March 2014: SCAMwatch and Telstra are warning consumers to hang up the phone if they receive a call out of the blue from someone claiming there is a problem with their internet connection or computer.

Recent months have seen a surge in reports of scammers calling people at home and raising a false alarm that they are at risk of their internet being disconnected immediately, as their computer has been hacked or infected with malware and is threatening Telstra's internet infrastructure. The caller claims that they are able to fix the problem on the spot, however a fee for this service will need to be paid and the person will also need to download software that will allow the caller remote access to their computer.

If the person resists or questions the scammer, they up the ante. Scammers have reportedly threatened to sue people for putting Telstra's infrastructure at risk. When the person has requested proof that they are a Telstra rep, scammers have given out a fake number for Telstra which, when the consumer calls, puts them back on the line with the scammer. These scammers are also well-versed at creating a sense of urgency to incite fear and anxiety that your device has been compromised and must be fixed immediately.

If you provide your credit card details and give remote access to your computer, the scammer may not only take more than the stated 'fee', but also infect your computer to gain access to your personal information and commit other acts of fraud.

Scammers often pose as well-known and reputable businesses to try and convince you that they're the real deal, with Telstra a popular target. Scammers pretending to be from Telstra have been known to switch consumers to another service provider that the consumer did not knowingly agree to. Scammers don't just fish for your details over the phone; they also send phishing emails pretending to be from Telstra or BigPond® to try to get you to hand over your account details, or to click on a link or open a document infected with malware. The 'Yellow Pages' directory scam has also targeted Australian small businesses, with scammers deceiving them to sign up to an online business directory service that falsely claims to be affiliated with Sensis and Telstra.

Watch out – scammers know how to press your buttons when they get you on the phone. If you receive a call out of the blue from someone claiming to represent Telstra and they ask for access to your computer, just hang up.

How this scam works

- You receive a phone call out of the blue from someone claiming to be a representative of Telstra or Telstra BigPond®. They may sound like the real deal, claiming to be from 'Telstra Technical Support' and using technical jargon.
- The caller claims that you need to take immediate action to avoid your internet connection being terminated or disconnected, as your computer has been hacked or infected with malware and is threatening Telstra's internet infrastructure.
- In order to fix the problem, the caller will claim that you will need to pay them a service fee (typically around $10) to have a specialist look at your computer. They will also ask you to download a software program so that they can gain remote access to your computer and run a scan.
- The scammer may initially sound professional and knowledgeable, however they will be very persistent and may become abusive if you don't do what they ask. They may even threaten to sue you for putting Telstra's internet infrastructure at risk.
- If you provide your financial details or give remote access, you might find a lot more money taken out of your bank account than you agreed to, with some victims reporting losing over $5,000 from multiple withdrawals. Your computer may also be infected with malicious software, giving scammers access to your personal details stored on the device (including

bank account information).
- Note: you don't have to be a Telstra customer to be called by these scammers. You don't even have to own a computer!

Protect yourself

- If you receive a phone call out of the blue from someone claiming to be a representative of Telstra and their call relates to a problem with your internet connection, just hang up.
- If you have doubts about the identity of any caller who claims to represent a business, organisation or government department, contact the body directly. Don't rely on contact details provided by the person – find them through an independent source such as a phone book or online search.
- Remember that you can still receive scam calls even if you have a private number or have listed your number on the Australian Government's Do Not Call Register. Scammers can obtain your number fraudulently or from anywhere it has been publicly listed such as in a phone book.
- Don't let scammers press your buttons – scammers use detailed scripts to convince you that they're the real deal and create a high pressure situation to make a decision on the spot.
- Always keep your computer security up to date with anti-virus and anti-spyware software, and a good firewall. Only buy computer and anti-virus software from a reputable source.
- Never give your personal, credit card or online account details over the phone unless you made the call and the phone number came from a trusted source.
- Never give a stranger remote access to your computer, even if they claim to be from a reputable business.
- If you think your computer's security has been compromised, use your security software to run a virus check. If you still have doubts, contact your anti-virus software provider or a computer specialist.
- If you think you have provided your account details to a scammer, contact your bank or financial institution immediately.

Report

You can report scams to the ACCC via the SCAMwatch report a scam page or by calling 1300 795 995.

More information

SCAMwatch has previously issued radars about scammers pretending to be affiliated with Telstra:

- August 2013: Small businesses beware – 'Yellow Pages' directory scam strikes again
- August 2011: Computer remote access scammers now masquerading as Telstra - new twist
- September 2010: Telstra warns of email scam targeting BigPond customers.

Stay one step ahead of scammers – follow @SCAMwatch_gov on Twitter or visit http://twitter.com/SCAMwatch_gov.