Press Release

Friday 11 September, 2015

Jersey Fraud Prevention Forum issues warning and advice re Microsoft scammers

The Jersey Fraud Prevention Forum (JFPF) has today issued a warning to local residents to advise them of the increasing amount of telephone scam calls targeting the Island alleging that they are from Microsoft.

The JFPF can confirm that these are not genuine calls from Microsoft and we'd like to state that Microsoft will never cold call nor charge users for computer security or software fixes. This scam in various guises has been plaguing residents for several years and sadly people have parted with significant sums of money, their computers have been compromised and their personal details have been put at risk.

Fraudsters often use the names of well-known companies to commit their crime, as it makes their communication with you seem more legitimate. This is why it's important to think twice before giving out any personal information.

The Chairman of the Forum, Detective Chief Inspector, Lee Turner offered the following advice:

"If you do get one of these calls, the best defense is simple. Knowledge, be 'scam smart' and to simply put the phone down. Please also spread the word to friends and family who may be less tech savvy. Remember that neither Microsoft nor its representatives will ever cold-call consumers to charge for computer security or software fixes. Our remit is to protect the general public from these scams and the more people who know what to look out for, the less effective the fraudsters will be."

The JFPF has put together some key advice that you need to know about phone scams, along with some useful tips to avoid falling victim.

What do I do if I receive a scam phone call?

If you receive a scam phone call:

- Hang up
- Some of the calls received start with 0011534, so although it is not a local number, it may appear so at first impression
- Treat all unsolicited phone calls with skepticism and suspicion. Do not provide any personal information
- It's better to avoid being scammed rather than try to repair the damage afterwards

JERSEY FRAUD PREVENTION FORUM

What organisations do the scammers claim to be from?

Cybercriminals often claim to be from any of the following or similar sounding names:

- Windows Helpdesk
- Windows Service Center
- Microsoft Tech Support
- Microsoft Support
- Windows Technical Department Support Group
- Microsoft Research and Development Team (Microsoft R & D Team)

What can the scammers do if they gain access to my PC?

If cybercriminals gain access to your computer, they may do the following:

- Trick you into installing malicious software that could capture sensitive data, such as online banking user names and passwords. They might also then charge you to remove this software
- Take control of your computer remotely and adjust settings to leave your computer vulnerable
- Request credit card information so they can bill you for phony services
- Direct you to fraudulent websites and ask you to enter credit card and other personal or financial information there

What do I do if I have already given access to my computer?

If you think that you might have downloaded malware from a phone tech support scam website or allowed a cybercriminal to access your computer, take these steps:

- Change your computer's password, change the password on your main email account, and change the password for any financial accounts, especially your bank and credit card
- Scan your computer with a trusted safety scanner to find out if you have malware installed on your computer
- The advice from Microsoft is to install Microsoft Security Essentials. (Microsoft Security Essentials is a free programme. If someone calls you to install this product and then charge you for it, this is also a scam)
- Call your bank or building society to check that everything is in order

How did the scammers get my phone number?

- Cybercriminals often use publicly available phone directories so they might know your name and other personal information when they call you. They might even guess what operating system you're using

- Although law enforcement can trace phone numbers, perpetrators often use pay phones, disposable mobile phones, or stolen mobile phone numbers

Will Microsoft ever call me?

- You will never receive a legitimate call from Microsoft or our partners to charge you for computer fixes

How can I report a phone scam?

- You can report a phone scam to the States of Jersey Police on t: 612612

Further information about the Forum and the various types of scams and frauds can be found at www.fraudprevention.je

Ends.

For further enquires, please contact:
Emma Martin, Head of Communications
T: +44 (0)1534 822166 E: e.martin@jerseyfsc.org
M: +44 (0)7797 763 446 W: www.jerseyfsc.org