Online Security Policy

vocal™

100% Aussie Telco since 2003

Internet security is an ongoing challenge – but it is a challenge that must be met if you are to enjoy a safer and more secure online experience. As Internet users, we are all required to play our part in promoting and practicing a "culture of cyber security".

The Internet Industry Association recommends that the following top tips be taken to help ensure that your computer stays adequately protected for a safer and more secure online experience:

- **Take action immediately if you suspect your computer has been compromised.** Report unauthorised access to the police. Change your passwords immediately and contact your bank if you suspect personal financial information has been stolen.

- Keep your anti-virus and other security software updated.

- Install a firewall to prevent unauthorised access to your computer.

- Turn on automatic updates so that all your software receives the latest fixes.

- Get a stronger password and change it regularly.

- **Stop and think before you click on links or attachments.** Don't open suspicious emails or attachments from unknown sources. Don't click on links in emails requesting your personal details.

- **Check your "sent items" file or "outgoing" email.** If you find unknown messages in your out box, it is a sign that your computer may be infected with spyware and may be part of a botnet. This isn't foolproof: many spammers have learned to hide their unauthorised access.

- Stop and think before you share any personal or financial information about yourself, your friends or family online.

- **Configure your wireless network securely.** If you are using a wireless router/modem, enable the security features with a strong password. Use WPA or WPA2 encryption on your Wi-Fi equipment (WEP is an older standard and is less secure). Refer to your router/modem manual or contact your ISP for further details.

- Know what your children are doing online. Make sure they know how to stay safe and encourage them to report anything suspicious. For further information about online safety go to the Australian Government's Cybersafety website: www.cybersmart.gov.au.

MORE INFORMATION AND TOOLS FOR ONGOING SECURITY

Learn more about securing your computer at www.icode.net.au. This site offers practical tips from the internet industry to help guard against Internet fraud, computer security, and the protection of personal information. This site also provides information about recommended products and services to help ensure ongoing protection.

In addition, the Australian Government undertakes a range of awareness raising initiatives including:

- The Australian Government's cyber security website www.staysmartonline.gov.au

- The Stay Smart Online email alert service.

- An annual National Cyber-security Awareness Week.

Visit www.staysmartonline.gov.au for more details about these initiatives.

The Australian Communications and Media Authority is a statutory body responsible for the regulation of broadcasting, the Internet, radiocommunications and telecommunications.

The ACMA operates a range of cybersafety and cyber security education and awareness programs designed for children, parents and teachers. To learn more about these programs visit www.cybersmart.gov.au

ABOUT DNS CHANGER MALWARE?

The Domain Name System (DNS) works like a telephone book for the internet, changing domain names into numerical Internet Protocol (IP) addresses. When you enter a domain name (such as 'www.staysmartonline.gov.au') into your web browser, the computer contacts the DNS servers to find the IP address that corresponds to the domain name (for example, 172.16.254.1).

Your computer then uses this IP address to connect to the website you are looking for. The DNS servers you use are usually operated by your Internet Service Provider (ISP) and form part of the network which connects your computer to the internet.

Without the DNS and DNS servers, you would not be able to access websites, send e-mail, or use many other internet services.

Criminals have learned that if they can control DNS servers, they can control which sites a user connects to on the internet. By controlling a user's DNS, a criminal can cause an internet user to unknowingly access fraudulent or malicious content, or otherwise interfere with a user's web browsing.

WHAT DNS CHANGER DOES TO YOUR COMPUTER

DNS Changer alters your computer's DNS settings to replace your 'default' DNS settings with settings that connect to the rogue DNS servers. DNS Changer also attempts to access devices on your network such as your router and change their DNS settings so that they connect to the rogue DNS servers.

This means that all the computers on your network can be affected by DNS Changer, even if they are not directly infected with the malware.

AM I INFECTED?

The Australian Communications and Media Authority (ACMA), CERT Australia and the Department of Broadband, Communications and the Digital Economy (DBCDE) have established a diagnostic website at dns-ok.gov.au that, in most cases, can be used to confirm whether your computer has been infected with DNS Changer. This website also provides links to tools, provided by anti-malware companies, that can be

used to remove the infection and gives advice about the steps to follow to remove the infection.

CHECKING YOUR COMPUTER

You can perform an automatic check of whether your computer is infected with DNS Changer by visiting the dns-ok.gov.au diagnostic website.

If you prefer to perform a manual diagnosis, you will need to check the computer's DNS settings and the settings of any wireless access point or routers you may be using. The FBI provides the following instruction (PDF) for checking the DNS settings on a range of operating systems.

You may also wish to seek advice from a computer professional to assist you in diagnosing and removing DNS Changer.

For further info please visit: www.acma.gov.au

CONTACT INFORMATION

If you require further information regarding Vocal's Complaint Handling Policy, you can contact VocalTM Customer Service Centre on:

Telephone: **1300 796700**

Vocal Channels Pty Limited
PO Box 1020
Surry Hills NSW 2010

Questions about the Complaint Handling Policy Policy should be sent to us at info@vocal.com.au

Retail Service Provider of

1300 796 700 | www.vocal.com.au

Vocal Channels Pty Limited
(ABN 44 131 307 858) PO Box 1020, Surry Hills NSW 2010

vocal

Hours 9am - 6pm AEST Mon - Fri
support@vocal.com.au