Don’t Get Scammed – Get Savvy

At some time or another you're likely to have heard the following words of supposed wisdom:

- If it looks too good to be true then it probably is.
- There's no such thing as a free lunch.
- You can't win anything if you've not bought a ticket.

They all warn of the risks we are likely to face if we give in to a prevalent human weakness, the one that scammers, fraudsters and con men /women so often rely upon – our desire to get something for nothing. It’s probably the biggest single factor that lead more than 32,000 UK citizens to the theft of their identity and/or savings during the year to March 2015 – a figure which was worryingly 31% higher than that of the previous year!! It goes to show that scams are BIG business for organised criminal syndicates, generating enormous sums of ill-gotten gain which are then used to fund other serious criminal activity in countries across the world.

Scammers use every available form of communication network to ply their evil trade – the internet, telephone and conventional mail systems. The scammer might reside in any land on the planet but his (or her) reach is world-wide. Some scams seem innocuous at first glance, with no obvious means of extracting benefit from their target, but rest assured they don’t do it for fun – it always ends up with someone paying the price. And once caught for the first time a victim’s details are flashed around the globe to others in the scamming game – added to a sinister list of those ‘who are worth pursuing again, and again, and again’. **Simple precautions, such as maintaining up-to-date anti-virus and firewall programs, can help to keep you safe, but they can’t protect you from your own actions, so the best way of avoiding the scammers is to know their game and remain vigilant at all times.** If you are targeted by scammers please report it, both to help prevent others becoming victims and also to give the authorities chance to investigate and chase those responsible. Options and reporting procedures are contained in a list at the end of this document.

There are so many different scams active at any given time that it would be impossible to maintain an up-to-date list of them here on a site such as this, but there are websites that do keep track of the latest developments and issue trusted information to warn the public of current and on-going risks. Probably one of the best of these is ‘Hoax Slayer’ – see http://www.hoax-slayer.com for more detail. Much of the information collated below has been provided courtesy of the Hoax Slayer team. Another good website to visit, and sign up to for advice and warnings, is http://www.actionfraud.police.uk/ the UK’s national fraud and cybercrime reporting centre.

The following is a précised list of common scams, followed by a more detail explanation of the way in which each one works.

Facebook Survey & Like-Farming Scams
Survey scam messages try to trick users into participating in online surveys by promising them expensive prizes. Like-farming scams are designed to trick Facebook users into liking and sharing posts or Facebook Pages as a means of driving traffic to the Pages and increasing their like-numbers under false pretences.

Phishing Scams - Anti-Phishing Information
Phishing scams try to trick users into divulging their personal and financial information to Internet criminals via fake messages and websites.

Advance Fee Scams - 'Nigerian Scams' - 419 Scam Information
Criminals send messages offering victims a percentage of a large sum of money in exchange for their help with a supposed business deal. Victims are then tricked into sending the criminals various upfront fees that are supposedly required to allow the deal to proceed.

Email Lottery Scams - International Lottery Scam Information
Lottery scams are types of advance fee scams that falsely claim that victims have won a large prize in an international lottery but must send various mandatory fees before the prize money can be released.

Payment Transfer Job Scam Emails - Laundering Scams
Scammers send bogus messages offering victims jobs in which they are instructed to bank payments from various third parties, keep a percentage as their 'wage' and wire the remainder back to their 'employers'. The scheme is a method of 'laundering' stolen money.

Overpayment Scams
Overpayment scams are another form of money laundering scam in which criminals send considerably more than the agreed price for an item or service and ask victims to wire the remainder to a 'third party'.

Internet Dating Scams
Criminals pretend to be romantically interested in people they have 'met' online. After they have gained the trust of victims, the scammers will begin asking them for money or try to involve them in money-laundering schemes or other criminal activities.

Phone Scams
These usually phish for personal information in a similar manner to the internet phishing scams but there can be one subtle difference – they rely on a quirk of the phone system to aid them.

Grandparent Scams
Scammers obtain information about family members, perhaps from social media sites such as facebook, and use the information to dupe relatives into thinking that they need to send money to a loved one who is in trouble in some remote part of the world.

