

Where to get information on how to WOF your computer

On the Internet

These websites provide information about online safety and security, and links to other good sites:

www.netsafe.org.nz
www.itsafe.gov.uk
www.symantec.com
www.microsoft.com/security
www.westpac.co.nz

Online Safety Guide

Westpac has recently produced a 24-page guide covering the basics, from the types of anti-virus and anti-spyware needed to tips for online shopping and email use. Download direct from www.westpac.co.nz or order a hard copy, either online or by phoning Westpac on 0800 400 600.

Articles

Watch for articles on computer security in newspapers, computer magazines and in publications like Consumer and NetGuide. Listen for radio shows about this topic too!

Courses

Courses on basic Information and Communications Technology (ICT) skills offered by local training providers and institutions can be big confidence builders. Check the NetSafe website for the upcoming computer security and cybersafety courses that the Internet Safety Group is developing with e-learning provider Intuto.

Computer retailers

Ask a store if they offer new computers pre-loaded with security software, and if those programs are the latest updated versions. It may cost you a little more, and may mean a few days delay before taking delivery of your new machine, but it's an investment of time and money you won't regret.

1	NetSafe	16
2	The Internet Safety Group	17
3	Warrant of Fitness	18
4	05/06	19
5		20
6		21
7		22
8		23
9		24
10		25
11		26
12		27
13		28
14		29
15		30
16		
17	FIREWALL	
18	OPERATING SYSTEM	
19	ANTI VIRUS	
20		
21		
22	UPDATED	
23		
24		
25		
26		
27		
28		
29		
30		

The Internet Safety Group thanks the industry and government sponsors who have generously given their financial support and encouragement to this NetSafe campaign.

Westpac

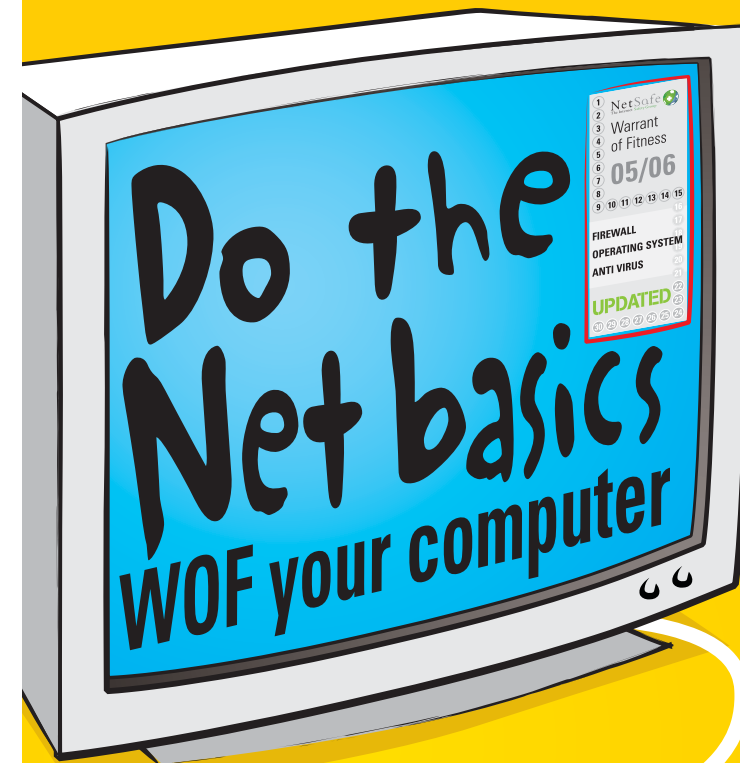
Primary Sponsor

symantec.



This brochure is endorsed by the Government's Digital Strategy which supports this campaign and other measures to ensure that Kiwis of all ages can enjoy a safer and more secure online experience.

Many organisations across New Zealand are helping spread the word about the Net basics by offering links to the NetSafe website. We appreciate that support.



Safe surfing starts with a secure system

visit www.netsafe.org.nz

NetSafe
The Internet Safety Group



Why WOF your computer?

Internet hazards are a fact of life on the 'information superhighway', and they're growing in both number and sophistication: viruses, trojans, spyware, keystroke logging, identity and credit card theft, phishing scams, spam, system compromise, and more.

