Fraud on the internet

If you use the internet, you're at risk from internet fraud. The internet is a cheap and easy way for fraudsters to con people out of money. This fact sheet tells you about some of the most common types of internet fraud (**scams**). But there are many others. If you suspect an email or something on a website is a con, you're probably right. If something sounds too good to be true, it probably is. Read on to find out how to spot internet fraud and what you can do about it.

Rogue traders

Rogue traders are untrustworthy or dishonest traders who sell goods or services. When selling something online, it's common for a rogue trader:

- to advertise goods that don't exist
- to make untrue statements about the things they are selling
- to sell dangerous goods
- not to tell you about import or transport costs
- to send you different goods to the ones they advertised
- not to deliver on time
- not to deliver at all.

If you do buy something online, it's best to pay by credit card. This is because if there's a problem with the product, the credit card company may be responsible as well as the trader. But before you submit your credit card details to an internet website, make sure it's a **secure site** (look for the padlock icon).

If you have a problem with a rogue trader, report them to the Citizens Advice consumer helpline by calling 0845 404 0506.

Phishing

Phishing is where you get emails pretending to come from a genuine company. They often look like they come from your bank. This is a scam to trick you into giving personal information that can be used for fraud. If you get an email and you're asked to type in a password or type in personal details, this is probably a scam as banks never ask you to do this.

To avoid phishing scams, log into your online accounts regularly – the more often you check your accounts, the quicker you'll spot any problems. If you check your bank and credit card statements regularly, you'll spot fraud more quickly.

You can report a phishing scam to the bank that the email is pretending to come from or you could report it to www.banksafeonline.org.uk. You could

also send these emails back to the Internet Service Provider (ISP) where it came from. Send the complaint to abuse@ISPname, for example, abuse@yahoo.com. The ISP can then close any account that's abusing its systems. If you've lost money becaue of phishing, contact the police.

Identity fraud

Identity fraud is where someone steals your personal details to con you out of money. It can happen when you're not using the internet, for example, if you lose important documents such as your passport or driving licence. But if you aren't careful with your personal details when you go online, you could easily become the victim of identity fraud. For example, a fraudster could get hold of your credit card details and use them to buy things over the internet or withdraw money from your account. Or they could get hold of your address and bank details and use them to borrow money.

To avoid being caught out by identity fraud, be careful about which companies you give your email address to online. Before you buy or sign up to anything online, check out the **privacy policy** of the company and make sure they won't send your details to other companies if you don't want them to. Also, be careful about the passwords you choose. Don't use whole words because these are easier for a fraudster to find out. It's safer to use a combination of letters and numbers.

If you think you've become the victim of identity fraud, report it to the police. You could also register with the fraud prevention service scheme. The way this works is that if you know someone has stolen your personal details, a warning will be posted on your credit reference record so that a lender will check with you before granting more credit. The website for this scheme is www.cifas.org.uk (follow the link to Protective Registration). For more about identity fraud, go to the Home Office website (www.identitytheft.org.uk).

Spam

Spam is unasked-for emails sent to a large number of email addresses. Many advertise illegal products, scams and pornography. It's against the law to send you marketing material by email unless you've given your permission. The Office of the Information Commissioner monitors these rules. You can contact them at www.informationcommissioner.gov.uk. But in practice, if emails are sent from overseas, it's difficult to enforce the law.

Never open spam, especially if it has an attachment. Attachments can contain a virus that will damage your computer. Delete an email if you aren't sure where it comes from. Don't reply to a link in a spam email that says they'll remove you from their mailing list. This can just lead to more spam.

Never respond to spam emails that ask you to confirm your user name, passwords or bank details. Never use links within an email to get to a

company's site. It's always safer to type in the internet address of the site you want to visit in the address bar at the top of the webpage.

There are also many software packages that can help filter out spam. Some can be downloaded for free. The BBC's website has useful information about security on the internet. You could also visit www.banksafeonline.org.uk, which has a list of commercial software producers.

Lottery scams

Lottery scams are very common on the internet. Even though you may never have entered a lottery, you get an email to say you've won a prize. But then you're told have to send money to claim the prize. Or you're asked to ring a premium rate number that is very expensive. All UK premium rate numbers start with 090. Or you're asked for your bank details so the prize money can be paid in. Don't reply to these emails. Report them to the police if you lose money.

Pyramid schemes

Pyramid schemes (sometimes called affinity schemes) promise you money in return for the number of people you recruit to join the scheme. You'll get an email telling you how much money you'll make. But these claims are misleading. Pyramid schemes are illegal. Report them to the police if you lose money.

Transferring money

This is a scam where you're offered a commission if you accept money into your bank account. You're then asked to withdraw the money in cash and transfer it overseas, for example, as a charitable donation. If you transfer money like this, it's a serious criminal offence and you could go to prison and be fined. Genuine charities never ask you to transfer money in this way. To check on whether a charity in England or Wales is genuine, visit the Charity Commission's website www.charity-commission.gov.uk/registeredcharities. To check on charities in Scotland, see the website of the Office of the Scottish Charity Regulator at www.oscr.org.uk.

Chain emails

A chain email is an email that you are asked to send on to your contacts**.** Some chain emails threaten you with bad luck if you don't pass them on. Others promise a small contribution to charity if you do pass them on. These are both scams. Don't pass on a chain email. Delete it before opening.

Further help

- www.getsafeonline.org.uk is a joint government and private sector website that helps you protect your computer and use the internet safely
- The Office of Fair Trading's website has information about current scams and what to do about them at: www.oft.gov.uk/Consumer/Scams
- Action Fraud is the UK's national fraud reporting centre. Go to www.actionfraud.org.uk 0300 123 2040
- APACS is a trade association of financial organisations. It has a useful website with information about how to protect your computer and current financial scams at: www.banksafeonline.org.uk
- The BBC's website has information about privacy and security when using the internet www.bbc.co.uk/webwise
- Search for details of your local police force in England and Wales at: http://local.direct.gov.uk and in Scotland at: www.scottish.police.uk
- The Advertising Standards Authority (ASA) monitors advertising. A company that is using spam to advertise its material may already have a complaint lodged against it. Check this out on the ASA's website at: www.asa.org.uk
- There are a large number of other websites that list common scams, for example, www.millersmiles.co.uk, www.ripofftipoff.net and www.scambusters.org.

Citizens Advice Bureaux
Citizens Advice Bureaux give free, confidential, impartial and independent advice to help you solve problems. To find your nearest CAB, including those that give advice by e-mail, click on nearest CAB, or look under C in your phone book.

Other fact sheets on Adviceguide which might help

- Offensive websites
- Buying over the internet
- The internet – using other people's material

This fact sheet is produced by Citizens Advice, an operating name of The National Association of Citizens Advice Bureaux. It is intended to provide general information only and should not be taken as a full statement of the law. The information applies to England, Wales and Scotland.

This fact sheet was last updated on 5 August 2012, and is reviewed regularly. If it is some time since you obtained this fact sheet, please contact your local Citizens Advice Bureau to check if it is still correct. Or visit our website - www.adviceguide.org.uk - where you can download an up-to-date copy.