Friends Against Scams
Guide to scams (additional reading)

Mass Marketing Scams are a crime where victims are persuaded to part with money as a result of postal, telephone or electronic communication received into the home. Examples would include fictitious prize draws, false investment opportunities and clairvoyant or dating scams

Doorstep Scams are where victims are cold called at their homes and persuaded to part with money as a result of rogue trading activity. Examples would include money taken for unnecessary work, for work not completed or where an extortionate price is charged. Offenders of this crime can use intimidating and aggressive behaviour and also befriending and grooming techniques to facilitate offending and repeat victimisation.

There are many different types of scams in existence, but the Friends Against Scams session focuses on four main types of:

1. Postal Scams
2. Telephone Scams
3. Online Scams
4. Doorstep Scams (or Doorstep Crime)

Postal Scams

Postal Scams come in many forms and attempt to extract personal details, financial information or money.

Lottery or Prize Draw Scams - claim that victims have won large sums of money on fictitious lottery or prize draws.

- Lottery and Prize Draw Scams are similar in nature.
- Normally a letter is sent claiming that victims have won a large or life changing sum of money on a lottery or prize draw that, in most cases, they didn't actually enter.
- Usually the winnings are for an overseas lottery, such as the Spanish Lottery, Australian Lottery, Canadian Lottery, etc.
- To claim the winnings, victims must contact an official and provide their personal details and financial information.
- They are also requested to send a fee to release the funds, often referred to as a processing or administration fee or to cover taxes.
- The fee is usually a small sum of money, commonly less than £50, which is purposely set so low (almost unnoticeable) to ensure that people think that the benefits/windfall outweigh the risks.

- Victims will be told to keep their winnings a secret to avoid people trying to 'scam' them or pester them for hand-outs. They are also asked to respond quickly otherwise the money will go back into the lottery and be added to the next winner's amount.
- The winnings do not exist and the criminals have obtained a great deal of information to help perpetrate additional crimes.
- Invariably, the victim will be contacted with requests for more fees, such as a small percentage of tax for the government, before the winnings can be released and additional exploitation will occur.

The **Prize Draw Scam** is a variation of the Lottery scam, whereby an alleged winner of a large amount of money is asked to send fees to release the windfall. Typically the winnings are less than for the lottery and may be shared by a few other winners.

Catalogue Scams - sell worthless or misleading products, e.g. home/garden products, 'miracle cures', vitamins, etc. whilst also claiming that victims have won money on non-existent prize draws but a purchase must be made in order to claim the winnings.

Catalogue Scams sell: food, toiletries, home and garden products, vitamins and 'miracle cures', which are misleading in nature as it is highly unlikely that such products have been properly tested or that there is any proof that they are medically effective. Some of these products may even be harmful.

- These products are often described as 'luxury', high quality and sold at bargain prices but are in fact highly overpriced, standard, sub-standard or are of no value.
- Although the items do physically exist they may or may not be received by the individual.
- Victims are usually entered into a fictitious prize draw as an incentive to continue ordering. The victim is more often than not told that they are a guaranteed winner and all they need to do to claim their winnings is to purchase a product.

Clairvoyant Scams - offer predictions of the future and requests payment for further information.

- These scams are effectively blackmail.
- Clairvoyant Scams lure victims by offering contact with a deceased relative – individuals going through a recent bereavement may be particularly susceptible.
- A variation of this scam is a letter stating that something wonderful (e.g. a lottery win) or terrible (e.g. a stroke or car crash) have been seen and are about to happen to either the individual or to a family member. They may be instructed to send protection money or purchase a 'lucky' talisman, or object to protect themselves.
- An even darker side of this scam is where a victim is warned that evil spirits exist upstairs and will get them if they do not keep up protection payments to the clairvoyant.
- Some victims have been known to live in constant fear and do not have enough money to pay for electricity and heating bills due to the regular payments they are making to the clairvoyants.

Inheritance Scams - is when an overseas lawyer or official contacts the victim stating that money from the Will of a recently deceased individual is due to them.

- Normally a lawyer or official from overseas contacts the victim stating that they have been processing the will of a recently deceased person who shares the same last name as the victim.

- The lawyer or overseas official states that they have not been able to identify any legitimate relatives and propose that they pay the large inheritance to the victim. The lawyer or overseas official will take a cut (rather than all of the money going to the government).
- Unbeknownst to the victim, the inheritance does not actually exist and the official or lawyer does not exist either but is in fact a criminal.
- The victim is instructed to keep quiet and act quickly.
- Before any inheritance can be paid into an account, administration, banking fees and taxes are required.
- After these fees are paid some type of 'unforeseen problem' will occur, and subsequently the criminals will demand additional fees and payments from the victim.

Telephone Scams

Communication by telephone is another method used by criminals as it is a very effective and easy method by which personal details and/or financial information can be obtained.

Sometimes the telephone is the only means used but it is often used in conjunction with other scams. For example, with postal scams the criminals may call a victim and instruct them to look out for a specific piece of mail and respond accordingly.

Vishing – a telephone call is used in an attempt to steal personal information.

- Vishing is the act of using the telephone in an attempt to scam the victim into divulging their personal information, which will then go on to be used for the purposes of identity theft.
- Criminals often pretend to be a genuine business, and mislead the victim into thinking that there will be a benefit to them by responding to their requests for information.

SMShing - occurs when mobile phone SMS text messages are used in an attempt to scam the victim into divulging their personal information. Furthermore, the SMS texts also try to:

- Lure the victim onto fraudulent websites.
- Invite the victim to call a premium rate mobile number.
- Request that the victim clicks on a link through the text, which will then download malicious content via the phone or web.

