

INTERNET INDUSTRY CODE OF PRACTICE

INTERNET SERVICE PROVIDERS
VOLUNTARY CODE OF PRACTICE

FOR INDUSTRY SELF-REGULATION
IN THE AREA OF e-SECURITY

September 2009

Consultation Version 1.0



Internet Industry Association
www.ii.net.au

TABLE OF CONTENTS

TABLE OF CONTENTS	2
PART A – PRELIMINARY	3
1. Preamble	3
2. Objectives	5
3. Scope of this Code	5
4. Principles	6
5. Terminology and interpretation	7
PART B – RECOMMENDED ACTIONS FOR ISPs	8
6. Detection, Education, Reporting	8
7. Trustmark	10
PART C - GENERAL	11
8. Dates of Implementation	11
9. Code Review	11
Schedule 1 – Standardised Information for Customers	12
Schedule 2 – Sources of Information Relating to Compromised Computers	15
Schedule 3 – Agencies to be notified in event of serious attack	17

PART A – PRELIMINARY

1. Preamble

- 1.1 The IIA recognises the enormous benefits that the Internet can bring to all Australians, including the provision of and access to health and education services, enhanced opportunities for business and as a communications, information and educational tool.
- 1.2 The IIA also recognises that the Internet can bring with it some risks to which end users may not wish to be exposed. Whilst it would be impractical and ineffective to monitor all Internet services for known risks, technologies can be utilised by end users to manage risk to some extent. Ultimately, however, the Internet cannot be made risk free if it is to function effectively, and ISPs and consumers can and must share responsibility for minimising the risks.
- 1.3 There are measures that Internet Service Providers (ISPs) can take to address some e-Security issues, which is why industry has developed this Code. It will assist and encourage all ISPs to follow this Code's recommendations on the identification and reporting of potentially compromised computers that are a security threat to not only the Internet but to their customers.
- 1.4 The IIA also endorses and supports effective, practical and appropriate measures that assist Australians to manage their use of the internet. The IIA recognises end user empowerment as one of the most effective strategies to manage content issues. Specifically, the IIA endorses, and this Code supports, the provision of information about security issues to end users, including strategies for managing risk behaviour as well as the availability of end user tools by which responsible users can facilitate controls that are appropriate for their level of exposure.
- 1.4 The IIA is aware that this is a dynamic area of development and as such has developed the Code with a view to being consistent with all currently known requirements in relation to this Code's subject matter. In particular, this Code does not purport to cover all aspects of online security, but rather it is intended to coexist with measures occurring elsewhere, for example other IIA Codes (including the Spam Code of Practice), the Cybercrime Act 2001 and other relevant Commonwealth, State and Territory legislation.

While present security technologies have various levels of sophistication depending on the medium to which they are applied, the IIA remains committed to monitoring developments in such technologies and to keeping its members informed of these developments.

- 1.5 The IIA is aware of significant benefits that will accrue from this scheme. In particular, the scheme enables ISPs to assist their customers by providing them with advice that their computer appears to be compromised, thereby giving them the opportunity to remedy this situation. Such restorative action by customers will contribute to the overall security of the Australian and international Internet. The problems associated with zombie computers and 'botnets' (aggregations of zombie computers) are many and varied; including:

- **identity theft:** the malware installed on the customer's computer potentially may extract personal information, such as Internet banking passwords and login information, for criminal usage;
- **ddos** (distributed denial of service) attacks on websites, which may render the website inoperable during the attack;
- **dissemination of Spam:** over 90 per cent of Spam is reportedly now sent from zombie computers;
- **dissemination of malware,** which is either embedded in the Spam sent from botnets, or through directing Spam email recipients to websites where malware is downloaded onto their computer; and
- **hosting of illegal content** on a zombie computer, such as child pornography.

Internet Service Providers also have an interest in the integrity of the email system, which is threatened by the onslaught of Spam routed through Spam zombies. In addition, recipients may blame the ISP for Spam that appears to have originated from its system, or its customers' systems. The Spam may also cause ISP network connections to bear unnecessary loads, increasing their administrative costs.

Through participating in the scheme, it is believed ISPs will contribute to the overall reduction of Spam and eSecurity compromises, thereby in general terms reducing their costs and those of Internet users.

