A SHORT GUIDE TO SCAMS

Using:
Computers
Post
Telephones
Deliveries
Door-Callers etc.

A SHORT GUIDE TO SCAMS using Computers, Post, Telephones, Deliveries and Door-Callers etc.
(offered as-is without any warranty)

There are too many scams to list them all and there will be more in the future. Some will be obvious, others will be clever and sophisticated. Hopefully this guide will help spot them.
At the end of this document there is a list of internet links to other guides by the Police, Which and other organisations.
Sadly scams tend catch out people who are vulnerable e.g. lonely, trusting, frail, sick, elderly or a combination of these things. Nevertheless, scams are indiscriminate and we are all seen as potential victims so it pays to be careful.
Saying "NO" does not make you a bad person!

General

- If at any time you believe you have been scammed/defrauded etc. contact Action Fraud: tel: 0300 123 2040 or www.actionfraud.org.uk
- Don't throw out anything containing your name, address or financial details without shredding it first.
- When you register to vote tick the box to opt out of the 'open register' so that companies can't buy your details.
- Be careful when using ATM's (cash machines).
    - If there is a machine inside the bank it is safer than outside.
    - If there is anything that looks like it may not be a normal part of the machine don't use it – tell the bank staff.
    - If your card isn't returned contact the bank immediately – it may be that the machine has been tampered with.
- Register with the Telephone Preference Service to help cut down on cold calls: http://www.tpsonline.org.uk/tps/contact.html
- Register with the Mail Preference Service to help cut down on unsolicited (junk) mail: http://www.mpsonline.org.uk/mpsr/mps_choosetype.html
  (personally I don't mind junk mail – from time to time something interesting arrives e.g. discount vouchers and it's easy to just drop it in the re-cycling bag)
- If you think you or someone you know is getting mail that might be a fraud contact the Royal Mail: scam.mail@royalmail.com tel: 08456 113413.

Computers/Mobile Phones

- If you receive an email from a company you don't deal with or someone you don't know and it has an attachment such as a Word document or a pdf (e.g. a delivery note/invoice/remittance advice) don't open it.
- If you receive emails asking you to confirm your security or account details or saying your account has been closed etc. it is most probably a scam. Unless you are sure it is genuine ignore it and do not use any links such as 'unsubscribe'. If you think it may be genuine contact the company and check.
- Don't unsubscribe or reply to unsolicited/suspicious emails – doing so just confirms you received the email. Delete them.
- Use an anti-virus product – there are lots out there and Barclays Bank offer their customers the full Kaspersky package for PC's Macs and mobiles FREE.
- Use an anti-malware product e.g. Malwarebytes.
- Never use a link on an email to connect to a site even if it is from a company/bank etc. that you do business or have an account with – go to the site direct on your browser.
- Several Banks and other financial institutions offer a FREE product called 'Rapport' by Trusteer (a division of IBM) which provides an additional layer of protection alongside anti-virus and malware software.
- If your bank offers a service to send messages to you when there are deposits and withdrawals – use it. That way you will know very quickly if money is being taken that you didn't authorise.
- Ignore emails with attachments from companies you've never heard of and banks you don't have accounts with.
- If you think of using an old PC/laptop to look at suspect emails/documents etc. do not connect it to your network as some viruses/malware can infect across a network – use a memory stick to transfer the files.
- Backup your PC/laptop/mobile phone regularly.
- If you get an email from someone who claims to have a lot of money they can give you if you will help them get it into the UK etc. it is a scam and anyway would be illegal. Do not be persuaded otherwise.
- The same applies if they say someone with your name died and they have a lot of money in a bank account and with your help they can get it and split it with you – it is a scam and anyway would be illegal.

