COMMUNICATIONS ALLIANCE LTD

INDUSTRY CODE

C650:2014

iCode

INTERNET SERVICE PROVIDERS VOLUNTARY CODE OF PRACTICE

FOR INDUSTRY SELF-REGULATION IN THE AREA OF CYBER SECURITY

C650:2014 iCode - Internet Industry Code of Practice

First edition published by the Internet Industry Association
as Version 1.0 1 June 2010

Communications Alliance Ltd was formed in 1997 to provide a unified voice for the Australian communications industry and to lead it into the next generation of converging networks, technologies and services.

Disclaimers

1) Notwithstanding anything contained in this Industry Code:

   a) Communications Alliance disclaims responsibility (including where Communications Alliance or any of its officers, employees, agents or contractors has been negligent) for any direct or indirect loss, damage, claim, or liability any person may incur as a result of any:

      i) reliance on or compliance with this Industry Code;

      ii) inaccuracy or inappropriateness of this Industry Code; or

      iii) inconsistency of this Industry Code with any law; and

   b) Communications Alliance disclaims responsibility (including where Communications Alliance or any of its officers, employees, agents or contractors has been negligent) for ensuring compliance by any person with this Industry Code.

2) The above disclaimers will not apply to the extent they are inconsistent with any relevant legislation.

Copyright

INTRODUCTORY STATEMENT

Communications Alliance 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.

The Code recognises that everyone has a role to play in internet security and safety. Government, equipment vendors, online businesses (such as search engines), application (app) developers, Internet Service Providers (ISPs) and consumers all need to be part of the solution. This Code, however, focuses on the steps that ISPs and consumers can take to minimise the security risks inherent in using the internet.

There are measures that ISPs can take to address cyber security issues, which is why industry has developed this Code. This Code is designed to provide a consistent approach for Australian ISPs to help inform, educate and protect their customers in relation to cyber security risks and their on line safety experience.

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 codes and relevant Commonwealth, State and Territory legislation and initiatives such as Stay Smart Online.

While present security technologies have various levels of sophistication, the Communications Alliance remains committed to monitoring developments in such technologies and to keeping its members informed of these developments.

Through following the Code, it is believed ISPs can contribute to reducing the number of compromised devices in Australia and thereby contribute to the overall security of the internet for the benefit and security of Australian and international users.

Implementation of the measures contained in this Code will also benefit individual ISPs by offering the potential to:

(a) improve awareness of suspicious activity on their networks, leading to a more timely and effective response to threats;

(b) reduce service calls from customers related to security issues; and

(c) offer customers a greater level of confidence in the security of their internet connections (as a potential 'service differentiator').

TABLE OF CONTENTS

1 GENERAL

1.1 Introduction

1.1.1 This Code will be subject to relevant Commonwealth, State and Territory legislation, and industry codes, particularly the following:

(a) *Broadcasting Services Act 1992* (Cth) (BSA);

(b) *Telecommunications Act 1997* (Cth);

(c) *Telecommunications (Interception and Access) Act 1979* (Cth);

(d) *Spam Act 2003* (Cth);

(e) *Criminal Code Act 1995* (Cth) (particularly Part 10); and

(f) *Privacy Act 1988* (Cth).

1.2 Scope

1.2.1 This Code is voluntary.

1.2.2 This Code applies to Internet Service Providers (ISPs) as defined under Schedule 5 of the BSA including mobile service providers that offer access to the internet.

1.2.3 The Code does not apply to electronic commercial messaging, as dealt with via the Spam Act, unless this is also Spam as defined in this Code (i.e. bulk unsolicited email).

1.2.4 It is recognised by all in the cyber 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 to either ISPs or mobile network providers who may wish to use the Code to address the risks associated with these services being attacked in the future.

1.2.5 The cyber security measures listed in this Code are not exhaustive, or exclusive. It is envisaged that these measures will change over time, in response to the changes in the nature of malicious activity. Communications Alliance invites ISPs to recommend changes to the measures listed in this Code to best address changes in the nature of malicious activity over time, for inclusion in this Code on the next review.

1.3 Objectives

1.3.1 The aims of the Code include:

(a) Instilling cyber-security culture within Australian ISPs and their customers.

(b) Providing consistent messaging and plain language information to customers that will:

(i) raise awareness and educate them about cyber security risks;

(ii) set out simple steps that they can take to better protect themselves online; and

(iii) assist those customers whose device has been identified as possibly compromised by providing them with steps they should take to rectify the situation.

(c) Assisting those customers who experience repeated compromises to their devices and develop a strategy to minimise the effect of such compromises to other customers on the ISP's network as well as customers on other ISPs' networks.

(b) Encouraging ISPs to identify compromised devices on their networks by:

(i) participating in the Australian Communications and Media Authority (ACMA) Australian Internet Security Initiative (AISI);

(ii) actively managing and protecting their networks; and

(iii) obtaining information on compromised devices via other trusted third party sources.

