Get involved
Get online
Neighbourhood Watch
Newsletter

SCAMBOOK

A COMPILATION OF SCAMS AND FRAUDS TARGETING RESIDENTS AND BUSINESSES

While conventional crime is falling, there is an increasing likelihood of becoming a victim of a scam. The offenders range from single individuals to international organised crime groups. Some are very obvious, including spelling mistakes and grammatical errors; others can be extremely convincing. The proceeds are huge. The victims can be anyone, whether elderly, vulnerable, someone caught off guard or short of money, or someone simply responding to a request for help. Keep one step ahead, and don't be taken in.

For further advice and to report any such scams and frauds, contact Action Fraud at www.actionfraud.police.uk, or on 0300 123 2040. For regular alerts and updates from Neighbourhood Watch about scams and crimes in your area, register your details at www.owl.co.uk, or on 01785 234129.

1. 'CHINESE INVESTMENT' SCAM

You receive a letter, supposedly from someone working for an investment bank in China or Hong Kong, dealing with the estate of a deceased person with the same surname as you. He wants to use your bank account to pay in the funds (usually millions) and will split 50/50. He needs your bank details, and payments in advance.

2. 'LOTTERY WINNER' SCAM

You receive a letter or email, suggesting you have won a large amount in a lottery. It often suggests your address has been chosen at random. There are often references to legitimate organisations, such as the BBC, Microsoft, FIFA, Coca Cola etc in an attempt to add authenticity. If you respond you will be asked for bank account details.

3. 'BANK/CREDIT CARD' SCAM

You receive a phone call, supposedly from a bank or credit card provider. The caller will try to convince you that your card has been stolen or used fraudulently, and will often be very convincing, including quoting some of your personal details. The caller will attempt to get you to either reveal your pin number, or the security number on the reverse of the card, in order for the transaction to be stopped. In some cases your card has actually been stolen (you may not be aware), and the caller is the thief attempting to discover your pin number by posing as your bank security department. Do not give any such information to anyone calling you.

4. 'MICROSOFT COMPUTER' SCAM

You receive a telephone call, claiming to be from 'Microsoft', suggesting there is a problem with your computer. The caller often asks you to switch on your computer, and provide information which will allow them to access it remotely. You will be charged around £150, and damaging software may be installed on your computer. Microsoft will never contact you in this way.

5. 'UKASH VOUCHER' SCAM

You receive a telephone call, suggesting you are owed a refund from an organisation such as a local council or government agency. In some cases the caller suggests someone will call on you with a cheque. In order to claim, you will be asked to purchase a Ukash voucher (often for £100 or more), usually from a local convenience shop, and will then be asked to phone back and quote the number on this voucher. This will then allow the caller to immediately access the value of the voucher.

6. 'UKASH VOUCHER LOAN' SCAM

You receive a telephone call, offering you a loan. Victims have often been applying for a loan, so are likely to believe it is a genuine offer. The caller then asks you to purchase a Ukash voucher, as above, to cover the first instalment.

7. 'COMPUTER LOCKED' SCAM

Your computer shows a screen, usually with police logos on, suggesting your computer has been used to view illegal sites and has been locked. It demands payment of £100 to unlock. Do not pay, this is not true. Contact a computer repair company for advice. For further information on computer security, go to www.getsafeonline.org.uk.

8. 'HOLIDAY ROBBERY EMAIL' SCAM

You receive an email from a friend or member of the family, suggesting they are on holiday abroad and have been robbed. The email asks for transfer of money to help. The sender's email address book will have been hijacked, and the same message sent to all contacts. Protect your email address book by deleting any emails from unknown senders without opening them, do not reply to 'phishing' emails asking you to update details, and install security software.

9. 'LONELY HEARTS' SCAM

This usually targets those looking for friendship or romance via the internet. Messages will be exchanged over a period of time, with the offender creating a plausible history. Eventually, the victim will be asked for financial help, perhaps for treatment of an illness, to pay for study or travel costs. The offender will usually live abroad. The identity will be entirely fictitious, but the victim will be 100% convinced. Payments may start as relatively small 'loans', but once they start will increase. Payments of thousands of pounds are not unusual.

10. 'UNEXPECTED PARCEL DELIVERY' SCAM

You receive an unexpected delivery of a parcel, often a mobile phone, correctly addressed to you and delivered by a legitimate courier company. A short time later someone calls at your door, claiming to be from the courier, and suggesting there has been a mistake and asking for the parcel. This will be the offender, who has used your details and address to order the item. You may then receive the bill.

11. 'STRANDED MOTORIST' SCAM

Motorists are flagged down by another motorist who has apparently broken down, usually in a lay-by or near a roundabout. If you stop, the stranded driver (usually Eastern European) claims to have run out of petrol, doesn't have any money, and offers to sell you 'gold' jewellery for cash. The jewellery is, of course, worthless. We are aware of several people taking pity on these and handing over cash.