- 1.6 As stated in subsection 4(3) of the Act, Parliament intends that internet content hosted in Australia, and internet carriage services supplied to end users in Australia, be regulated in a manner that:
- (a) enables public interest considerations to be addressed in a way that does not impose unnecessary financial and administrative burdens on Content Hosts and Internet service providers (ISPs);
 - (b) will readily accommodate technological change; and
 - (c) encourages:
 - the development of Internet technologies and their application;
 - the provision of services made practicable by those technologies to the Australian community; and
 - the supply of Internet carriage services at performance standards that reasonably meet the social, industrial and commercial needs of the Australian community.
- 1.7 To give effect to Parliament's intent as expressed above, all recommendations for ISPs as set out in this Code will be interpreted in a manner that is consistent with that intent.

2. Objectives

2.1 The aims of the Code include:

- (a) Instilling within ISPs in Australia a culture of e-Security within their organisations and with their customers.
- (b) Providing a means by which consistent messaging and plain language information can be provided to end users that will:
 - i. raise awareness and educate them about e-Security risks; and
 - ii. set out simple steps that they can take to better protect themselves online.
- (c) Encouraging ISPs to actively check for suspicious activity within their networks and source information on compromised computers, through participation in the Australian Communications and Media Authority's (ACMA's) Australian Internet Security Initiative (AISI) or by seeking information from other sources.
- (d) Encouraging ISPs to report repeated or severe instances of suspicious activity to relevant Government agencies, where it is believed the suspicious activity constitutes a serious threat to Australian communications networks.

2.2 The Code will provide guidance on how service providers can:

- (a) detect malicious activity on a customer's compromised computer;
- (b) take steps to respond to the AISI reports or any other source of information that may relate to malicious activity;
- (c) inform a customer that their computers maybe compromised;
- (d) educate consumers on what actions they can take to protect their computers from malicious activity; and
- (e) notify Australian authorities of a malicious activity without prejudice.

The Code provides a list of resources that ISPs could access to provide intelligence on sources of attack.

3. Scope of this Code

3.1 This Code is voluntary.

3.2 This Code is applicable to the following industry sectors:

- (a) Internet Service Providers (ISPs) as defined under Schedule 5 of the *Broadcasting Services Act 1992* (Cth).

3.3 The Code does not apply to:

- (a) the provision of premium SMS or MMS services which involve the sending of Content to or between End Users;
- (b) steps that ISPs and Email Service Providers are required to undertake to minimise the amount of Spam sent and received by their customers under the Internet Industry Spam Code of Practice, which has been registered with the Australian Communications and Media Authority. (Although this Code should be read in conjunction with the Internet Industry Spam Code of Practice.)

At this point in time, this voluntary Code is directed primarily at Internet Service Providers, but it is recognised by all in the e-Security community that attacks on mobile networks are likely to appear in increasing numbers in the future. Due to this, the Code has been written in such a way as to provide guidance which can be implemented by either ISPs or mobile network providers.

3.4 The e-Security measures listed in this Code are not an exhaustive list, but a guide as to some of the steps ISPs (and other service providers) can take to improve the e-Security of their customers and their networks. It is envisaged that these measures will change over time, in response to the changes in malicious activity and compromises that will appear.

3.5 The Code makes provision for the use of a Trustmark to signify to users that their ISP complies with this Code.

4. Principles

4.1 In seeking to achieve its objectives, the Code applies the following principles:

- (a) as far as practicable, there should be “electronic equivalence” (that is, behaviour and transactions that can take place in the real world should be permissible over the Internet without additional requirements or restrictions);
- (b) the Code should be technically neutral;
- (c) requirements should be fair to all concerned;
- (d) the measures recommended in the Code should not adversely affect the commercial viability of the parties and the services they make available;
- (e) just as ISPs have a role to play in Internet security, so do end users. End users must accept some responsibility for securing access to their home computers and Internet connections (for example, by installing and keeping up to date anti-

virus software, securing their wireless networks, etc);

- (f) the Code is designed to be flexible and allow for a range of responses according to ISPs' circumstances;
- (g) the development of the Code is predicated on a recognition that compromised computers represent a threat to the integrity of networks;
- (h) the privacy of end users is paramount. In support of this principle the Code does not require the surveillance of individual online activity; indeed the fulfillment of objectives of this Code will advance the privacy interests of users by reducing the scope for identity theft;
- (i) the Code draws upon existing industry best practices;
- (j) it is recognised that some attacks are more severe than others and ISPs should make provision for prioritisation or deprioritisation, as the case may be, of action depending on the nature of the threat;
- (k) education of Internet users is a key element of the strategy;
- (l) in some cases, ISPs may be required to report instances of compromises, malicious activity or attacks to relevant law enforcement agencies or to provide reasonable assistance as required under the *Telecommunications Act 1997*.

