

Neighbourhood Alert information sent on behalf of Nottinghamshire Police

Scams warning for Internet users 15/02/2012 10:07:46 [8913]

Police have asked computer users in Nottinghamshire to be on their guard after a number of suspected internet frauds were reported to the force.

Nottinghamshire Police have received a number of calls in relation to an internet scam where members of the public receive an online pop-up message claiming to be from Strathclyde Police or the Metropolitan Police.

The message states that the individual's computer has been locked by police, and that they will need to call a given number or pay a fine online for viewing inappropriate or illegal content online.

The computer screen locks in most cases.

Samantha Hancock, of Nottinghamshire Police's Pre-Crime Unit, said: "Various police forces across the UK have informed the public that this is an internet scam and has absolutely nothing to do with them.

"The police would like to make it clear that they would never ask the public for money under such circumstances and urge anyone who receives the pop-up to not to follow the payment instructions or call the number given.

"They should definitely not pay any money or divulge personal details."

Action Fraud and the National Fraud Intelligence Bureau are aware of the scam and are in the process of updating their websites with the correct information.

If you receive such a message on your computer, rest assured that no one has discovered any illegal material on your system.

Removal of the virus needs to be done with care using the operating system's 'Safe Mode' as an incorrect removal could easily lead to your computer becoming unusable and all your data and files being lost.

If you do not have specialised knowledge in this area, you are advised to seek professional advice in unlocking the computer and removing any associated virus.

In a separate scam reported in the county, a man paid £260 to secure a £1,500 loan after receiving an unsolicited telephone call from a company who knew he had been researching loans on the internet.

He never received the loan, and was verbally abused when he rang the company to enquire about it.

In several other cases, PC owners have been contacted by callers claiming to represent software companies, including Microsoft.

The callers have offered to install security packages on the computer and have been able to access the computer remotely.

The packages were installed, but it is not clear whether they are genuine packages or 'trojans' – computer programmes which contain viruses or damaging malware.

In all three cases, the computer owner was asked to make payment at shops with a Paypoint or Ukash facility or at a Western Union money transfer shop. Another similarity was that the callers all had telephone numbers with 0203 dialling codes.

Samantha Hancock added: "There is a real warning here about internet security. We all

know that when we go online our security is compromised to a certain degree, but you should always exercise caution if you receive a cold call from someone who appears to know exactly what you have been searching for.

“There is always a risk in accepting offers from cold callers in any event. It is also highly unusual for companies to request payment in this way. Certainly, in the case of the loan, we know that this has proven to be a fraud.

“There is nothing illegal about charging a fee to install a computer security package for someone or to resolve any other problem, as long as the service offered is legitimately provided. However, many genuine security packages can be easily downloaded free of charge.

“There are undoubtedly individuals around the world who have identified this as a potential cash-generating enterprise, but it is difficult to know whether they can be relied upon to do what they offer.

“If you are also suspicious that the caller is not the person they purport to be, it should sound alarm bells. Do not reveal personal financial information to anyone whose identity you cannot verify and trust. Loans should only be taken out with reputable, recognised companies.”

If anyone has any information about a similar incident, they should telephone:

**Nottinghamshire Police on 101
or Crimestoppers on 0800 555 111.**

Message sent by Lindsay Donnelly (Police, Administrator, Nottinghamshire)