to send to the psychic in return for a more favourable future. Others may ask that you purchase lucky charm items for the same reason, however if you receive the items they're worthless. If you stop paying for your predictions or help with so-called future events, the psychic may threaten to cast a curse on you or claim that your future will take a negative turn.

How to protect yourself:

- Don't respond to calls or mail that you're not expecting.
- Be wary of callers claiming that they know something about you. The chances are the information they claim to know in order to prove they're genuine can apply to anyone or may be information easily obtained, such as from social media sites.
- Don't send money to the psychics.
- If you do want to engage a psychic, find reviews of reputable psychics and ensure you're aware of all the costs associated. Don't send money for any unexpected costs or items.

Inheritance scams

You may be contacted via email, telephone or post from someone posing as a lawyer or other official claiming that you're entitled to claim the inheritance of a distant relative, or an unrelated wealthy client who shares the same last name as you.

The typical sums of money involved in this type of scams are quite large, so scammers (to sound bona fide) will advise that because of this you'll need to provide your personal details to verify your identity or pay administrative fees to access the inheritance.

How to protect yourself:

- If you are asked for a fee to release the 'inheritance' this is likely to be a scam.
- Look out for badly written text or spelling mistakes.
- Legitimate companies will often have a formal email address rather than using addresses like '@hotmail.com' or '@yahoo.com'
- If someone proposes you can access some inheritance as you share the same surname of the deceased this again should cause alarm bells to ring.
- No legitimate lawyer or company would ask you to keep something a secret.

TELEPHONE SCAMS

Billing scam
Service interruption scam
Pension and investment scam
Computer scam
Clairvoyant scam (see Postal scams)

Billing scam

You may be contacted by a scammer posing as one of your utility companies (gas, electric, telephone). If they do not claim to be your utility provider, they may claim to be from one which is closely associated with them. They may be able to confirm some very basic details about you to verify their identity, such as your name and address. Often the scammer will claim you're due a refund on your bill and to process this refund back to your account they just need your bank details. You won't receive your refund but the scammer now has enough details to access your bank account.

How to protect yourself:

- If you're not expecting a refund or don't suspect you've overpaid, then the chances are the call isn't genuine.
- Refunds are usually credited back to you on your next bill. If you're being asked for bank details for a refund, hang up the phone.
- Contact the company directly using a trusted number (i.e. from a genuine bill) and ask them if they've attempted to contact you. They should have a log on their systems.

Service interruption scam

A scammer will contact you by telephone claiming to work for one of your utility providers (gas, electricity, water, telephone or broadband). They may be able to confirm some very basic details about you to verify their identity. They'll claim that there's some outstanding money that's owed to them and that if you don't pay this immediately your service will be cut off. Once you've provided your bank details to make this 'outstanding payment' the scammer has enough details to access your bank account.

How to protect yourself:

- Are you being pressured into making a payment? Is there a sense of urgency to do this and you've not been aware of this 'outstanding payment' before? If this happens the call isn't genuine.
- Legitimate companies won't contact you out of the blue and threaten to cut off your service or supply if you don't pay immediately.
- Contact the company directly using a trusted number (i.e. from a genuine bill) to check the status of your account.

Pension and investment scams

Pension and investment scammers attempt to lure you into transferring your pension(s) or savings to them with claims of guaranteed high returns and up-front payments. You may be offered a free pension review with a no obligation consultation. If you decide to invest your pension or savings into another scheme, these are either high-risk investments, such as parking or overseas properties, or the money is stolen outright and not invested at all.

How to protect yourself:

- Don't accept unexpected calls.
- Don't be pressured into making a quick decision.
- Look out for claims of high guaranteed returns. If the investment seems too good to be true then it probably is.

Computer scam

A fraudster contacts you pretending they're from your broadband provider or other IT support company, claiming that there is a fault or virus on your computer (a provider will normally wait for you to report a fault). Only the caller can help you to remove the virus and if you don't take immediate action the computer will stop working and its contents will be lost.

The caller either requests a payment over the phone to fix the computer, or asks you for remote access to remove the virus. Using remote access, the fraudster is able to steal personal details stored on your computer. The personal details will often be used to take money from your bank account.

How to protect yourself:

- Don't accept unexpected calls. Hang up if you receive a call claiming to be from your broadband provider.
- Don't provide payment details over the phone to an unknown company who have contacted you rather than you contacting them for a service that you want.
- Don't allow remote access to your computer.
- Look out for claims that only the caller can fix the issue. Check with your broadband provider's IT support or install and run anti-virus software. Free antivirus software is available to download online.