Premium Rate Phone Scams
Scammers phone a mobile number at random but only allow it to ring once in the hope that the victim will be curious enough to phone the caller back – but if they do they incur high costs associated with a premium rate phone service.

Goods For Sale Fraud Scams
Fraudsters target ‘goods for sale’ adverts on popular online auctions sites with the intention of duping sellers into sending items to them for which they have no intention of paying.

How Facebook Like-Farming Scams Work

There are many fake Pages on Facebook that are just designed to get people to click the 'like' button. They usually promise expensive prizes, store gift cards, or even cash as incentives for people to click ‘like’. Of course, the promised prizes do not exist, but why do they go to such trouble? What do they get out of it? There are two main reasons why Facebook scammers try to gather ‘likes’ by using these tactics:

- To sell the Facebook Page – there is a thriving market for Facebook pages with high numbers of 'likes', some sell for thousands of pounds. A scam page can often harvest many thousands of 'likes' in just a few days. Once sold then the Page's new owner will use it to reach its built-in audience and push their own products or scam messages.
- To re-use the Facebook Page for further scam campaigns – after a scam Page has accumulated a large number of 'likes', the scammers may then run yet more bogus giveaways. But, this time, as well as 'liking and sharing', the scammers will trick users into clicking a link that takes them to suspect online survey websites. There, via dodgy marketing schemes, they earn money each time one of their victims supply their personal details. So be warned – there could be occasions when you may not ***like*** the outcome of clicking the 'like' button.

How Phishing Scams Work

Phishing scams attempt to trick people into providing sensitive personal information such as credit card or banking details. In order to carry out this trick, the phishing scammers send a fraudulent email disguised as an official request for information from the targeted company. Generally, they also create a "look-a-like" website that is designed to closely resemble the target company's official site. The fake website may appear almost identical to the official site. Style, logos, images, navigation menus and other structural components may look the same as they do on the genuine website. Recipients of the scam email are requested to click on an included hyperlink. Clicking this link will cause the fake website to open in the user's browser. Once at this fake website, the user may be presented with a web form that requests private information such as credit card and banking details, and other account data such as a home address and phone number.

Often, the visitor is requested to login using his or her username and password. All information entered into this fake website, including login details, can subsequently be collected and used at will by the criminals operating the scam. A variation of the scam involves using an embedded form within the bogus email itself. Victims are instructed to enter details such as a password and bank account number into the form provided and return the email to the sender. Another variation attempts to trick recipients into installing a Trojan (an invisible sinister program which secretly sends information from the victim's computer to the scammers), either through opening an email attachment containing the program or inadvertently downloading it with material from a website. The scammers can then use the Trojan to collect data from the infected computer. The scam emails are randomly mass-mailed to many thousands of Internet users in the hope of netting just a small number of victims. The majority of people who receive these scam emails will probably not even be customers of the targeted institution. However, the scammers rely on the statistical probability that at least a few recipients will:

- Have accounts with the targeted institution.
- Will be unaware of such scams and believe the email to be a legitimate request.

The scam can prove to be a lucrative exercise for the scammers even if only a very small percentage of recipients ultimately become victims. The way to avoid becoming a victim of such scams is to never open programs or links from suspicious emails or follow a link to a banking site from an email sent to you – instead always open a new page in your browser and connect to the bank's page as you normally would when visiting their site. If the email contains a hyper-link you can see where it would divert you to if you just hover your mouse (don't click anything) over the link. The destination is then shown at the bottom left-hand side of your screen (or in a separate box in some browser programs). This URL address may contain the name of the financial institution that you expect to see but it will be different to the genuine one – because it will lead to the scammer's site.

How Advance Fee Scams Work

Advance fee scams, also commonly known as "Nigerian" scams, have been around in various forms for decades. In fact, they predate the Internet and email. Nigerian scammers still use surface mail and faxes as well as email and social media. The scams are also called "419 scams" after the appropriate part of the Nigerian criminal code. Although many still originate from Nigeria it is certainly not only Nigerian based criminals that send them. In spite of the longevity of this type of scam and the large amount of publicity that it has received, many people around the world are still being conned out of substantial sums of money by use of it.