- Take very great care if you consider using a dating agency or responding to offers of friendship. If you get an email out of the blue from a young and attractive male/female wanting to be your 'friend' or telling how they need help it's undoubtedly a scam and they will no doubt need some money at some point.
- If you get an email from someone (it may even appear to be from a friend) saying they are stuck somewhere and need some money urgently be very suspicious especially if you don't know them and even if you do know them. If they are a good enough friend or relation that they would ask you for money you'd know they were away. Check it out with other friends/relations.
- If you get a text message or any other type of message that offers services such as PPI, loans, insurance claims etc. be very wary of replying to the message or calling any phone numbers they contain.

Delivery scams and people who come to the door

- If an item (usually a fairly high value item) gets delivered to you that you know nothing about and then you get a call from someone who says there's been a mistake and they will call round and collect it – call the supplier direct and check it out. It is probably a scam. It has been ordered in your name and when the scammers collect it they are effectively stealing it from you and you'll be left to pay for it.
- If someone delivers an item you weren't expecting and asks for a delivery charge or similar refuse to accept it. If you are shown a delivery note don't assume because you phone the supplier using the number on the delivery that it's genuine. I've never had a delivery where I had to pay on collection except where I know I have ordered it and it is pay on delivery.
- If someone calls at your door saying there is a problem locally with the water/electricity/gas/telephone etc. and wants to come in to your house be very suspicious especially if there is more than one person. I have never had anyone arrive out of the blue and say they need to come into my house to check something. Always ask for ID and do read the ID carefully. Even if you believe they are genuine never leave the door open while you go and get something they ask for. If it's a meter reader who needs to come in to the premises it is unlikely there will ever be two of them so only ever allow one person in at a time even if they say the other person is being trained etc. Close the door when you go in!
- If you want to check on the callers ID don't call the number on the ID card, tell them to wait, close the door then look the company up on the internet or in the directory and phone them.
- Beware of people looking for charity sponsorship for a fun run or similar. Sometimes they show you a form purporting to show lots of people in your area have pledged £5 or £10 or more. They may even indicate that people have paid already even though the event hasn't taken place.
    - You may choose not to sponsor them if you don't know them.
    - If you do decide to sponsor them:
        - Check with the charity when they've gone.
        - Don't pay until they return with proof they did what they are being sponsored for (think – how would you know?)
- If someone calls on your house and offers to provide a new driveway, trim your trees or other kinds of services;
    - By all means get a quote IF YOU ARE REALLY INTERESTED but then get quotes from other companies. NEVER agree to the work being carried out there and then.
    - Does the caller's paperwork have an address and landline telephone number? If not they may just be passing through the area.
    - Do they have a website?
    - If you can, perhaps discuss it with a friend or family member.
    -

Phone Calls

Get caller ID – it costs a couple of pounds a month and you need a phone that has the facility but it will help you identify who is calling.

If someone phones saying they are from your bank/credit card company etc.

- Be suspicious
- They will ask security questions – try making a mistake with the answer, you'll always get a second go and if they don't question a wrong answer you know it's not the bank.
- Never give full bank account or credit card details – banks will tell you the card number not ask you for it.
- Banks NEVER ASK FOR YOUR PIN NUMBER!
- If they suggest you call the bank to confirm try phoning a friend first – if the caller was a scammer and is still on the line they will answer the phone pretending to be the bank.
  Alternatively use a different phone to call the bank e.g. your mobile.

- If you get a call out of the blue from someone saying they are from Microsoft and are calling because there is a problem on your PC/laptop – hang up. Microsoft never phone out of the blue.
- If you get a call out of the blue from someone saying there is a virus problem on your PC/laptop and they can help you fix it – hang up, it is a scam.
- If you get a call out of the blue from someone who wants to discuss your pension be very suspicious. It's probably some kind of scam. Check with your own advisor or call the pension company for advice.
- If you get a call out of the blue from someone who wants you to invest in shares/property etc. etc. don't agree to anything on the phone. Check it out and take advice.

