



# Advice for Internet Users

*Effective 1 April 2009*

**0508 888 800**  
[www.telstraclear.co.nz](http://www.telstraclear.co.nz)

**TelstraClear** Now's Good

### Would you like to get a large unexpected bill?

The internet is a great source of information, and a convenient method of keeping in contact with friends and family but there are some risks. If you are an internet user, regardless of your internet provider, online security is an important consideration.

## What are some of the risks?

### Malware

Malware is a generic term used to describe malicious software, which installs itself on your computer system or network and is designed to cause damage, redirect your internet connection or steal personal information. Common types of malware include:

#### **Virus:**

This is software intended to cause damage to your computer and/or network. Usually delivered via email, it is frequently self-propagating and generates high amounts of internet usage.

#### **Trojan:**

A Trojan is created to hijack your computer system. Often a Trojan will use your computer to relay spam email or redirect your internet traffic which sometimes results in toll charges.

#### **Spyware:**

Designed to steal your personal or financial information, spyware is often downloaded unwittingly when online. Once installed, it sends out information on websites you visit and anything you've typed on your computer e.g. usernames, passwords and credit card details.

### Hoaxes and Scams

Hoax emails are designed to deliver malware to your computer system or trick you into providing personal information (often known as phishing). They may also link to a website for the same purpose.

## What can I do to minimise these risks?

### Use TelstraClear Email

TelstraClear provides its email customers with virus scanning on all email sent to your TelstraClear email address and this is scanned before you receive it. If a virus is detected, an attempt will be made to remove the virus. A successful attempt will mean that the email and attachment will be passed on to you without the virus, while an unsuccessful attempt will result in you receiving a copy of the original message without the attachment, and a notification message advising the virus and attachment has been removed.

### Install Security Software

We strongly recommend that customers install a trusted internet security software suite making sure that it includes anti-virus protection, a firewall and spyware detection capabilities.

#### **Anti-virus:**

Anti-virus software maintains a database of known viruses by way of regular updates. As well as performing regular scheduled scans of your entire computer system, it is also designed to run in the background while your computer is running and detect any newly introduced threats.

#### **Firewall:**

A firewall allows you to dictate which computers on the internet can make contact with your computer. Some firewall software comes pre-configured and will automatically stop some of the more common that might access your computer.

#### **Spyware Detection:**

Spyware detection works in a very similar way to anti-virus software but specifically targets spyware.

It is important to note that no security software is going to be 100% effective all of the time. Unfortunately there is always going to be some time between when new malware is created and the time updates can be issued to address them.

### Update Regularly

Ensure that you regularly update your security software to protect you from new threats. Most security software has an automatic update option. We recommend you turn this on. We also recommend that you regularly update your operating system. Manufacturers of popular operating systems such as Microsoft Windows frequently create security updates for their products to protect users from exploits in their products that malware could take advantage of.

### Read Before You Click

It can be easy to click 'yes' or 'ok' on everything that pops up on your screen when surfing the internet. However doing this without paying attention can result in you agreeing to terms and conditions that could install spyware on your system. Always make sure you understand what you are agreeing to before you confirm it.

### Look For Signs Of A Secure Website

Before you enter any personal details into a form on a website, ensure that you check that it's a secure website. These are noted by the presence of a padlock icon usually located in the bottom bar of your web browser, and a URL (website name) that starts with https rather than the usual http. The 's' notes that the website is secure.

### Enable Toll Call Control

Internet diallers, sometimes called Premium Rate Diallers, are a security problem experienced usually by dial up internet users. Internet diallers install themselves on your computer and replace the phone number your computer normally uses to connect to your internet provider to that of a paid service. The first most users know of the issue is when they see 0900 and toll calls on their phone bill. If this is an issue for you, ask your phone provider about putting a pin number in place that must be used every time a toll call is made from your phone line.

