Bexley Borough Neighbourhood Watch Association

NEWSLETTER Scam Alert Special-Edition Sept 2012

Patron- James Brokenshire (MP-for Old Bexley & Sidcup) Chairman/Newsletter Editor/Communications-Dana Wiffen
Vice Chair –Jo Tanner, Treasurer-Sophie Kingston, Secretary-Claire Tack

Telephone Office 0208 284 5537 or Email us: bexwatch-office@btconnect.com WEBSITE www.**bexleywatch**.org.uk

SCAMS GALORE

If you have received scam email you can report it to Action Fraud', the government's anti-fraud agency, through its reporting tool online or over the telephone.

Visit:-www.actionfraud.police.uk/scam-emails or call **0300 123 2040**

The reports will be forwarded to the National Fraud Intelligence Bureau run by the City of London Police for 'collation and analysis'. Action Fraud states that this will 'enable crucial intelligence to be gathered and preventative action taken'.

Courier Scams

Operation Sterling from the Metropolitan Police Service's Specialist and Economic Crime Directorate is reissuing its warning regarding "Courier Scams" - a fraud that is mainly targeting the elderly and vulnerable in our communities. These scams are becoming increasingly prevalent across London and beyond.

Method;

1) Elderly members of the public have been receiving unsolicited telephone calls from fraudsters purporting to be from the police or their bank.

2) A fraudster will ring a member of the public, claiming to be from their bank (or in some cases claiming to be the police), stating that their systems have spotted a fraudulent payment on their card or that their card is due to expire and needs to be replaced.

3) The person may be asked to ring the bank back using the phone number printed on the back of their bank card. This helps to convince the person that the call is genuine.

4) However, the fraudster has kept the telephone line open so even though the person has called the bank, the call does not go through. Instead they are unknowingly connected straight back to the fraudster.

5) The fraudster then gains the person's trust by pretending to be from the bank and seeming to offer assistance. In many cases the person is asked to provide their full bank card details and key in their PIN so that their existing card can be "cancelled" and their new one "activated" or "authorised." The fraudster will then explain that the bank will need to collect the card.

6) The fraudster will then attend the person's address or send an innocent courier company driver to collect the card and sometimes provide them with a "replacement" card which is subsequently found to be fake.

7) Therefore, the fraudster has obtained the person's name, address, full bank details, the card itself and the PIN. The bank cards are then used fraudulently without the victim's knowledge.

Prevention Advice

If you receive such a call end it immediately. Please be aware of the following:-**Your bank will never attend your home. Your bank and the police will never collect your bank card. Your bank and the police will never ask for your PIN,**

I would underline these points of use.

Reporting Advice

In an emergency dial 999.

In a non-emergency, report to Action Fraud on 0300 123 2040 or online at **www.actionfraud.police.uk** or contact your local police by dialling 101 and report the matter to your bank.

MICROSOFT-SCAM

Britons are being targeted by cold callers pretending to be from Microsoft phoning to fix a fake computer problem.

The scam always starts the same way: the phone rings at someone's home, and the caller usually with an asian accent asks for the householder, quoting their name and address before saying "I\'m calling for Microsoft. We've had a report from your internet service provider of serious virus problems from your computer." Dire forecasts are made that if the problem is not solved, the computer will become unusable.

The puzzled owner is then directed to their computer, and asked to open a program called "Windows Event Viewer". Its contents are, to the average user, worrying: they look like a long list of errors, some labelled "critical". "Yes, that's it," says the caller. "Now let me guide you through the steps to fixing it."

The computer owner is directed to a website and told to download a program that hands over remote control of the computer, and the caller "installs" various "fixes" for the problem. They then are told that they owe £185 for a "subscription" to

the "preventative service".

There was never anything wrong with the computer, the caller is not working for Microsoft or the internet service provider, and the owner has given a complete stranger access to every piece of data on their machine. Though people on dozens of web forums have recorded their experiences with the scammers, police and trading standards officers in the UK are powerless to stop them.

UK telephone numbers for contacting the company on the sites are not "geographical" tied to a location but instead allocated to voice-over-internet providers. That means that the calls connect internationally, but cost the scammers almost nothing when anyone calls them. In the same way, it costs them virtually nothing to make the calls because the international part of the call goes via the internet.

If the payment has been made on a debit card as many are there is no hope of reversing the payment. A number of payment organisations used by the scammers have shut down their accounts. PayPal, the eBay-owned credit transfer company, and Alert Pay have both taken rapid action against scam sites which used them.

POSTAL-SCAM

The NHW office has received several calls regarding a letter which originates from Hong Kong claiming that a name-sake of yours has left you a huge fortune. The writer asks you to contact them and not to inform the authorities as they won't be able to get the money out of China if discovered. Remember 'if it sounds too good to be true – it is'. If you receive such a letter please contact Royal Mail Security, Security Help Desk, Floor 2a, Battersea D.O, 202 Lavender Hill, London, SW.11 1AA or ring 020 7 239 6655.

PPI CLAIM-SCAM

A call to a woman who was claiming PPI payments back through a UK claims company has scammed her out of £500.

When she got the call she thought she was talking to the company she registered with some months earlier. The caller told her she was to get a large amount back but they needed some money to cover their costs. She was persuaded to buy £500 worth of cash vouchers then call an 0203 number. She did so, gave the voucher numbers and lost her money.

If you are unable to claim PPI monies back, for FREE, by yourself or with the help of family or friends make sure you only agree to payment after the company you use has been successful. Never pay cash. Never pay by cash voucher. The Internet has FREE advice on how you can make your own claim at NO COST to yourself.

CREDIT CARD RADIO FREQUENCY DEVICE-

We have already discovered that some of our cards have this radio frequency device enabling **contactless payment**. We believe that the card payment limit is restricted to £20.00, with the banks prepared to swallow that amount should it be used fraudulently

This system of payment is more widely used in the USA & Canada. Some of our debit cards and credit card have the symbol and "pay pass" on them, meaning. This type of fraud could happen over here, so best be aware!!

Visit below to see explanantion;-

http://www.youtube.com/v/lLAFhTjsQHw%26sns=em