If you keep getting unsolicited sales calls or calls about PPI and insurance claims:

- Tell them you are on the Telephone Preference List (if you're not you should be see here: http://www.tpsonline.org.uk/tps/contact.html) and tell them never to cold call again.
- If they keep phoning ask them to hold on and then leave the phone unattended for 5 minutes. When you go back they will have hung up and may well mark your number as not worth calling again.
- If you answer the phone and there is nobody there (a so called 'silent call') try dialling 1471 to see if the callers number is there. It probably won't be but if it is:
    - If the number is outside the UK or is an unusual number (starts 090) it is a premium rate number and cost you a lot of money to call it so don't. Try calling Ofcom and see if they can help http://consumers.ofcom.org.uk/phone/tackling-nuisance-calls-and-messages/abandoned-and-silent-calls/
    - If the number is in the UK try calling it because it may offer a way to opt-out.
    - Rather than call the number you can report them to Ofcom.

Never reply to text unsolicited messages offering services or PPI etc. If you are interested in what they offer look the company up on the internet to check them out then phone them if still interested.

- Companies try to get around the law by calling you to carry out a survey which may, in fact, be a sales call in disguise. If you do the survey they will probably ask a whole load of questions like – 'do you have this?' – 'are you interested in this?' etc. If you say 'yes' you are interested (or probably even if you say 'no') you will start getting sales calls from companies offering the product or service.
  After I once did a survey and said 'no' to everything I got dozens of sales calls saying I had expressed an interest in their product. I never do the surveys now – I am polite but I always say 'sorry but NO'.

If You Are Called By Charities

- Be firm. If you already have charities you support, already give and don't want to increase your donation (or can't afford to) say NO. Charities are also businesses these days and saying no does not make you a bad person.
- If you do want to make a donation be careful that:
    - it is actually the charity you think it is.
    - what you think is a one-off donation isn't processed as a monthly donation.

If in doubt and you do want to donate it's probably best to do it direct with the charity by calling them or on-line.

Postal

- If you have a post box at the gate people can access your mail before you by watching for deliveries. Be careful that people don't intercept your mail (e.g. steal new credit cards) or use your address for illegal purposes.
- If you get donation requests from charities – see above.
- If you get a letter from someone who claims to have a lot of money they can give you if you will help them get it into the UK etc. it is a scam. Do not be persuaded otherwise.
- The same applies if they say someone with your name died and they have a lot of money in a bank account and with your help they can get it and split it with you – it is a scam.
- If you get a letter saying you have won something and asking for a fee before you get your winnings or gives a phone number to call (starting 090 or some other non-standard number) be very suspicious as it is almost certainly a scam and you will either lose your money, the prize (if there is one) will be worth less than the fee or the phone call will cost several pounds per minute and there is no prize at the end.
- Invitations to financial seminars and investment seminars etc. can turn out to be high pressure sales seminars – be careful !

Links to websites with information on the latest scams. They often cover the same things but they all have something to add.

Met Police: http://www.met.police.uk/docs/little_book_scam.pdf (this is very good)
Met Police: http://www.met.police.uk/docs/little_book_big_scams_business_edition.pdf
Which Guide to Scams: http://www.which.co.uk/consumer-rights/problem/scams?gclid=COnwo4a2iMkCFRNmGwod0WsLwA#link-1
Which - How to spot an online scam: http://www.which.co.uk/technology/computing/guides/how-to-spot-an-online-scam/
Money Advice Service: https://www.moneyadviceservice.org.uk/en/articles/beginners-guide-to-scams
Citizens Advice: https://www.citizensadvice.org.uk/consumer/scams/scams/common-scams/
Age UK: http://www.ageuk.org.uk/Documents/EN-GB/Information-guides/AgeUKIG05_Avoiding_scams_inf.pdf?dtrk=true
Australian Consumer Commission: https://www.accc.gov.au/system/files/Little%20Black%20Book%20of%20Scams%20-%20Pocket-sized%20guide.pdf