There are a great many versions of this scam and they work like this. You receive an unsolicited message that masquerades as some manner of business proposition, request for assistance, notice of a potential inheritance, or opportunity to help a charity. In fact, there is a seemingly endless array of cover stories that the scammers use in order to draw potential victims into the con. In spite of this diversity, virtually all of the scam messages share a common theme. The messages all claim that your help is needed to access a large sum of money, usually many millions of dollars. The scammers use a variety of stories to explain why they need your help to access the funds.

For example: They may claim that political climate or legal issues preclude them from accessing funds in a foreign bank account and request your help to gain such access, or that your last name is the same as that of the deceased person who owned an account and suggest that you act as the Next of Kin of this person in order to gain access to the account's funds. They may claim that a rich businessman, who has a terminal illness, needs your help to distribute his wealth to charity. Or they may claim that a soldier stationed overseas has discovered a cache of hidden cash left by a fleeing dictator and needs your help to get the money out of the country.

The messages offer to let you keep a significant percentage of the funds in exchange for your assistance. This percentage is the bait that the scammers use to entice potential victims deeper into the scam. Once a recipient has taken the bait, and initiated a dialogue with the scammers, he or she will soon receive requests for "fees" that the scammer claims are necessary for processing costs, tax and legal fees, or bribes to local officials. The scammers will warn the victim that these advance fees need to be paid before the funds can be procured. In reality, the supposed funds do not exist. The major purpose of these scam messages is to trick recipients into parting with their money in the form of these advance fees. Fraudulent requests for fees will usually continue until the victim realizes he or she is being conned and stops sending money. In some cases, the scammers gain enough information to access the victim's bank account directly or steal the victim's identity.

How Email Lottery Scams Work

You receive an unsolicited message, which states that you have won a major prize in an international lottery. Supposedly, your email address, name or nickname was collected online and attached to a random number that was subsequently entered in a draw for the lottery. In order to claim your prize, you are instructed to contact the official "agent" in charge of your case. You are also advised to keep the win confidential for "security reasons". This part of the scam is an initial phish for potential victims. If you respond in any way to the email, the scammers will send further messages or even contact you by phone in an attempt to draw you deeper into the scam. You may be asked to provide banking details, a large amount of personal information, and copies of your driver's licence, passport and/or other identity documents. Ostensibly, these requests are to prove your identity and facilitate the transfer of your winnings. However, if you comply with these requests, the scammers may gather enough information to steal your identity. In due time, the scammers will

request some sort of advance fee supposedly to cover administration, legal, insurance, or delivery costs. This type of scam is just a reworking of the classic “Nigerian" advance fee scam, in which scammers also ask for upfront fees to facilitate a supposed business deal of some form. Like other types of advance fee scams, victims who do actually pay the requested fees will probably find that they receive continuing payment demands to cover "unexpected expenses". The requests for money will go on until the victim realizes what is happening or has no further money to send.

Payment Transfer Job Scams - Laundering Scams

Scammers are using unsolicited email and social media "job offers" to trick recipients around the world into falling for payment transfer scams. Victims are promised a percentage of the payments transferred. In fact, the scheme is a method of "laundering" stolen money and victims may be unwittingly participating in illegal activities. These bogus "job offers" are very common. The messages ask recipients to accept cash or cheque payments into their bank accounts and then wire-transfer the payment to the "company" running the scam. In some versions, victims are asked to accept direct electronic transfers into their own bank accounts. Victims are instructed to keep a specified percentage of the transferred funds as payment. Typically, the scammers claim that there is some impediment, such as slow processing or currency conversion problems, which stops them from accepting overseas payments in their country. Therefore, they claim, they need an overseas "agent" who can accept payments and then forward these payments back to them in an acceptable format such as a wire transfer. However, the real purpose of such schemes is to "launder" stolen funds by making it difficult for law enforcement agencies to follow the money trail. Sadly, there are plenty of recipients that are naïve enough to take these offers as genuine and apply for the "job". At face value, it may seem like an easy and legitimate way of making extra money. The criminals may directly target potential victims by responding to "work wanted" ads or resumes posted online. In other cases, they may randomly distribute thousands of "job offer" emails in the hope of netting just a few victims.

