An article from Computer Friendly, the local charity offering advice and courses to help you keep pace with the technology of today. www.computerfriendlystalbans.org.uk

Telephone and Internet Scams

Fraudsters have been conning people out of their money and possessions for centuries, but these days technological advances have given them even more ways to deceive and cheat you, and relieve you of your money. In the past the fraudster, or their agent, had to deal with you face to face, but today by using the phone or internet they can do so without your knowing anything about who they, are or their whereabouts – most likely they are not even in the UK.

This short article is to give you a few hints and tips on how not to fall prey to these criminals, and covers both telephone and internet fraud. Please talk to Computer Friendly if you need further help.

Unfortunately, the best piece of advice is, "**Don't trust anybody!**" Do not give your bank account or credit card details to anybody who does not have the right to have them! You wouldn't give them to someone who came to your door, so why give them over the phone, or on the internet?

No bank or credit card company will call you and ask you for your account details.

The Police will not call you to say your account has been compromised and ask you for your account details.

Neither Microsoft, Apple, nor any other reputable company, will phone you to tell you that you have a problem on your computer that they can fix for you.

How to recognise a scam

A scam is usually uninvited (unsolicited) from a company or person you've never heard of.

A scam will:

- give extravagant promises - if it sounds too good to be true, it almost certainly is!!
- ask you to pay for something upfront, eg you have to pay a fee to claim a prize.
- put pressure on you to make a quick decision, eg unless you pay immediately an investment opportunity will end.
- ask for bank account details so they can steal your money.

Telephone scams

To read about Top 10 phone scams and how to avoid them go to:
www.moneymagpie.com/article/top-10-phone-scams-and-how-to-avoid-them

Two of these scams are to do with computers, but the rest cover such things as:

Sky Protect scam - callers tell you that you should get cover for your Sky service and ask you to verify your bank details – they may even know your Sky account number which may make this seem more legitimate.

BT disconnecting phone scam - scammers posing as BT staff trick customers into revealing their bank details by claiming that they have an overdue bill that needs paying immediately or else their phone service will be disconnected. The scammers may tell the customer to put down the phone and try to call someone, but they cannot use their phone as the fraudsters have not put down the phone: that cons people into thinking that they have been disconnected.

Telephone lottery scams - trick customers into thinking they've been entered into a prize draw and they've won a prize, but in order to claim it they must first send money to pay for admin fees etc. The prize does not exit, but the scammer claims your money and your personal details.

Mobile phone insurance - hoax calls offering you a very attractive mobile phone insurance deal, you give your bank details but discover your phone is not insured at all**.**

The fraudster may suggest that you contact your bank to confirm details, or you may want to do so if you are suspicious. Make sure you use another phone, or if you have to use the same phone wait 5 minutes or so before doing so, or phone a friend (whose voice you recognise) before making a call to your bank, as the fraudster can stay online and eavesdrop to get your bank details, which is what he wanted anyway.

There are some very good call blocker devices on the market, but don't buy one from a cold call!

Internet scams

There are about 24 online scams. To read about The Top 10 Internet/Email Scams go to http://netforbeginners.about.com/od/scamsandidentitytheft/ss/top10inetscams.htm.
Press the right hand arrow to read all the stories (don't click on any adverts).

Phishing – the most widespread email scam

- Phishing (pronounced 'fishing') – uses an email that looks as if it comes from a bank or credit card company asking you to submit details of your account
- Phishing attempts are becoming increasingly clever and realistic
- Report the phishing attempt to your bank or credit card company.

Stay safe online

In addition to being very suspicious of anyone who contacts you, as above, you need to ensure that your computer is secure from malicious software (malware) which could be used to take over your computer to steal account details, copy your password as you type it (key logging), or be used to automatically send spam/scam emails to other people.

- Make sure you have a secure password for every online service.
- Have a different password for each account.
- Ensure you have good up-to-date anti-virus (AV) software.
- Ensure you have a good up-to-date firewall – install one if you are still using XP.
- Ensure your browser is up to date – do not use Internet Explorer if you are still using XP.
- Only go to websites you can trust: install Web of Trust www.mywot.com on your web browser. This uses a traffic light scheme to indicate a site's safety rating.
- Do **NOT** click on any link in a message from anyone you don't know.
- Do **NOT** open any file/attachment to an email or from a website (even if it is from someone you know or a reputable source) without checking it first. Carry out the following steps:
  a. Save the file to a convenient place on your computer: desktop or a folder, eg download.
  b. Right click on the file.
  c. When the menu opens select your AV or Malwarebytes, www.malwarebytes.org/free.
  d. Wait till you are told that there are no threats, then open/run the file.

What to do if you have been a victim of fraud

Report it to your bank or card provider immediately: phone them or look on their website.
Report the details to Action Fraud, the UK's national fraud reporting centre: call 0300 123 2040 or visit www.actionfraud.police.uk.
Contact Trading Standards via Citizens Advice Consumer Helpline on 03454 040506, as in certain cases they may visit people that have been scammed.
If the fraud occurred online, **change** your account password (s) immediately, and do a thorough scan by running Malwarebytes.

Help and advice you can trust

Online Watch Link, OWL, www.owl.co.uk, the online Neighbourhood Watch, keeps communities safe, helps reduce crime and keeps people informed of what's going on locally. It's a shared, secure platform for the public and local authorities to maximise the potential of Neighbourhood Watch, and many other schemes. OWL sends you the latest local crime alerts.
Get Safe Online, www.getsafeonline.org, is the UK's leading source of unbiased, easy to understand information on online safety. The website provides practical advice on protecting yourself, your computers and mobile devices, and your business against fraud, identity theft, viruses and many other online problems.