# Microsoft and Netsafe issue fresh warning about scammers

***New wave of scam reports a "timely reminder" of the need for vigilance***

**AUCKLAND, 5 December 2016** – Microsoft New Zealand and Netsafe are today renewing their call for New Zealand internet users to be aware of a fresh wave of scammers who are targeting this country with warnings about fake viruses on their computers.

The call for vigilance comes as Microsoft and Netsafe have both received a notable increase in reports of scammers trying to defraud people by phone or by using 'pop up' messages on screens. The scammers are claiming to be representatives of Microsoft and telling users that they have identified a problem with their device.

The scammers then offer to fix the 'compromised' device and ask for remote access which can reveal passwords, credit card details, bank account numbers and other information. They may also explicitly ask for payment so that protection software – which is in fact malicious – can be installed.

Netsafe says that some people have allowed access to their computers in these ways and have consequently lost money upwards of $400.

Chief Executive for Netsafe, Martin Cocker, says this pattern of phone scamming is not new and variations of it have been circulating for several years.

"The scammers claim to represent the Microsoft brand because the company is well known to have trusted experts, and so the calls may sound genuine," says Cocker.

"People are led to believe they are doing the right thing by handing over private passwords or details, but are soon fraudulently charged money, have their identity stolen, find their computer has been infected with viruses or other malware that seriously compromises their security."

Microsoft NZ's Marketing and Operations Director Frazer Scott says the key message Microsoft wants to make clear once again to New Zealand internet users is that the company will never call them asking for remote access to their computer.

"Microsoft DOES NOT call customers at home saying that we have detected a problem with their computer, and we will NEVER ask for passwords or other private details in any forum," says Scott.

Cocker says their advice to people who receive suspect calls is to hang up immediately.

"If you have given someone remote access to your device you should immediately end the session and contact Netsafe. If you have given any bank details to a caller, then contact your bank as soon as possible to advise them of the possible fraud."

Microsoft and Netsafe say that the recent fresh wave of reports about these scams is a timely reminder for people to be vigilant, and refer users to the following advice in the event they are called by a scammer.

**Features of scammer calls:**

- Overseas caller states they are from Microsoft or a Microsoft certified technician.
- Suggests the victim's computer is infected and harming others online or that their ISP has identified their system as a problem.
- Will get the computer owner to give the caller remote access using a genuine networking service or website like logmein123 or TeamViewer.

- They will use the 'Event Viewer' tool on the computer to highlight error messages which are supposedly signs of an infection.
- The cold caller will offer to clean up the infection and/or install security software and provide an ongoing support service costing anywhere up to $500.

**How to deal with the overseas cold callers:**

- Hang up the phone – engaging with or taunting these companies can lead to you receiving many more calls at all times of the day or night. Some technicians have resorted to threats or abuse to get computer owners to give remote access.
- If you do give access but become suspicious, disconnect from the session immediately. Netsafe has received some reports of these cold calling companies installing ransomware on the computer to ensure they get paid to unlock the PC.
- If you have previously given remote access, it may pay to check what has been installed on your computer and be certain there is no way for the company to continue accessing your system and files. Consult a trusted local PC technician if unsure.
- If you have paid money to these companies using a credit card, call your bank and discuss your options. If you sent funds via Western Union or another wire transfer service, then the money is gone and cannot be recovered.
- If you have given remote access to your device, handed over private passwords or other information report it Netsafe toll-free on 0508 NETSAFE (0508 638 723) or visit netsafe.org.nz/report
- For advice on how to stay safe online visit netsafe.org.nz

- ENDS -

***For more information, contact:***

**Netsafe:** Kimberly Burgess
Marketing & Communications Advisor - Netsafe
Mobile: +64 221600697
Email: kimberlyb@netsafe.org.nz

**Microsoft:** Brendan Boughen
Senior Communications Manager – Microsoft NZ
Mobile: +64 27 839 6044
Email: brendan.boughen@microsoft.com

**About Microsoft**

Microsoft (Nasdaq "MSFT" @microsoft) is the leading platform and productivity company for the mobile-first, cloud-first world, and its mission is to empower every person and every organization on the planet to achieve more.