How Overpayment Scams Work

People selling items such as cars, motorcycles, boats, computer equipment, or even animals via the Internet should be aware of a money-laundering scam that is cheating victims out of thousands of pounds. Typically, an overpayment scam works like this: A genuine seller places an Internet advertisement for an item with a high price tag. Later, the seller receives a generous offer for the item, usually via email from scammers. The seller agrees on the price, and, often, also agrees to the proviso that he or she refuses any other offers for the item. The scammers then send a cheque / money order for the item or instead transfer the funds directly to the seller's bank account. However, the amount sent will be for substantially more than the specified selling price. The scammers invent some excuse for this overpayment and ask that the balance be electronically transferred to a specified bank account. For example, they may claim that the extra funds are to pay the fees of an agent who is handling the sale or to cover shipping costs. Or, they may claim that an error was made and ask the seller to send back the extra amount via a wire transfer. The seller dutifully transfers the amount as requested. Later, the seller finds that his or her bank has dishonoured the cheque or money order. In some cases, the bank may actually have cleared the funds, but discovers later that the cheque or money order is a forgery or was stolen. Or the funds may have been transferred from a bank account compromised via a phishing scam or malware attack. Thus the seller has been tricked out of a substantial amount, with little chance of recovering the money. Furthermore, the item remains unsold and the seller may have rejected legitimate offers to genuinely purchase it in the meantime.

How Internet Dating Scams Work

There are a great many quite legitimate dating service websites that allow members to establish online friendships. Often, these online friendships blossom into genuine long-term relationships. An increasing number of people have found life-partners via relationships started online. Sadly however, scammers have managed to effectively exploit this trend to further their own nefarious ends. Many people around the world have been duped into sending money to Internet fraudsters posing as would-be girlfriends or boyfriends. A typical Internet dating scam goes like this:

1. A person registers at an online dating service and creates a profile. The profile will include information, and possibly a photograph, of the person along with a way for interested people to make contact.

2. In due course, a scammer contacts the person posing as someone interested in exploring a possible romantic relationship.

3. The victim responds and the pair begins corresponding regularly. They may soon bypass the dating service contact system and start communicating directly, usually via email.

4. Over time, the scammer will slowly earn the trust of the victim. He or she may discuss family, jobs and other details designed to make the correspondent seem like a real person who is genuinely interested in the victim. Photographs may be exchanged. However, the "person" that the victim thinks he or she is corresponding with, is likely to be purely an invention of the scammer. Photographs may not even show the real sender. In reality the scammer may not even be of the same gender as the person in photo that is sent to the victim.

5. After the scammer has established the illusion of a genuine and meaningful relationship, he or she will begin asking the victim for money. For example, the scammer may claim that he or she wants to meet in person and ask the victim to send money for an airfare so that a meeting can take place. Or the scammer may claim that there has been a family medical emergency and request financial assistance. The scammer may use a variety of excuses to entice the victim to send funds.

6. If the victim complies and sends money, he or she will probably receive further such requests. With his or her judgement clouded by a burgeoning love for the scammer's imaginary character, he or she may continue to send money.

7. Finally, the victim will come to realize that he or she has been duped, perhaps after waiting fruitlessly at the airport for a "lover" who, will, of course, never arrive.

8. Meanwhile, the scammer pockets the money and moves on to the next victim. In fact, the scammer may be stringing along several victims simultaneously.

