View this email in your browser

May 2017

The purpose of this scams bulletin is to enable Hampshire residents to be aware, and therefore guard against the type of scams currently being reported to the Hampshire County Council Trading Standards Service.

Online Bank Account Scam

Hampshire Trading Standards Service has recently received reports from concerned residents whereby a fraudster had attempted to gain remote access to their computer.

The fraudster will make an unsolicited telephone call and pretend to be from a major company or organisation. They will impersonate well known internet service providers, computer companies, banks and law enforcement agencies. They may make claims that they can help with a slow internet connection or that there has been a recent data breach. They will offer to fix the problem and ask for remote access to the computer. Once this is given, they will gain entry to their victim's personal information including online banking facilities. At this stage they will transfer money from their victim's account into their own where it will not be traceable.

Case study 1

Mrs B was contacted on two occasions from someone who claimed to work for her internet provider company. They asked for remote access to her computer so they could check the internet connection speed. The fraudster managed to transfer £4000 from her bank account and they used her details to set up separate loans. Since this happened, Mrs B has not been able to use her computer as it has been corrupted. Mrs B is receiving support from the fraud department at her bank and from other agencies to help safeguard her.

Case study 2

Mr G received a cold call from someone who claimed to work for his telephone and internet provider. They said that there was a problem with his router and asked for remote access to his computer so they could carry out a fix. The caller said that if he did not allow this he would lose his internet connection. Once Mr G gave remote access to his computer the caller asked him to log into his bank account. Mr G said the caller continued to make threats that he would lose his internet access. Mr G became suspicious and terminated the call. Mr G contacted his bank and thankfully no money had been taken. He has since had the computer cleaned by a reputable company to remove any malware that may have been installed.

Case study 3

In other reported cases, sometimes the caller will take a long time to 'fix' the problem. They will then apologise to their victim and make an offer of compensation for the delay. They will ask their victim to log onto their bank account to check it has arrived. However, they will have installed a 'fake' screen showing the deposit has been paid but they will be working away in the background transferring money from the account.

To avoid falling victim to this scam, you:

- Should be wary of unsolicited approaches by phone claiming to offer a refund.
- Should avoid letting someone you do not know or trust have access to your computer, especially remotely.
- Should never log onto your internet bank while someone else has access to your computer.
- Should not share one-time passcodes or card reader codes with anyone.
- Should not disclose your 4-digit card PIN or your online banking password, even by tapping them into the telephone keypad.

Email Scams

Residents in Hampshire should remain alert over scam emails that appear to be from an official body. The email address will look genuine in an attempt to

confuse the recipient. If the email is opened it will contain a link asking for personal information including bank details.

Case study 1

Miss R received an email offering a tax refund. Because she received it at the start of the new tax year, Miss R assumed this was genuine. However, in order to claim the refund she was asked to click on a link to start the process. At this stage, Miss R became suspicious and reported the scam to Trading Standards so they could warn other residents. Miss R said she was due a tax rebate so very nearly went along with the scam.

Case study 2

Mr P received an email which appeared to be from O2 alleging his telephone bill needed to be paid. He was asked to click a link to make the payment. Mr P was concerned as he normally paid he telephone bill by direct debit and he did not think the email address looked correct. On checking with O2 they advised this was a scam.

Do not open any emails you are concerned about, click on links or open attachments. If in doubt, contact the official organisation for guidance and delete the email.

Global ransomware attack

Following the recent global ransomware attack, Hampshire residents are warned to be on the look out for emails claiming preventative measures can be taken to protect their data on an international scale.

One such email appears to be from BT and asks the recipient to click on a link to confirm a security upgrade. The email address may appear similar to the genuine one used by BT and this may catch people out. Remember that fraudsters can “spoof” an email address to make it look like one used by someone you trust.

If you receive one of these emails do not click on any links and follow our advice on how to stay safe. Go to the BT website directly and log in from there.

Doorstep crime warning

With the summer months approaching Hampshire residents are advised to be on their guard against strangers at the door. It can be difficult to tell whether the person is genuine, a rogue trader offering repair or home improvement or a bogus caller/distractions burglar trying to gain access to a property. Reports of doorstep crime in Hampshire include;

- Gardeners or Tree Surgeons offering general gardening work, garden clearance or felling branches from trees.
- Pressure washing of driveways or roofs.
- Drain inspection which normally results in an alleged fault being discovered.
- Gutter clearance.
- Driveways including block paving and tarmac.

There is no obligation for you to allow any person into your home and you are within your rights to refuse access. Sound advice is to say **"No"** to all doorstep cold callers.

If you are a Hampshire County Council resident you can request a free door sticker which may help you to say "No" to cold callers. Please contact Hampshire Trading Standards on 01962 833620 or **email**. You can also download a sign from the **Trading Standards website**.

Hampshire County Council residents are advised to report incidents of doorstep crime to the Quick Response Team at the Trading Standards Service on **01962 833666** or contact the Police on **999** if they feel the situation is urgent or that they are threatened in any way.

If you are worried about a potential scam please contact the Citizens Advice Consumer Helpline:

By telephone on **03454 04 05 06**
Web site: **Online consumer complaint form**

Trading Standards Service
Montgomery House, Monarch Way
Winchester, Hampshire, SO22 5PW

Hampshire County Council www.hants.gov.uk

Follow us on Twitter Unsubscribe from this newsletter

Hampshire County Council is not responsible for the content of external internet sites

Unsubscribe from this newsletter