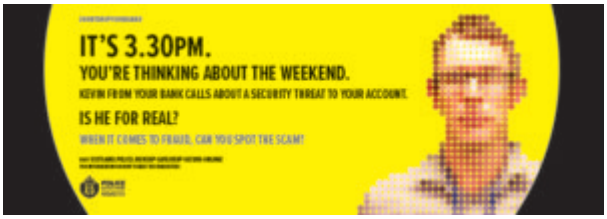
# Over £7 million scammed from businesses and individuals




Police Scotland are warning the public to be alert after businesses and individuals across the country were scammed out of millions of pounds.

Officers are investigating 19 significant crimes of vishing fraud since July last year, with just over £7 million stolen from both businesses and individuals collectively.

Frauds of this nature are generally orchestrated by organised criminal gangs operating in the UK, Europe and further afield.

The variety of techniques used suggests involvement of multiple individuals or groups and can be broken down into three categories: phishing, vishing and smishing.

Phishing type incidents often use emails from the well-known online purchasing sites, either informing a victim that there is an issue with the items they have just ordered (items that they have not ordered at all) and asking them to click the link in the email to verify payment or account details.

Vishing crimes involve contacting a victim by telephone or voice messages pretending to be from the victim's bank or a reputable company and thereafter persuading the victim into revealing personal information, such as bank details, credit card numbers and other personal security information. Once this information is obtained the criminals can access the victim's account and move money or through social engineering persuade the victim to make the transfer on their behalf.

Smishing frauds are conducted in the form of text messages, which aim to obtain personal info related to credit card and banking details. Complainers receive a text message from an unknown number with wording along the lines of: “we have noticed that there seems to be fraudulent activity on your credit card/bank account, please clink the link within the text message to confirm your banking details.” The complainer then clicks the link and follows the instructions set up on the fake webpage, allowing the offender to view the complainer’s personal information and use it to their advantage.

The three types are all aimed at getting the victim to provide personal information that will assist the criminal.

Police Scotland is reminding everyone that their bank will not contact them asking for personal information or to carry out a transaction.

Detective Chief Inspector Jim Robertson, from the Economic Crime and Financial Investigation Unit, said, “Cyber enabled crime is still crime. People make sure that their house and cars are locked and secure, and the same policy should be adopted online. Simple things like making sure you use strong passwords for personal and business accounts and being wary when accessing public or open Wi-Fi can help keep people safe.”

Police have reported a rise in reported incidents such as impersonation and deception scams where bank details are compromised to enable criminals to commit fraud.

DCI Robertson added, “Banks will not contact businesses or individuals asking for personal information or ask you to carry out a transaction. If someone starts asking for these details end the call and contact your bank.

“If you decide to ring back and verify the call it is advisable to do so on a different phone line like another

landline or your mobile. If you are still unsure, consider visiting your local branch instead of speaking to someone over the phone.”

If you live in Scotland and are the victim of a fraud in Scotland then please report this to Police Scotland either through the internet reporting page or by calling 101. You can also read more about Cyber Crime in our Keep Safe section.