### Turn It Off

If your modem or computer are off, there's no internet traffic passing through them. Switch your computer and modem off when you are not using them. With modems in particular, make sure they are completely off rather than in Standby Mode. If unsure, unplug it from the power supply.

### Do Personal Stuff At Home

If at all possible, avoid using public computers such as those in libraries and internet cafés to perform personal tasks such as internet banking. You can never be sure about how safe and secure public computers are.

### Change Your Password

Although it sounds like an inconvenience, regularly changing commonly used passwords is highly recommended for internet users. How often you do this is up to you but at least once a month is a good starting point. When thinking of a new password try and use a combination of letters and numbers and avoid anything that's immediately recognisable such as car registration numbers, birthdays and addresses.

### Check your Usage

TelstraClear recommends you regularly check your internet usage online on the TelstraClear website at [www.telstraclear.co.nz/go/usagemeters](http://www.telstraclear.co.nz/go/usagemeters)

### Be Wary When Handling Email

Email is often used to target internet users. There are some common sense checks that you can make if you suspect an email you've received may be of a malicious nature. In general, if you think it's suspicious, delete it and definitely don't reply.

#### *Do you recognise the sender?*

If not, it's probably not a good idea to open or reply to this email. It may just be harmless spam, but it could be a scam designed to trick you into revealing personal information.

#### *Is the email addressed to you directly?*

Check the 'To' field of the email. If you see a large number of email addresses or an email address that looks similar to yours but is not quite right, be suspicious. Also look for emails that address you with Dear Customer or use your email address as a name.

#### *Does the email address look legitimate?*

Always check the 'domain' of the email address. The domain is the last part of the email address after the @ symbol e.g. the domain of help@clear.net.nz is clear.net.nz. If an email looks as though it's come from one company but has an unrelated domain, this could indicate a scam or malware.

#### *Are you being asked for personal information?*

Common hoax emails will often ask you to provide personal information and advise that failure to do so will have negative consequences eg the shut down of your account.

#### *Is there incorrect spelling and grammar throughout the email?*

Hoax emails are sometimes literal translations of scams originally written in another language. This often results in obvious grammatical errors and spelling mistakes. It's also not unusual for some hoax emails to be completely typed in CAPITAL LETTERS.

#### *Is the email warning you of a potential threat?*

Unless you've subscribed to a service that updates you about internet security threats, emails you receive about potential threats are most likely not genuine.

#### *Are there outlandish promises being made in the email?*

If it looks too good to be true, then it probably is.

#### *Do you see any suspicious links or attachments?*

### File Sharing Software

TelstraClear discourages the use of file sharing software. We remind users to monitor all data transfer and that users are responsible for all charges incurred.

### What can I do to help TelstraClear?

#### Let Us Know

While we have systems in place to advise us if a threat is present on our network, we also rely on our users to notify us if they suspect something is wrong. If you receive a hoax or scam email, forward a copy of the email to **missedspam@clear.net.nz**

Once we have received multiple examples of the same email and the threat has been confirmed, our systems will proactively block any further examples of this email.

#### Be Security Smart

By ensuring you follow 'best practice' in relation to your online security, you may be helping to stop the spread of a scam or malware. Not only are you assisting TelstraClear, you are also assisting other TelstraClear customers and all internet users.

#### More Information:

For more information about Online Security, visit the **NetSafe** website on **[www.netsafe.org.nz](http://www.netsafe.org.nz)**

NetSafe is a programme of New Zealand's Internet Safety Group (ISG), which has been designated the Ministry of Education's 'agent of choice' for cybersafety education in New Zealand.



### **Residential Customer Care**

Phone TollFree 0508 888 800

Fax TollFree 0508 888 801

Freepost

TelstraClear, Freepost 4768,

Private Bag 92143,

Victoria Street West, Auckland 1142

# 0508 888 800

[www.telstraclear.co.nz](http://www.telstraclear.co.nz)



**TelstraClear**

**Now's Good**