12. 'ASKING FOR DIRECTIONS' SCAM

You are approached by (usually) a female in a supermarket car park, after returning to your car with your shopping. She asks for directions, and often shows you a map. While helping and distracted, a second offender removes your bank card from your car. The offenders will have been able to see your pin number being entered at the checkout; cash will be withdrawn from your account before you realise your card has been stolen. It has also been known for the offenders to follow the victim home, and approach them there. Please be aware of anyone paying close attention at checkouts, and wary if asked for directions.

13. 'CRIME PREVENTION BOOKLET' SCAM

Small businesses, farmers, churches and schools receive a telephone call, suggesting they have previously contributed to a publication such as a crime prevention magazine, or police diary, and asking for further payment. No such publications exist. The offenders will often claim you have entered into a contract, and demand payment.

14. 'TARMAC GANG' SCAM

Tarmac gangs targeting owners of car parks, such as church halls, schools, village halls etc, suggesting they are from County Highways (or similar) and offering to resurface the car park with surplus tarmac. Work is very poor standard, overcharged, and of course nothing to do with the council.

15. 'MONEY MULE' SCAM

This targets students and the unemployed. Victims are offered employment, as 'payment processing agents', 'administration assistants' or similar, with salaries of hundreds of pounds a week. It look likes a proper job offer, sometimes with a convincing contract. The real purpose is to channel cash from criminal activity, by paying it into the victim's bank account; they then transfer it into an overseas account for a small percentage. This is classic money laundering. Jobseekers are often contacted after uploading their CV onto the internet.

16. 'SKY DISH INSURANCE' SCAM

You receive a telephone call supposedly from 'Sky', suggesting your insurance cover for a satellite dish is about to expire and asking for payment to renew. In some cases the recipients do not even have a satellite dish. Do not respond to any callers asking for payment.

17. 'UPDATE YOUR DETAILS' SCAM

You receive an email supposedly from a bank, credit-card company or phone/broadband provider, suggesting they have 'updated their security' system, and you need to 'verify your details' in order to continue to have access. The emails often appear genuine, and may include bank logos etc. You may or may not have an account with the bank concerned. Such emails are known as 'phishing', an attempt to steal your details. Do not click on any such links, or provide any information.

18. 'HM REVENUE AND CUSTOMS EMAIL' SCAM

You receive an email supposedly from HMRC, suggesting you are owed a tax refund. You are naturally delighted, and click on the link. Don't. Again, the email looks very convincing.

19. 'FAILED PARCEL DELIVERY' SCAM

You receive an email supposedly from a parcel delivery company, such as Federal Express, suggesting they have a parcel for you and asking you to click on a link. This would appear to be another 'phishing' scam, or alternatively may upload damaging software when you click the link. A similar scam involved receiving a card through the letterbox, asking you to phone a 'premium rate' number to arrange delivery. We understand this particular scam has now been stopped, but be aware, particularly if you are not expecting a delivery.

20. 'COURIER' BANK CARD SCAM

You receive a phone call allegedly from a shop or business, claiming that someone has attempted to use your credit card fraudulently, suggesting you call your bank to cancel the card. The fraudsters then stay on the line, meaning that when you think you are talking to your bank you are actually speaking to one of the scammers. They then helpfully suggest that, under a new scheme, you can cancel all your cards in one go, even for rival banks. They ask you to dial your pin numbers into the phone (this should be the point where you stop – banks NEVER ask for your pin numbers). The fraudster then says your 'cancelled' cards would be collected by courier, giving a code number for security. A short time later, the courier will arrive to collect the cards, which of course are then used. This is a sophisticated variation of other scams.

21. 'JOB OFFER' SCAM

This targets those looking for employment. You may respond to an advertisement, or upload your cv. You are offered a job, which appears legitimate. The prospective 'employer' takes all your personal details. You then start receiving letters saying you have taken out phone contracts, insurance etc. The scammer has used your details. In a variation of this, mobile phones are delivered to you, supposedly as part of the job offer, again using your details. The phone may then be collected by the scammer, posing as a courier, and you will be left to pay the bill. See scam 10 above.

22. 'VACATION' SCAM

You receive a phone call, offering an opportunity to buy a holiday / cottage / apartment / villa etc. A variation suggests you have won the property. The property, of course, doesn't exist. This fits in to the 'if it sounds too good to be true, it is' category. As with other similar cold calls, this is an attempt to get your bank account details, or to convince you into paying for something that appears to be an amazing opportunity.

23. 'BT ACCOUNT' SCAM

You receive a phone call, usually claiming to be from BT, suggesting you owe some money and that your phone line or internet connection will be disconnected unless you pay. The scammer (usually Asian) sometimes demonstrates that they can disconnect your line by asking you to attempt to make a call (you can't, because they are keeping the connection open!). Don't pay.

Updated July 2013

KEEPING YOU INFORMED, AWARE AND ALERT
NEIGHBOURHOOD WATCH + BUSINESS WATCH + FARM WATCH + SHOP WATCH
SCHOOL WATCH + PUB WATCH + FORECOURT WATCH
ACCOMMODATION WATCH + HORSE WATCH + TAXI WATCH

Published by Staffordshire Police