How Phone Scams Work

Phone scams usually phish for personal information in a similar manner to the internet phishing scams but there is one subtle difference – they rely on a quirk of the phone system to aid them. The scam works like this: The victim receives a phone call out of the blue advising them that a suspicious transaction has taken place on their bank account. They may be told that steps have been taken to safeguard their funds in that account but they are either encouraged to move money out of other

accounts into new ones that the scammer offers to set up, or they are told to check any other accounts that they have with other institutions by phoning them. This is the scammer's bait, intended to ensure that the victim feels anxious enough about the security of their savings to do something quickly to 'safeguard' them – without the time to think things through. If the victim agrees to movement of funds into another account the scammers provide details of their own account. As soon as the transaction goes through the victim loses their money. If they try to make contact with their bank the scammers are prepared…. Many BT exchanges allow the phone line to be kept open by the last caller if they don't replace their handset, so when the victim, called by the scammers, hangs up and tries to make another call, to their bank, they end up still connected to the scammer – only this time it is made to sound just like the banking telephone system's call centre, complete with touch pad choice selections and prompts for input of security information etc. Then the call is answered by a different voice pretending to be from the institution that the victim intended to call. In no time, without even realising it, the victim has divulged information that could allow the fraudsters to steal money from their account. The way to avoid this type of scam is to firstly be very wary of phone calls which purport to be from your bank advising of concerns about possible suspicious transactions on your account; and secondly by ensuring that you use a different phone line (or a mobile phone) to call your bank after receiving such a call, or alternatively phone and speak to someone that you know first, to ensure that your phone line has not been 'hijacked' by scammers.

How Grandparent Scams Work

The grandparent receives an unexpected phone call from a person claiming to be a grandson or granddaughter. The 'grandchild' will often claim to be travelling overseas. The scammer - posing as a distraught grandchild - will invent a fictional tale explaining why he or she needs money urgently. For example, they have been in a car accident and may be assaulted or held against his will by the other driver if money to cover damage to the vehicle is not paid immediately. Or, he/she may claim that she will be arrested for drug possession or other offences and thrown in a foreign gaol unless a 'fine' is paid within a few hours. Or, he/she may claim that that they have been mugged and had all his possessions - including passport and wallet - stolen and needs money to pay for medical treatment and get home. They may even claim to have been kidnapped and a ransom must be paid for release.

In many cases, the scammer will use one or more accomplices to make the scenarios seem more plausible. For example, after a brief conversation with the grandparent, the 'grandchild' will pass the phone over to a 'police officer', 'kidnapper', 'angry accident victim', or 'embassy official'. The 'grandchild's portion of the conversation may be deliberately muffled, if the victim suggests that the caller does not sound like his or her grandchild, the scammer may point to a poor phone connection as the reason.

After stressing that the matter is urgent and the required funds must be sent immediately, the accomplice will tell the grandparent how to send the money. Typically, the grandparent will be told to go out and buy one or more prepaid Green Dot debit cards and then call the scammer back. The scammer will ask for the number on the back of the card and then transfer the card's funds to his or her own account. Alternatively, the grandparent may be asked to transfer the money via a money wire system such as Western Union.

In many cases, the scammers may have researched the family of potential victims by accessing social media sites such as Facebook. For example, a grandson's Facebook posts may reveal that he is currently travelling in South America. Other posts may mention grandma and perhaps point to her own Facebook profile. The scammer may then be able to identify grandma's name and location and

find out her phone number via a phone directory. The scammer can then place a call to grandma and come up with a plausible story based on information lifted from the family's social media feeds.

Of course, many grandparents will be far too astute to fall for such scams and will know immediately that the person on the line is not their grandchild. Nevertheless, elderly and vulnerable grandparents do regularly fall for the scam and are panicked into sending their money to criminals. Scammers may also target other family members such as aunts and uncles or cousins.

To avoid becoming a victim, don't be intimidated into acting immediately. Attempt to contact the grandchild directly or talk to other family members to determine if the call is legitimate. Any claim that you must pay money over the phone immediately - regardless of the cover story used - should be treated with the utmost suspicion. If you have elderly relatives that you feel may be vulnerable to such a scam, be sure to discuss the issue with them.