5. Terminology and interpretation

5.1 In the Code, the following terms have the meaning shown:

ACMA	the Australian Communications and Media Authority
Act	the Broadcasting Services Act 1992 (Cth)
AISI	Australian Internet Security Initiative
Bandwidth	refers to the rate supported by a network connection or interface usually expressed as bits per second (BPS)
Botnet	A botnet (also known as a zombie army) is a number of Internet computers that, although their owners are unaware of it, have been set up to forward transmissions (including Spam or viruses) to other computers on the Internet. Any such computer is referred to as a zombie - in effect, a computer "robot" or "bot" that serves the wishes of some master Spam or virus originator
Daemon	is a process that runs in the background and performs a specified operation at predefined times or in response to a certain event.
DBCDE	the Department of Broadband, Communications and the Digital

	Economy
DDOS	distributed denial of service
Malware	is short for malicious software and is designed to specifically damage or disrupt systems (for example a virus)
Network firewall	protects a computer network from unauthorized access. Network firewalls may be hardware devices, software programs or a combination of the two. They guard an internal computer network against malicious access from the outside and may also be configured to limit access to the outside from internal users.
Spam	has the meaning given in the Spam Act 2003
Telco Act	the Telecommunications Act 1997 (Cth)
Trustmark	such mark or device as the IIA determines will represent compliance with this Code and other initiatives which may complement this Code relating to e-Security
Virus	attaches itself to a program or file which is how it spreads from one computer to another. A computer virus can be spread by the sharing of infected files or the sending of e-mails with viruses as attachments. It requires people to continue the spread of the virus
Worm	is similar to a virus but can spread without the need for any human action
Zombie	a computer that has been infected with a virus or daemon that places that computer under the control of a malicious hacker without the knowledge of the owner of the computer

5.2 In the Code where examples are provided of the manner in which a Code provision may be satisfied, these examples should not be read as limiting the manner in which the provision may be satisfied.

5.3 Where documents are referred to in the Code by means of URLs, the URLs are intended for reference only and the operation of the Code will not be affected where the document referred to is subsequently relocated to another URL.

PART B – RECOMMENDED ACTIONS FOR ISPs

6. Detection, Education, Reporting

There are several activities that ISPs can undertake with the end goal of improving Internet security. The sections below provide examples of such activities. It is recommended that ISPs will undertake at least one of the items noted under each different heading, but it is recognised that each ISP will implement e-Security programs that accord with their infrastructure, network

and systems abilities, their position as a retail or wholesale ISP, their resources, customer base and so on.

6.1 Detection of Malicious activity / Compromised computers

ISPs can typically find out about malicious activity and compromised computers in two ways:

- (a) by active monitoring as part of normal network management activities; and/or
- (b) by notification by trusted third party sources. (Note that a list of sources is included in Schedule 2 to this Code.)

ISPs are encouraged to undertake one or both of the above activities to detect compromised computers on their networks.

6.2 Actions to be Taken once a compromised customer is detected

Once an ISP has detected a compromised computer or malicious activity on its network, it should take action to address the problem.

ISPs should therefore attempt to identify the end user whose computer has been compromised, and contact them to educate them about the problem.

Examples of actions that ISPs can take when they become aware of a compromised computer and have identified the relevant customer are:

- (a) Notify the customer directly (by phone or email);
- (b) Apply an 'abuse' plan where the customer's Internet service is speed throttled;
- (c) Temporarily suspend the customer's account until they advise they have taken remedial action. (Suspension could occur for customers appearing on the source lists for the first time and/or customers re-appearing on the lists);
- (d) Place the customer's account in a 'walled garden' with links to relevant software/information pages that will assist them to clean-up their computers;
- (e) Temporarily suspend compromised ports/protocol activity;
- (f) Regenerate the customer's account password to prompt customers to call the helpdesk so they can be educated about the issue;
- (g) In the case of Spam sources, apply restrictions to outbound SMTP; and/or
- (h) Provide the customer with a timeframe in which to take remedial access and if this is not adhered to, terminate their service. (Termination of a customer's service would generally only be suggested in the most extreme of cases, where the customer has refused to take action to resolve the situation, e.g. by installing anti-virus software, or where the amount of Spam being sent via the customer's

account is causing network impacts, etc.)

