Scams glossary

Here are some common types of scams to look out for in your community.

Coronavirus scams

There are many new scams around at the moment as a result of coronavirus. Scams to look out for include:

- **Adverts for face masks or medical equipment at high prices**
- **Adverts selling fake cures for coronavirus**
- **Emails or texts pretending to be from the government**
- **Emails offering life insurance against coronavirus**
- **People knocking at your door and asking for money for charity**

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. While this is a relatively new crime and reporting figures are low, there has been media speculation about the rise of this type of scam.
- **Copycat Government official service scams** – Callers or websites claim to be official government departments and sell services for a 'fee'. For example, they might claim to help process passports or driver's licenses. Universal Credit scams have also been widely reported, where 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.
- **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. For example, Citizens Advice and UK energy companies recently warned the public to stay safe and guard against scammers on the doorstep claiming to be energy network engineers who are trying to take advantage of the uncertain and worrying times.
- **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. For example, there have been reports of fraudulent invoices being submitted to owners for the provision of medical testing services in relation to the coronavirus.

- **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. Average losses are very high. For example, the Financial Times recently reported that scammers are exploiting fears over Covid-19 to persuade investors to withdraw money from their investments.
- **Job scams** – Scams include taking money to write CVs or carrying out security checks. Some offer expensive training programmes that don't exist, some even offer jobs that don't exist!
- **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. The BBC recently reported that social-media sites, including Facebook and Twitter, have been used as platforms by scammers to sell people's personal details as well as stolen credit-card details and Netflix and Uber Eats accounts.
- **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. The report also showed 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.
- **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. The government has reaffirmed their commitment to tackle subscription traps and empower consumers, but in the meantime, consumers still need to take care.
- **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.
- **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.