ONLINE SCAMS

Phishing
Pharming
Ransomware
Impersonation scam
Romance scam
Clairvoyant scam (see Postal scams)

Phishing

Phishing emails often look professional and from a trustworthy source, such as your bank, utility provider or Government body.

The purpose of a phishing email is for the scammer to obtain your password. The email usually demands that you update your password or other information urgently to prevent account closure, pressurising you to act there and then.

How to protect yourself:

- Don't open emails you're not expecting.
- Don't click on links or open attachments contained in emails asking you to update your details.
- Never update your details, such as your password, via one of these emails. Reputable companies will not ask you to do this.
- Check for spelling mistakes and poor grammar.
- Is the email address genuine? Does another email address appear if you hover over the displayed email address? If this happens the email is highly unlikely to be genuine.
- If you're unsure if an email is genuine, access the company's website by using a trusted URL in your web browser.

Pharming

Pharming is known as a 'cyber-attack' where malicious code is installed onto your personal computer or a server, which directs you to a fake website. This usually happens without your knowledge or consent. The purpose of this scam is to trick you into believing you're accessing a trusted website, such as your bank, where you'll enter your personal details (for example, username and password). The fraudster then has your personal details and can steal money from your bank account.

How to protect yourself:

- Don't open links in emails that you don't trust or know.
- If you do want to follow a link remember it is better to enter a trusted URL directly into your web browser so you know you're accessing a legitimate website.
- Check the URL is spelled correctly.
- Check if there's any difference to the look of the website you're trying to access.
- Check if 'https' has been used at the beginning of the URL.
- Clear your DNS cache.
- Run anti-virus software.

Ransomware

Ransomware is a type of malware which takes control of your computer system until a ransom is paid to remove it. Ransomware can be installed on your computer system by downloading an email attachment or clicking on an email link or by visiting a malicious website. The purpose of the ransomware scam is to extort money from you so that you can regain access to your computer system and files.

How to protect yourself:

- Don't click on email links from unknown or untrusted emails.
- Don't open attachments from emails you weren't expecting or don't trust.
- Always use trusted URLs to access a website.

Impersonation scams

Online impersonation scams are similar to phishing emails by claiming to be an official body, such as the Government or utility company. The email will claim that you're due a refund or that you need to make an urgent payment. Both require you to enter your bank details, which are then stolen and used to access your bank account.

How to protect yourself:

- Don't act on the email immediately. Stop and consider if the email is pressurising you to do something and if there's a sense of urgency to do it.
- Don't enter your bank details. Most companies will not ask you to make an urgent payment online.
- If you're unsure, access the company's website with a trusted URL in your web browser.
- Contact your provider directly if you're unsure.

Romance scam

Scammers often use dating apps and websites, creating fake profiles and preying on people looking for a romantic partner. They attempt to gain your trust by providing written and verbal affection and sharing personal information. Once they've gained your trust they start to ask you to send them money, often for a personal emergency (such as needing money for personal treatment, a sick family member or suffering from financial hardship). Once you've sent them the money they will often come back and ask for more.

How to protect yourself:

- Be wary of very quick and strong romantic feelings towards you.
- Look out for excuses to not meet you in person or video call.
- Is their profile picture genuine? Does it appear anywhere else on the internet or on other dating websites under different names?
- Check that their life story is consistent. If the person is disingenuous their story will change over time.
- Don't send them any money. Look out for stories of personal emergencies requiring financial assistance.

HOW TO JOIN UAS

Utilities Against Scams is part of the Friends Against Scams initiative developed by the National Trading Standards Scams Team to protect and prevent people from becoming victims of scams by empowering people to take a stand against scams.

www.friendsagainstscams.org.uk

All utility companies are being encouraged to join Utilities Against Scams to demonstrate their commitment to scams prevention work.

Members of the NMCF Utilities Working Group have worked with the National Trading Standards (NTS) Scams Team to develop a version of the Friends Against Scams (FAS) training specifically for the utilities industry. This training is available on PowerPoint free of charge to any utility company that becomes a Utilities Against Scams company along with access to key social media messages and tailored consumer materials that have been developed by the group.

