



IMPORTANT INFORMATION for 13th March 2008

EMAIL NEWS

A phishing email this week from Nat West Bank referring to 'Online Form Released' which requires you to complete a Nat West Online Form to keep your banking details up to date. The link goes to a website in Carlsbad, California and has an advertisement for an 'Internet Marketing System' if you give your personal details. Also a Halifax Legal Solutions email claiming that a new system called i38-BankSecure will establish a secure link to your bank. It also claims 'sequel to our new security measures, our records indicate that your account was withered and has upshot an internal error in our processor'! The link led to a site owned by Fiet Assistance in the Russian Federation.

A N/W member has forwarded a scam lottery email supposedly from the UK National Lottery informing you that you have won £850,000 and you should contact their claims officer giving a number of personal details, which could be used for ID fraud or be sold onto a spammers email list. The contact email address is for a website in Scottsdale, Arizona USA. As always if you did not buy a ticket you cannot win. This email uses a slight variation on the correct National Lottery UK website address and has a very confused postal address quoted.

BOGUS CALLERS

A bogus caller in SOUTH CROYDON this week when a white male approx age 42 years 5'04" tall walked into a flat where the door was open and claimed to be a neighbour, he asked the victim for a glass of water to he could take some medication. While victim was distracted he entered the bedroom and stole the victim's handbag and contents. No other description other than that he had short black hair. In WADDON a smartly dressed Asian male called holding a clipboard and said he had come to survey the house. The victim asked for ID but he did not show it clearly so entry was refused.

In nearby SUTTON there have been bogus callers targeting homes using the methods of asking for a pen and paper or to use the toilet, at each offence there were two suspects and while victim was distracted items were taken.

POLICE APPEAL FOR WITNESSES

We are appealing for any witnesses or information concerning an incident on the Shrublands Estate in Croydon in the early hours of Thursday 6 March.

Police believe the incident, in which three people were stabbed, began in the street in Larch Tree Way around 0300. Police were made aware by LAS of a man with stab wounds in Gorse Road, Shirley at 0321. On arrival they found a man; (Victim1) aged 29 yrs suffering stab wounds. He was taken to a hospital in Kent where his condition is described as serious but stable.

At 0323 officers were again notified by LAS of a man with stab wounds in Lilac Gardens, Shirley. At the location they discovered a man, (Victim2), suffering from injuries to his hands. He was taken to a south London hospital and later released.

We were notified by a south London hospital at approx 0330 of a man suffering stab wounds. It is believed the man; (Victim3) aged 19 yrs was stabbed on the Shrublands Estate in Shirley. He was taken to a local hospital and later transferred to a west London hospital for surgery. His condition is described as stable.

The incident is being investigated by Croydon CID. DCI Jon Wilson said: "We believe the incident began in Larch Tree Way with a disturbance. I want to hear from anyone who was in that street or any of the surrounding streets who may have heard or seen anything of the disturbance."

The number to ring with any information is 020 8649 1212 and ask for the CID or phone Crimestoppers on 0800 555 111 to remain anonymous. Police arrested three men in connection with the incident - no further details at this stage.

INFORMATION FROM BROAD GREEN SAFER NEIGHBOURHOOD TEAM

POLICE SURGERY FOR LADIES

Hindi/Urdu/Singhalese spoken

FIRST MEETING ON FRIDAY THE 4TH OF APRIL 2008

TIME: 10.30 am – 11.30 am

AT THE BROAD GREEN LIBRARY
CANTERBURY ROAD CROYDON

Regular meetings will be held throughout the year. Dates will be published at the Library and local shops.

IF IT SMELLS A BIT "PHISHY", IT MIGHT BE!

That email you received from your bank asking you to click on their link ASAP to update your personal details or risk your account being closed. Was it a genuine request or a phishing trick?

The costs to individuals and companies worldwide that have been conned by phishing scams are extremely high and run into the millions. Ensure you aren't one of them by using a firewall and an antivirus programme together with a programme such as Spybot S&D which can be downloaded free of charge to give comprehensive protection against phishing scams available.

Not sure of your fish from your phish? Phishing is where hackers send an email out to a mass audience in the hope that a number of recipients will respond. The email appears to be from a legitimate source such as a bank or credit card company and generally requests you to update your personal details such as account numbers and passwords or risk having your account closed. The recipient will be encouraged to click on a link that supposedly will direct them to the bank's website to update these details. What really happens is they are sent to a deviant website that for all intensive purposes looks and feels like the bank purportedly being represented.

An early example of this was when people received emails allegedly from eBay requesting them to update their credit card details by clicking on a link or risk having their account suspended. The link directed them to a site that appeared to be eBay in terms of appearance, layout and logos. Instead the site stole their information. Once they have this information they are able to create accounts in the user's name and rack up large debt on their behalf.

The term "phishing" is a spin off from "fishing" whereby the hacker throws the bait (i.e. the email) out into the water in the hope of catching some fish. Those people that respond to the email are the unwitting "fish". Hackers are now refining their techniques and conducting targeted campaigns commonly referred to as "spear phishing". Instead of sending an email to a mass audience, rather an individual or department in an organization is targeted. The target user receives what appears to be an internal email from within their company requesting information such as logins and passwords. Once they have responded with the information, the hacker is now able to access the company's network.

A recent example reported was where an employee from Salesforce.com fell for a "phishing" email and was duped into releasing their customer database. Their almost one million customers became targets of virus and malware attacks with personalized emails being sent to them that appeared to come from Salesforce.com. Forums and chat rooms provide an abundance of information that hackers utilize to target individuals such as the thousands of MySpace users who recently fell victim to a bogus Macy gift card giveaway.

Be alert to emails from companies requesting that your personal details be updated, ensure the email is legitimate as it is easy for hackers to change the "from" address. The safest option is to take note of the URL attached to the clickable link and delete your email from both the inbox and trash folder. By then opening your browser and typing in the URL you are able to view the site attached to the link, ensuring you know exactly what website you are actually visiting.

SERIES OF HANDBAG THEFTS

In the PURLEY/SOUTH CROYDON area there has been a series of handbag thefts where the unseen suspect has entered properties through unlocked rear doors or open windows so please be aware. Keep rear doors locked and remove the key.