ISPs may choose to use one or more of the above examples, and may choose different options depending on whether it is the first time a customer's IP address has appeared on the source lists or whether they continue to appear on the lists and have taken no remedial action.

6.3 Educating customers

- (a) It is recommended that customers be notified that their computers are suspected of being compromised according to standardised notifications as set out in Schedule 1 to this Code.
- (b) Additional resources are available at www.tortoise.iaa.net.au. ISPs are encouraged to direct customers to this resource.

6.4 Reporting of malicious activity

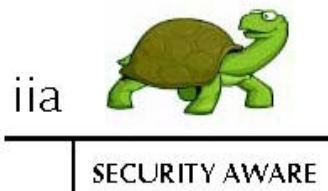
- (a) Where the ISP believes that that the nature and extent of the network compromise is of sufficient severity, the ISP should report this to the relevant agencies as set out in Schedule 3 of this Code. In the event of serious network incursions which invoke concerns about major cyber attack or major criminal activity, Schedule 3 contains a list of agencies to be notified.

7. Trustmark

- 7.1 ISPs who are compliant with this Code are entitled to use the IIA Security Friendly ISP Trustmark on their websites and other communications materials subject to such terms and conditions as the IIA shall determine.
- 7.2 The Trustmark must point to mandatory information as contained in Schedule 1 to this Code. Alternatively, the Trustmark should link to a URL provided by the IIA which contains educational materials for end users.

This page may also link to additional tools and resources as the IIA may determine from time to time.

- 7.3 Example of Trustmark



PART C - GENERAL

8. Dates of Implementation

8.1 This Code will come into effect on **xx xxx 2010**.

9. Code Review

9.1 This Code will be formally reviewed within 18 months from the date of implementation.

9.2 In reviewing this Code and in considering any proposed changes to it, the IIA will consult with ACMA and DBCDE and other government agencies as deemed appropriate.

Schedule 1 – Standardised Information for Customers

THE INFORMATION BELOW IS TO BE INCLUDED IN MANDATORY INFORMATION PROVIDED BY ISP OR ON RESOURCE CREATED BY THE IIA THAT ISPS CAN LINK TO

1. Internet security is an ongoing challenge – but it is a challenge that must be met if you are to enjoy a safer online experience. As Internet users, we are all required to play our part in promoting and practising a “culture of security”.
2. The Internet Industry Association recommends that the following steps be taken to ensure that your computer and its associated hardware is fit for connection to the Internet:
 - (a) You limit access to your computer and do not leave your Internet connection on and unprotected;
 - (b) You have installed adequate anti-virus software;
 - (c) You download updates to your anti-virus software frequently;
 - (d) You have “patched” your operating system (i.e. you have downloaded and installed the latest security updates). Examples of operating systems are: DOS, OS2, Windows, Linux, iPhone.
 - (e) You have correctly configured your router or modem according to best practice safety standards – this is not a hard process to do but a very necessary one. See below for more information;
 - (f) You have a personal firewall running on your home computer. (This could be a Microsoft Windows firewall, two-way third-party firewall software, internet security software suites, hardware firewalls or firewall features on your router or modem);
 - (g) You have disabled the “preview Pane” in Outlook to prevent you unwittingly viewing or activating a virus, worm or Trojan;
 - (h) You may opt to disable HTML for email as this can sometimes be used to transfer hidden commands via email;
 - (i) You may opt to disable ActiveX in Internet Explorer;
3. Router/Modem safety is the responsibility of the end user and below are some steps that may assist in providing you with a more secure system minimising the possibility of infection (always ensure that you refer to your manual as well):
 - (a) Use strong, secure passwords that cannot be easily guessed. Instead of using a weak password such as ***pwd1234*** or ***admin*** or something related with your

date of birth or your name, try utilising a mixture of upper and lower case letters as well as numbers (such as **A1kl3B4n9oQ2**) and making the password at least eight characters long or more;

- (b) Ensure remote connections are encrypted. For example, utilise HTTPS for web-based access instead of HTTP which transmits everything in clear text. Although this may not prevent infection, it does improve overall security.

Other suggested actions a customer could be encouraged to undertake include:

Using anti-virus and anti-spyware software and keeping it up to date. Customers can download software from ISPs or software companies or buy it. Customers need to look for anti-virus and anti-spyware software that removes or quarantines viruses and that update automatically on a daily basis.