How to become a Utilities Against Scams organisation

Your company can become a UAS organisation if they are prepared to commit to the following:

Promotion – ensuring that the FAS initiative is promoted to your customers by actively distributing the materials that have been developed

Training – giving your staff access to the UAS training materials and agreeing to feed back the number of staff trained to the NTS Scams Team

In addition to these commitments above, it would also be useful if your company could:

Pledge – make a pledge about the work you are planning to support Utilities Against Scams

SCAMbassador – consider signing up at least one senior 'SCAMbassador' within your company. This person should be able to help raise the profile of UAS and scams awareness in your company, such as a Chief Executive or a Director

Social media – actively support UAS on social media by using the hash tags #FriendsAgainstScams #ScamAware

If you would like to become a UAS organisation, please contact the lead contact in the NTS Scams team, Nikki Pasek – **nikki.pasek@surreycc.gov.uk**

FRIENDS AGAINST SCAMS PARTNERSHIP

In addition to supporting Utilities Against Scams, utility companies also have the additional option of becoming Friends Against Scams (FAS) partners.

Friends Against Scams partner businesses are essential in helping to provide the resources that are needed to continually develop the Friends Against Scams initiative.

As a partner, you will be demonstrating your company's commitment to working in partnership with the National Trading Standards Scams Team and providing the initiative with vital support.

Your logo, with a link to your website, will be added to the FAS homepage and you can benefit from a number of bespoke services, such as branded UAS training in a format compatible with Learner Management Systems and joint social media campaigns with the team.

In addition to their standard partnership package, the team are also happy to work on bespoke partnership development with companies if there is a particular scams related issue that they wish to research or develop further.

Partnership packages start from £10,000 for the first year, with an ongoing annual fee of £2,000 to maintain the partnership.

Please contact the lead contact in the NTS Scams team, Nikki Pasek, if you would like to discuss partnership options further – **nikki.pasek@surreycc.gov.uk**

REFERENCES

1. The Mental Capacity Act 2005, legislation.gov.uk, 16 May 2019
2 FAS Website homepage, friendsagainstscams.org.uk, October 2019
3. The economic and social costs of crime Second edition Research Report 99, Matthew Heeks, Sasha Reed, Mariam Tafsiri and Stuart Prince. July 2018
4. Older people, fraud and scams, Age UK, October 2017
5. FAS Website homepage, friendsagainstscams.org.uk, October 2019
6. Changing the story on scams. Protecting consumers and increasing reporting. Xanthe Couture and Anne Pardoe, citizensadvice.org.uk
7. Fraud the facts 2019, UK Finance, March 2019
8. Older people, fraud and scams, Age UK, October 2017
9. FAS Website homepage, friendsagainstscams.org.uk, October 2019
10. Family spending in the UK: April 2017 to March 2018, Office of National Statistics, Tracy Williams, 24 January 2019
11. TNS Research Express polling for Age UK, June/ July 2017 – sample of 1,367 people aged 65+ in GB
12. TNS Research Express polling for Age UK, June/ July 2017 – sample of 1,367 people aged 65+ in GB
13. Fraud and economic crime, CPS, www.cps.gov.uk/fraud-and-economic-crime
14. Older people, fraud and scams, Age UK, October 2017
15. FAS Website homepage, friendsagainstscams.org.uk, October 2019
16. Population estimates for the UK, England and Wales, Scotland and Northern Ireland: mid-2018, Office of National Statistics, Neil Park, 26 June 2019
17. Changing the story on scams. Protecting consumers and increasing reporting. Xanthe Couture and Anne Pardoe, citizensadvice.org.uk
18. Older people, fraud and scams, Age UK, October 2017
19. Older people, fraud and scams, Age UK, October 2017
20. Fraud the facts 2019, UK Finance, March 2019
21. Fraud the facts 2019, UK Finance, March 2019
22. Fraud the facts 2019, UK Finance, March 2019
23. Fraud the facts 2019, UK Finance, March 2019
24. Fraud the facts 2019, UK Finance, March 2019
25. Crime in England and Wales: year ending March 2019, Office of National Statistics, Meghan Elkin, 18 July 2019
26. FAS Website homepage, friendsagainstscams.org.uk, October 2019
27. Action Fraud, What is Fraud and Cybercrime, actionfraud.police.uk/what-is-fraud
28. Action Fraud, What is Fraud and Cybercrime, actionfraud.police.uk/what-is-fraud

CREATED AND SUPPORTED BY

love every drop anglianwater

British Gas

Cadent
Your Gas Network

CONSUMER COUNCIL FOR Water

plusnet
We'll do you proud

sse

YorkshireWater

Utilities Against SCAMS

www.friendsagainstscams.org.uk