



Tasmanian Perpetual Trustees

Security Alert

Computer Virus cold call scam

Tasmanian Perpetual Trustees are committed to protecting their customers against any potential threats to personal banking security. As such, we would like to make sure all customers are aware of the scams and fraud attempts currently circulating.

The **computer virus cold call scam** involves customers receiving a phone call out of the blue from someone claiming to be from, or associated with, Windows or Microsoft. The caller will then claim that they have detected a virus on your computer, and will ask you to open Windows Event Viewer on your machine to confirm that it is infected. When you open the program, you'll notice several error messages. The scammers will use these error messages to convince you that your computer has a virus, however it is important to remember that **errors such as these are very common and mostly harmless**.

Nonetheless, the caller will tell you that you should be concerned, and will then offer to refer you to a 'technician' who can fix the problem for a fee. From here, you will be offered a number of solutions – all designed to trick you into compromising your personal security or paying for things you don't really need. These include:

- Install an antivirus program on your computer (usually the kind you can download from a reputable source for free) and charge you a 'fee' for the service
- Ask for your credit card details but install nothing. Your details might then be sold to other parties or used for fraudulent purposes
- Install malware (short for malicious software) on your computer to enable it to be controlled remotely for other illegal and harmful activities
- Access and steal personal and financial details from your computer

Scammers have also been known to make follow up calls to people who fell victim to the initial scam, claiming they're from a foreign government, law enforcement body or even from your bank and promising to recover the money you lost from the first scam – in return for a fee.

Remember, **stay vigilant**. If you're being pressured into disclosing personal information or sending money to a stranger, it's almost certainly a scam.

We take the safety and security of our customers' banking and personal details very seriously, so if you're unsure about anything, or feel your account may be at risk, please don't hesitate to contact us on 1300 138 044, drop into your nearest branch or visit our [Security](#) page.

You can stay on top of current fraud and scam attempts by visiting the Australian Government's [SCAMwatch](#) and [Stay Smart Online](#) websites.