TELEPHONE SCAMS

Card Fraud Telephone Scam

The UK Cards Association is advising customers to be aware of a new variation on an old style scam that involves people being telephoned by fraudsters and duped into handing over their debit or credit card, and revealing their PIN.

How does the scam happen?

A fraudster rings you, claiming to be from your bank, saying their systems have spotted a fraudulent payment on your card or that your card is due to expire and needs replacing. You may be asked to ring back using the phone number on the back of your card - which further convinces you the call is genuine. However, the criminal keeps the line open at their end so, when you make the call, you are unknowingly connected straight back to the fraudster. Then, by seeming to offer assistance, the fraudster tries to gain your trust. In most cases you are asked to 'cancel' your existing card or 'activate' or 'authorise' a replacement card by keying your PIN into your phone's handset.The fraudster then poses as a bank representative to pick up your card from your home, sometimes giving you a replacement card, which is a fake.

In some cases a genuine courier company is hired to pick up the card, which the victim has been asked to place into an envelope.Once they have your card and PIN the fraudster uses them to spend your money. A variation of the scam involves the fraudster ringing a prospective victim and claiming to be from the police – again with the aim of going to the victim's home to collect the card and PIN.

What can I do to avoid this scam?

Remember this advice: Your bank or the police will NEVER ring you and tell you that they are coming to your home to pick up your card, so never hand it over to anyone who comes to collect it. Your bank will NEVER ask you to authorise anything by entering your PIN into the telephone. NEVER share your PIN with anyone – the only times you should use your PIN is at a cash machine or when you use a shop's chip and PIN machine.

What should I do if I think I may have been the victim of a fraud or scam?

If you think you have been the victim of a fraud or scam of this nature you should call your bank or card company immediately.Visit www.financialfraudaction.org.uk for more information.

Energy Saving Scam

Trading Standards Institute (TSI) warns of dangerous energy saving scam targeting elderly TSI is urging consumers to be aware of rogue telephone cold callers offering energy saving devices after trading standards up and down the country reported hundreds of complaints. TSI are currently dealing with more than 200 complaints about people claiming to be their energy supplier or working in partnership with them, offering a plug in device which they say can save them 40 per cent off their energy bills. Trading standards have had a number of the items tested which not only failed to satisfy electrical safety standards but do not deliver any tangible energy savings. Ron Gainsford from the Trading Standards Institute said: "Consumers are warned not to use the products as they pose a risk of fire and electrocution and a safety recall has been issued for the items traced so far.

"Unscrupulous criminals are using the rising energy prices as an opportunity to lure in cash strapped consumers - elderly people seem to have been deliberately targeted. "The number of complaints we are currently dealing with is bound to be only the tip of the iceberg." Westminster trading standards have been investigating the scam as the caller gives a London W1 Oxford Street address for the company. Sue Jones from Westminster trading standards said: "The address they give is that of a virtual office provider, the companies involved in these scams are not actually situated there - we believe the call centre they use is based abroad and the appliances appear to be distributed by a number of individuals in the UK. "We know that these fraudsters have been duping consumers across the country into paying £99 for the energy saving device and have been told the caller always appears to be very credible by already knowing the consumers' details, their energy supplier and sometimes some or all of the digits of their credit / debit card. "Often consumers do not realise that they have been defrauded until they receive the dodgy looking device with instructions in broken English and the accompanying

invoice which names an unknown supplier and often gives an American address."

So far four different suppliers have been named, 1 Stop Marketing Solutions, ITC Development Corp, Power Saver and Athico Ltd. but the fraudsters could be operating under other names too. Some of these names could be very similar to genuine companies - for example Power Saver Ltd, based in Tonbridge, Kent is not involved in this fraud. The director of Athico Ltd appears to have been a victim of the scam himself. He fully cooperated with trading standards and the company has now ceased trading.

Advice to consumers If consumers have responded to one of these cold calls they should report the matter to Action Fraud on www.actionfraud.org.uk - 0300 123 2040 - or Consumer Direct on 08454040506 . They should also contact their bank to stop their debit / credit card. If a device has been received they should not use it and dispose of it carefully. Consumers should be cautious about giving out any personal or financial information. They should independently verify a caller's identity before agreeing to purchase any goods or services.

Microsoft Windows Support Scam

WHICH? The which magazine warns that many people are falling for this scam. They report that victims are losing on average £529 from this scam and by installing malware on your computer they can do even more substantial damage.

Which? are not on their own.

The http://money-watch.co.uk/8183/windows-support-scam-worsens web site tells us there is no end in sight for the Windows Support telephone scam previously reported. As a reminder, households are receiving calls out of the blue from a so-called "Microsoft or Windows Support Centre", often sounding like an Indian call centre, who ask if your PC is running slowly, as they have detected a virus on it and would like to help you sort it out. For a fee of course. There have been numerous reports from people receiving these calls, being taken in, and handing over cash. Costly and annoying certainly, but now it looks like there might be another similar tactic where the callers are

actually installing software, whether it is genuine anti-virus software such as Kaspersky, or something more sinister like spyware which could potentially open you up to wider ID and bank fraud. The Guardian says that this "takes the scam into new territory altogether, because it means that the scammers are now changing the setup of the computer, and while it's still fraud, it also now strays into fields such as the Computer Misuse Act".

If you have been taken in by this scam:

- contact your card issuer and get the transaction reversed; if you think your card has been compromised ask them to cancel the card and issue you with a new one.
- report what happened to Action Fraud, the UK's national fraud reporting centre. It has its own page on Microsoft-related scams, as does Microsoft itself.
- contact the police so you can get a crime number.
-

If you are targeted by such calls, it's best to put the phone down straight away. Or you could string them along and help to increase their phone bill although this is not advised.

BT Threat to disconnect you

Similarly telephone scams continue to take different forms. We have received the following on that topic:
A phoney 'representative' of BT calls announcing they will disconnect you because of an unpaid bill. He demands immediate payment or it will cost you more to reconnect later. If you are with another provider he tells you they have to pay BT a percentage for line rental!
He is very plausible giving his name and a "BT Business" number to ring. If you don't believe his story he offers to demonstrate that he is from BT by disconnecting your phone. He tells you to hang up and try phoning someone. The phone will be dead - no engaged tone, nothing - until he phones again. He asks if that is enough proof that he is with BT. He asks for payment by credit card, there & then. Refuse.

Phone the police to let them know. They advise letting as many people as possible know.
The "disconnection" would probably convince some people it's real but is easy to fake; he stays on the line with the mute button on and

you can't dial out but he can hear you trying. (This is because the person who initiates a call is the one who must terminate it). When you stop trying he hangs up and immediately calls back. You could almost be convinced!