One way to reduce your risk online, and protect your information, is to do the Net basics.

- Install a firewall and keep it updated.
- Get your operating system updated, and automate this if possible.
- Make sure your system is equipped with an effective, updatable anti-virus program (can come bundled with a firewall & anti-spyware).
- Don't forget to scan for spyware (this can be automated as well).
- Keep your password private and change it regularly.

Before you venture online, do the Net basics... it's like getting a computer WOF!

For more detailed information on the Net basics, computer security, and other online safety issues, visit the Internet Safety Group's NetSafe website www.netsafe.org.nz.

What are some of the risks online?

'Malware' or malicious code including:

- Virus - self-replicating; attaches itself to files or programs so it can spread, often via an email attachment.
- Worm - exploits computer weaknesses without any human action needed
- Trojan - looks benign but hides malicious code which can give someone access to your machine and the ability to take control
- Dialer - 'hijacks' a modem and switches an Internet connection to a premium-rate phone line, often located overseas
- Adware - brings up unwanted banner ads and pop-ups
- Spyware - gathers information about the user without their knowledge and forwards that to advertisers or other parties
- Keystroke loggers - hardware or software that records all the information typed on the keyboard for the installer (who may not be a stranger - can be a spouse, flatmate or co-worker etc)

Spam

Junk email that can deliver scams, such as phishing emails which falsely claim to be from a legitimate business or agency (often with the correct logo) in an attempt to trick the user into revealing account details & passwords.

Hackers

Criminals seeking to break into your system (often young opportunists, but sometimes highly skilled computer criminals) to vandalise your machine or to steal from you: your bank account, credit card or other identity details, your stored passwords, your work projects or your sensitive correspondence.

Compromise

A compromised computer is under someone else's control; often the victim may notice only a periodic slowdown of their computer, perhaps because the machine is sending out SPAM (junk) email. It is estimated that the average time until your computer is compromised, when using a broadband connection without a firewall, is now 12-14 minutes.

How would I know if my computer might be 'infected' or compromised?

You may notice one or more of the following:

- A periodic slowdown or your computer sending out much more data than you have asked it to send
 - Random dialing by the modem or dialing strange numbers
 - New icons or toolbars appear on your machine
 - Programs lock-up frequently
 - Your browser homepage has changed.
- Sometimes there are no symptoms at all, which is why periodic scanning is vital.**

The Net basics

Firewall

A firewall, either software or hardware, protects your computer from unauthorised access. It controls who is allowed to access the information on your machine. Zone Alarm (www.zonelabs.com) offers a basic free version or you can also purchase packages that bundle a firewall with other security software, such as anti-virus and anti-spyware. Good packages include Symantec's Norton Internet Security, McAfee and Trend Micro.

Operating system (OS)

Most people use a version of Microsoft Windows® as their operating system. Whenever new security risks are identified, Microsoft releases free updates (for versions '98 and after). Installing updates is critical! Keep your system up-to-date by either switching-on your system's Automatic Update function (versions 2000 and after) or regularly visiting the Windows Update site <http://update.microsoft.com>. If you're running Apple Macintosh or Linux, check out their updates.

Anti-virus software

Anti-virus software is absolutely essential. It can detect viruses on your system, screen incoming email attachments and even prevent you emailing viruses to others. Your Internet Service Provider (ISP) may offer an email filter, which will help, but you still need your own on-board anti-virus program. Check out proven AV programs at computer stores, or download your choice from a reputable Internet site. Some programs are free! All feature update functions and scanners that let you regularly check all your files for viruses.

Check for spyware

Choose a reputable brand, such as AdAware (www.lavasoft.com), SpyBot (www.spybot.info/en/index.html) or Microsoft AntiSpyware (Beta), which is offered free online, or brands mentioned previously that come bundled with other security software. Be aware that some free 'anti-spyware' actually contains spyware!

Use a STRONG password

Keep your password secret and select one that is 8 characters with a mix of lower case (abc..) and upper case (ABC..) letters, symbols (#&*..) and numerals (123..). There are good techniques on the NetSafe website to help you remember as you change your password regularly.