How Premium Rate Phone Scams Work

This scam seems more prevalent in America than the UK – but could affect users here at some future point. The scammers use auto-dialling software to call random cell/mobile phone numbers. The diallers are configured to hang up after just one ring. The scammers hope that recipients will call the number back either out of simple curiosity or because they mistakenly believe that the call was cut off. If users do take the bait and call back, they will be inadvertently calling an international number. And, they may not realise that they are actually calling a "premium" phones service that incurs hefty per minute fees. Thus, the users may rack up a sizable phone bill, first for the international call connection and then for the per-minute premium service. The exact costs incurred may vary depending on the victim's phone provider and the per-minute cost of the premium call. The goal of the scammers is to keep users on the line for as long as possible. The longer the call, the more money the scammers make. The calls originate from outside of the country of the victim but may have area codes that look like they are local. The majority of the scam calls currently originate from Antigua, the Dominican Republic, Jamaica, Grenada, and the British Virgin Islands.

If you receive one of these 'one ring' calls, do not call back. In the UK you might be able to establish the cost of doing so by making a note of the number and entering it into a free 'Number Checker' by going to http://www.phonepayplus.org.uk/Number-Checker/Check-a-Number-Results.aspx to see the name and contact details of the company running the service. This facility is provided by PayphonePlus, the nonprofit making agency which carries out the day-to-day regulation of the premium rate services' market on behalf of Ofcom.

How Do Goods For Sale Fraud Scams Work

Fraudsters often target 'goods for sale' adverts on popular online auctions sites, with the intention of getting hold of the goods without paying for them. This is how the fraud works: The fraudster will contact the seller to say that they want to buy the advertised item. The seller then receives what looks like a genuine PayPal email, to confirm that the money has been paid by the buyer into their account. With confirmation of payment, the seller will then send the item to the buyer's address. The seller will later find that the PayPal email is a fake and that the money has not been paid. The seller ends up losing out twice as not only do they not have the money, but they no longer have the item to sell. To avoid being caught by this scam:

- Check your PayPal account to ensure that the money has been paid in and has cleared into your bank account before you send the item to the buyer.
- Do not be bullied or rushed into sending items before you know that the payment has cleared – a genuine purchaser will not mind waiting a day or two for you to send them their item.
- If you are selling a vehicle, think carefully when selling to overseas purchasers – especially if they tell you they will send an extra payment for shipping – check that the funds have cleared before arranging this.

Reporting Scams

If the 'correct authorities' are not informed of fraudsters' attempts to dupe us then they can't be expected to help protect us – and that's worrying considering that, according to consumer watchdog 'Which', only 39% of us know how to report scams to the correct authorities. So just in case you're one of the 'uninitiated' here's a quick guide.

- **Email scams**

  If you've spotted a scam or phishing email, report it to the company or body being mimicked so that they can warn their customers about it by putting notices on their websites. Also notify the internet service provider (ISP) that was used to send you the email. Yahoo can be told at www.abuse@yahoo.com ; Gmail has a 'Report spam' button; and Hotmail a 'Report phishing' button on their sites.

- **Premium rate phone scams**

  If you want to complain about or report a premium-rate telephone service scam, contact PhonepayPlus, the organisation set up to regulate phone-paid services in the UK, call free on **0800 500 212** from a landline or visit http://www.phonepayplus.org.uk/

- **Reporting scams to trading standards**

  Trading standards may be able to offer advice. And telling them will help stop other people becoming victims. Contact Trading Standards on **03454 04 05 06** or at http://www.kent.gov.uk/business/trading-standards/consumer-advice/report-a-problem-to-KCC-trading-standards

- **Reporting to Action Fraud**

  Action Fraud is the UK's national fraud and crime reporting centre. It provides a central point of contact about fraud and financially motivated internet crime. It offers an online reporting tool at http://www.actionfraud.police.uk/ or you can call and speak to an advisor on **0300 123 2040**. After reporting a scam, you'll get a national crime reference number and the case will be referred to the National Fraud Intelligence Bureau for analysis, by the City of London Police.

- **Reporting a scam to local police**

  You should consider contacting your local police, on the non-emergency **101** number, to report the scam. This may provide them with useful information to assist in catching the fraudsters.

- **Stop scam mail through the post**

The Mailing Preference Service (MPS) allows you to have your name and address removed from mailing lists. To register for the free service, call **0845 703 4599** or visit www.mpsonline.org.uk