Investment or 'Boiler Room' Scams – a telephone call offers worthless, overpriced or non-existent shares.

- Investment or 'Boiler Room' Scams are share scams.
- They are often run from 'boiler rooms'.
- Criminals cold-call investors (victims) offering them worthless, overpriced or even non-existent shares.
- While they promise high returns, those who invest usually end up losing their money.
- Investments Scams target those who have money in their bank to invest.

- Common Investment Scams include buying precious metals, diamonds and gemstones, wine and land.
- Victims of this crime are sometimes given official looking documentation regarding the investment, only to find out that the company is a fake.
- The criminals will often entice the victim into investing more money for shares or sometimes they will simply just disappear.
- Victims who invest in these scams ultimately lose all the money they have invested with very little chance of getting any of it back.

Computer Scams – a telephone call states that there is a problem with the victim's computer or laptop and help is offered to fix the issue.

- The criminal calls a victim (sometimes asking for them by name).
- They state that they are a computer security expert from a well-known or legitimate tech company such as Microsoft.
- The 'security expert' criminal is often plausible and polite, but officious.
- Sometimes the call will sound like it is being made from a busy call centre.
- They explain that the individual's PC or laptop has been infected with a virus or malware, and that they can help to solve the problem.

Ways in which the Computer Scam can be conducted:

- The criminal will gain remote access to the PC or laptop, and then use that access to look through the victim's files, obtaining their personal data.
- The criminal gets the victim to download a tool, which they say is the "fix" for the problem, but is actually a virus or malware.
- A more straightforward way to conduct this scam is to simply ask for money in return for a lifetime of 'protection' from the virus or malware they pretend is on the machine

Doorstep Scams

Criminals use a variety of door step tactics to make victims part with their money or gain entry to their homes.

Doorstep callers (Rogue Traders) – criminals pose as legitimate business people, selling goods or services that are faulty, unnecessary, overpriced, poor quality or non-existent.

- The victim will usually be charged an extortionate rate for the work or goods.
- The criminals sometimes damage the victim's property deliberately in order to get money.
- The victim may be asked to pay for work upfront, either a large cash deposit or the total fee. Once the criminals have received the funds, the work may never be started and the criminal disappears with the money leaving the victim out of pocket.
- The quality of the work can often be poor, can take longer than necessary to complete or never be completed in full.
- The criminal will often not explain to the victim their cancellation rights, give them an adequate cooling off period or provide them with any paperwork for the work or product.
- Victims may also be billed for services that they did not request.
- Criminals can appear friendly, polite and trustworthy however, they use intimidating behaviour in order to get money from the victim.

Bogus callers (Distraction Burglary) – criminals pose as legitimate business people in an attempt to enter the victim's home to commit theft by distracting the victim.

- Criminals pose as legitimate sales/business people in an attempt to enter the victim's home to steal their money, their valuables or take inventory of their possessions.
- Criminals sometimes pose as utilities officials, canvassers or doorstop salespeople.

- Often they work in pairs; whilst one criminal distracts the victim the other enters their home.
- Children are sometimes used in this scam to distract the victim whilst an accomplice carries out the burglary in the property.

Online Scams

Criminals trick internet and email users into giving personal details, including financial information, in order to steal their money.

Phishing – an email from the 'bank' or other payment provider such as PayPal designed to trick victims into revealing their personal information and passwords.

- An email, apparently from the receiver's bank or payment provider, arrives requesting them to update, validate or confirm their details.
- This scam is designed to trick people into revealing personal information and security information such as passwords or PIN numbers so that criminals can access their accounts and steal the victim's money.

Pharming – the fraudulent practice of directing online users to a fake website, which mimics the appearance of a real or legitimate one.

- The fraudulent practice of directing online users to a fake' website, which appears genuine as it will mimic the appearance of a real or legitimate website, in order to obtain personal information such as passwords, account numbers, etc.

Romance Scam – a confidence scam whereby a criminal displays (fake) romantic intentions towards a victim in order to gain their affection and trust to extort money.

- Using online dating websites, a victim enters into an online relationship, which appears to be genuine.
- Criminals will groom the victim through emails, instant messaging, texting and sometimes phone calls.
- Once confident of the victim's trust, criminals will then use emotional manipulation to extort money.
- In some cases, they do this by telling the victim about a problem they are experiencing and ask for financial help.

Impersonation of UK officials – criminals impersonate a UK official to obtain personal information and steal money, often claiming that the victim is due a refund or must make an urgent payment.

- Criminals impersonate a UK official of a government department e.g. HMRC, Ministry of Justice or a crime fighting agency or financial institution e.g. Met Police or a bank to obtain personal information and steal money.
- They may make false promises of a refund (see Council Tax Scam below), tax rebate (see HMRC Tax Rebate Scam below) or state that the victim's bank account has been fraudulently used to launder money.
- They may also make final demands for overdue payments (see Council Tax Scam below).
- The ultimate goal of this scam is to obtain the victim's financial information and gain access to the victim's bank account enabling the criminals to empty the account of all funds.

HMRC Tax Rebate Scam

- *Criminals email victims offering a tax rebate.*
- *The email contains a link to a website and requests to provide personal information, such as bank account information, to claim the non-existent rebate.*

Council Tax Scam

- *Individuals are contacted by criminals claiming to be from the Local Council with details of either a Council Tax refund or demands for outstanding Council Tax payments.*
- *The criminal then obtains bank details in which to pay the fictitious refund into or convince the victim to pay the fictitious outstanding balance directly to the criminal.*