Setting operating system software to download and install security patches automatically. Operating system companies issue security patches for flaws that they find in their systems.

Being cautious about opening any attachments or downloading files from emails they receive. Don't open an email attachment — even if it looks like it's from a known friend — unless they are expecting it or know what it contains. If they send an email with an attached file, include a text message explaining what it is.

Using a firewall to protect their computer from hacking attacks while it is connected to the Internet. A firewall is software or hardware designed to block hackers from accessing their computer. A firewall is different from anti-virus protection: while anti-virus software scans incoming communications and files for troublesome viruses, a properly-configured firewall helps make their computer invisible on the Internet and blocks all incoming communications from unauthorised sources. It's especially important to run a firewall if they have a broadband connection because the connection is always open. Most common operating system software (including Windows XP and Vista) comes with a built-in firewall, but they may not have to enable it.

Disconnecting from the Internet when there away from their computer. While anti-virus and anti-spyware software, along with a firewall, are critical protections when there connected to the Web, they're not foolproof. Hackers just can't get into their computer when it's disconnected from the Internet.

Downloading free software only from sites they know and trust. It can be appealing to download free software like games, file-sharing programs, customised toolbars, and the like. But remember that many free software applications contain other software, including spyware.

Checking their “sent items” file or “outgoing” mailbox for messages they did not intend to send. If customers do find unknown messages in their out box, it's a sign that their computer may be infected with spyware, and may be part of a botnet. This isn't foolproof: many spammers have learned to hide their unauthorized access.

Taking action immediately if their computer is infected. If their computer has been hacked or infected by a virus, disconnect from the Internet right away. Then scan their entire computer with fully updated anti-virus and anti-spyware software. Report unauthorised accesses to their ISP. If they suspect that any of their passwords have been compromised, call that company (i.e. bank) immediately to change their password.

Learning more about securing your computer at (AusCERT or its successor, IIA or ISP). These sites offer practical tips from the government and technology industry to help them be on guard against Internet fraud, secure their computer, and protect their personal information.

4. Software protection and remediation for affected computers

If you need assistance in removing malware from a infected computer please visit www.tortoise.iaa.net.au to find resources and services that can help you.

Schedule 2 – Sources of Information Relating to Compromised Computers

1. ISP Monitoring Activities

There are several ways an ISP can determine that a customer's computer is compromised via undertaking monitoring activities on their own networks. Examples are:

- a) Monitor mail queues and network traffic patterns for anomalies or known patterns of bot/malicious activity;
- b) "Ingress" AV and Spam checking;
- c) Ingress address validation (not accepting any packets from computers that have source addresses not assigned within the ISP's allocation block);
- d) Gateway IPS/IDS;
- e) Internal firewall systems;
- f) Internal systems used to identify well known trojan/viruses using well known TCP and UDP port numbers;
- g) Reports from customers.

2. ACMA Australian Internet Security Initiative (AISI)

ACMA developed the Australian Internet Security Initiative (AISI) to help address the emerging problem of 'zombie' computers. These computers become compromised through the secret installation of malicious software, such as a 'trojan', that enables the computer to be controlled remotely for illegal and harmful activities. See www.acma.gov.au/aisi

The AISI collects data on computers that are operating as zombies, analyses this data, and provides daily reports to participating Australian Internet Service Providers (ISPs) on the zombie computers operating on their networks. The ISPs then inform their customers that their computer is compromised and provide advice on how they can fix it.

The AISI is a voluntary program, with over 65 ISPs currently participating. For additional information on the AISI, visit the [ACMA website \(www.acma.gov.au/spam\)](http://www.acma.gov.au/spam).

3. Other sources of information

There are also external sources of compromises / malicious activity which an ISP may choose to use, such as:

- (a) Spamcop reports;
- (b) DNSBL reports;

- (c) AOL reports;
- (d) Hotmail reports;
- (e) SORBS reports;
- (f) RBLS (Blacklist notification subscription);
- (g) Internal Spamassassin scanning and reporting of outbound mail destined to popular Spam target domains like Hotmail, Yahoo, BigPond;
- (h) Reports from other organisations such as AusCERT, My Net Watchman, SpamCop, RoadRunner, JunkMail Filter, other ISPs and external individuals.

Schedule 3 – Agencies to be notified in event of serious attack

AustCERT or its successor

[Direct phone and email details to be added here]