Scams glossary

There are lots of different types of scams, and people can be targeted in many ways - whether that's phone, email, mail or even in person. Here are some common types of scams to look out for in your community.

Scams and the Cost of Living

The increased financial pressure many will be facing has put more people into difficult situations, with many facing issues with debt and being able to afford essential goods and services. Scammers are likely to exploit these pressures.

Scams to look out for include:

- **Scammers pretending to be energy companies, using high energy prices to lure people into "too good to be true" deals in order to steal their money**
- **Fake sales representatives selling counterfeit shopping vouchers**
- **Fraudsters sending out phishing emails pretending to offer an energy rebate or government support to steal people's personal information**

Common scams

- **Antivirus/computer** - People are cold called and told they have a problem with their computer which, for a fee, can be fixed. Alternatively the victim might initiate the contact in response to an online advert or prompt claiming that their device has been infected with a virus. Other computer scam methods involve offering bogus virus protection or warranties
- **Contactless card scams -** Contactless cards are 'skimmed' (where details are read or copied) by a card reader or phone nearby
- **Copycat Government official service scams** – Scammers claim to be official government departments and sell services for a 'fee'. For example, they might claim to help process passports or driver's licences. They use channels like phone and text, email and fake websites.
- **Credit Card Scams -** This is where customers give credit card details to buy a genuine product/service and those details are sold to a scammer. The scammer sets up a fraudulent purchase of, for example, an expensive mobile phone. They then send you something of no or little value by tracked delivery so that when you challenge the purchase they have a delivery receipt
- **Cryptocurrency scams** - These are a type of investment scam, where someone offers a fake, but often convincing, opportunity to make a profit by investing

money in cryptocurrency - virtual peer-to-peer currency that is decentralised and only exists online. These scams may involve: a fake cryptocurrency which doesn't and won't ever exist – for example if it's a fake Initial Coin Offering (ICO); a bogus investment which promises to put money in a legitimate cryptocurrency; a dangerous website link that then downloads malware onto your computer. For more information about these scams, Kaspersky has a summary of the different types of cryptocurrency scams

- **Delivery text/email scams** - These can be text messages or phishing emails pretending to be from a delivery courier like DPD or Royal Mail. These messages claim that you have missed a delivery and ask you to reschedule for a fee, thereby obtaining your bank details. Whilst it can start with a small fee, it can end with criminals emptying a person's entire bank account

- **Doorstep/street selling** - These all begin with the person getting an unrequested knock on their door. They are often for expensive home improvements which the victim did not want or was pressured into. Another variation of this can be where someone agrees to a service, such as having their gutters cleaned, and the trader then 'discovers' a larger problem (e.g. a roofing 'fault') which needs to be corrected at huge cost.

  Read more information on our website about consumer's rights if they've been mis-sold items on the doorstep or have been pressured into signing a contract

- **Fake Service / invoice** - This also covers a wide range of situations, but asks for payment for either a service the scam victim has never heard of or for a service which ended up being non-existent. Read more about these scams at Experian.

- **HMRC Scam -** These often involve receiving a call (often automated) saying you have committed tax fraud and you should press one to make a payment to avoid a prison sentence

- **Investment -** Often conducted either online or over the phone, these can result in people losing thousands of pounds for non-existent stocks, shares and other investments such as rare wine or art. These will sometimes involve scammers 'wining and dining' investors to convince them it's genuine. Average losses are very high - the BBC reports that victims last year lost an average of £45,000

- **Job scams** – Scams include taking money to write CVs or carrying out security checks. Some ask for bank details to pay (non-existent) wages, others offer expensive training programmes (or even jobs) that don't exist

- **National Insurance (NI) Scam -** You receive a call stating that your NI number has been compromised and you should press 1 to obtain a new one and you are connected to a premium cost number

- **Online shopping and auction sites -** Items are advertised for sale, often at a bargain price with pictures to make it appear more genuine. The buyer may be

pressured into paying via bank transfer instead of a third party payment service. Once the payment is made the item is either not received or is counterfeit.

- **Pension scams** – Pension freedoms introduced in April 2015 give consumers added flexibility but it's essential they make informed decisions using trusted sources. The Citizens Advice report 'Too good to be true' calculates that 8.4 million people have been offered unsolicited pension advice or reviews since April 2015, and that 88% of consumers selected a pension offer containing scam warning signs, including out of the blue offers promising high returns, pressure to sign paperwork, and offers to access pensions before the age of 55

- **Phishing** – Emails and harmful links designed to deceive people into revealing personal/financial details. By spoofing emails, email addresses, websites and payment services, scammers can trick people into believing they are dealing with genuine banks, traders and/or authorities

- **Premium Rate Number Scams -** You look for the number of a government department online and see an advert for the phone number of the relevant government advice line that looks genuine. It does put you through to the right department but it is actually a premium rate switching number that charges you a high connection fee – in some cases, as much as £20 or £30 a call. It's always best instead to look for the number directly from the official government website

- **Refund Scam -** Often involves getting a letter or email from a utilities company saying you are entitled to a 'refund' and asking you to confirm bank details to receive the repayment. This has also been a common HMRC scam in the past, with scammers using emails and texts to trick people into thinking they are owed a tax rebate, resulting in people handing over their account and personal details

- **Romance Scams** - Romance scammers create fake profiles on dating sites and apps, or contact their targets through popular social media sites like Instagram, Facebook, or Google Hangouts. The scammers strike up a relationship with their targets to build their trust, sometimes talking or chatting several times a day. Then, they make up a story and ask for money - usually a 'disaster story', like needing to pay for medical treatment urgently or claiming to be kidnapped. The scam can take place over a long period of time and cause significant financial loss and emotional distress. Read our blog on how to avoid romance scams

- **Remote Access Scam -** This involves the scammer convincing people to allow them remote access of their computer to fix something, but this allows them access to personal data and even direct access to people's bank accounts if they have stored the login information

- **Smishing** – Text messages used to lure people into scam websites or inviting them to call premium rate numbers or download malicious content

- **Subscription traps or free trial scams** – Some unscrupulous companies use subscription traps, and in particular continuous payment authority (CPA), to help

themselves to consumers' accounts. Common ones include those offering health and beauty-related products such as slimming pills or skin creams

- **Telephone Preference Service (TPS) or call blocking scams** – Scammers demand payment for the free TPS or sell call blockers which either do not work properly or are part of an expensive subscription service.

- **Ticket scams** – Consumers buy tickets for an event that is already sold out or the tickets haven't yet gone on sale. The tickets then either do not arrive or are fake. Consumers should use credit cards or secure payments and ensure purveyors are members of STAR – Society of Ticket Agents and Retailers.

- **Universal Credit scams** - Someone offers to apply for a Universal Credit Advance Payment on your behalf and takes some of the money as a fee. Victims can be approached both online through social media groups, direct messages and adverts, or in person by smartly dressed people claiming to be from Jobcentre Plus

- **Upfront payment/fee scams** - This covers a wide range of situations and scam delivery channels, but they usually ask for an upfront payment to unlock either a cash prize, a PPI claim amount or for initiating a service. This also includes loan fee fraud: scammers prey on individuals who have a bad credit rating or who need a loan quickly are asked to hand over a fee – usually between £25 and £450 – when applying for a loan or credit that they ultimately never receive.

- **Vishing** – This is where the consumer received a cold call aimed at extracting personal information and details from them. Scammers impersonate someone from a trusted organisation, such as a bank, to manipulate people into transferring money or pass on financial/ personal details