(d) Encouraging ISPs to identify, communicate with each other and report any cyber security issue that may affect Australia's critical infrastructure, or that may have a national security dimension.

(e) Implementing these measures in a manner that protects the privacy of customers, consistent with relevant legislative obligations.

1.3.2 The Code provides guidance on how ISPs can:

(a) undertake network management practices to help identify abnormal traffic patterns from an IP address that may indicate that a customer's device has been compromised (See Schedule 2);

(b) take steps to respond to the AISI reports or any other trusted source of information that may relate to malicious activity (See clauses 3.1.2 and 3.1.4);

(c) inform a customer that their device may be compromised (See clause 3.1.2);

(d) educate customers on what actions they can take to protect their devices from malicious activity (See clause 3.1.3); and

(e) notify Australian authorities of a malicious activity (See Schedule 3).

The Code provides a list of resources that ISPs could access to gain intelligence on sources of attack (see Schedule 2).

1.4 Principles

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

(a) education of customers is a key element of the strategy;

(b) the Code should be technology neutral (that is, it is applicable across networks and systems and not linked to specific proprietary technologies);

(c) the requirements of this Code 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) there is a shared responsibility for internet security; end users must accept some responsibility for securing access to their devices 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 the ISP's circumstances;

(g) the Code is predicated on a recognition that compromised devices represent a threat to the integrity of networks and a threat to customer privacy and security;

(h) the privacy and protection of Personal Information of customers is a paramount concern;

(i) the Code draws upon existing industry best practices;

(j) it is recognised that some threats 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) in some cases, ISPs may be required to report instances of compromises, malicious activity or attacks to relevant law enforcement and other government agencies or provide reasonable assistance as required under the *Telecommunications Act*.

1.5 Date of Implementation

This Code will come into effect on the date of publication.

1.6 Code review

1.6.1 This Code will be formally reviewed at intervals of 5 years or earlier as required.

1.6.2 ISPs that are compliant with the Code are encouraged to track and review their internal activities undertaken to comply with this Code, in order to provide feedback to Communications Alliance on the Code requirements to assist the process of review and improvement.

2 ACRONYMS, DEFINITIONS AND INTERPRETATIONS

2.1 Acronyms

ACMA

means the Australian Communications and Media Authority.

AISI

means the Australian Internet Security Initiative.

ASD

means Australian Signals Directorate.

CERT

means Computer Emergency Response Team.

DMARC

means Domain-based Message Authentication, Reporting & Conformance.

IETF

Internet Engineering Task Force.

PIN

means Personal Identification Number.

SMTP

means Simple Mail Transfer Protocol.

WEP

means Wired Equivalent Privacy.

WPA

means Wi-Fi Protected Access.

WPA2

means Wi-Fi Protected Access 2.

WPS

means Wi-Fi Protected Setup.

2.2 Definitions

Australian Signals Directorate (ASD)

means an intelligence agency in the Australian Government Department of Defence that provides advice and assistance on information and communications security.

Bot

means a single compromised device.

NOTE: A Bot is sometimes called a zombie.

Botnet

means a network of compromised devices.

NOTE: A Botnet is sometimes called a zombie army.

CERT Australia

means the Australian national computer emergency response team.

NOTE: CERT Australia is operated by the Attorney-General's Department.

Code

means the Communications Alliance voluntary code of practice for ISPs, known as the iCode, designed to provide a consistent approach for Australian ISPs to help inform, educate and protect their customers in relation to cyber security risks.

Device

means a computer, smart phone, tablet and other computing devices connected or capable of connecting to the internet.

DKIM

means Domain Keys Identified Mail a method for associating a domain name to an email message.

Firewall

means a hardware device, software program or a combination of the two to protect a device or network from unauthorised access.

NOTE: A Firewall guards the network of a device against malicious access from outside the network. It may also be configured to limit access to outside a network by users within the network.

Ingress/Egress Address Validation

means not accepting any packets from devices that have source addresses not assigned within the ISP's allocation block.

NOTE: The IETF BCP 38 is the best current practice for ingress/egress filtering to stop spoofing (see: http://tools.ietf.org/html/bcp38).

IIA

means the Internet Industry Association, the industry body that originally developed the iCode.

NOTE: The IIA has since been dissolved, and Communications Alliance is now the industry body responsible for this code.

ISP

means Internet Service Provider, being a business or organisation that offers connectivity to the internet including related products and services.

Malware

means malicious software, designed to specifically damage or disrupt systems or devices (e.g. a virus).

Personal Information

has the meaning given by the *Privacy Act 1988* (Cth).

NOTE: The Privacy Act defines personal information as "information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion".

Phishing

describes electronic communications that masquerade as coming from a trustworthy entity in order to lure unsuspecting recipients into disclosing valuable information or installing Malware.

Personal Identification Number (PIN)

means a secret code consisting of letters and/or numbers that is used to verify the identity of an individual trying to access a computer system, network, device, bank account, etc.

Spam

means unsolicited bulk email.

NOTE: The definition of Spam used in this Code is different to that in the Spam Act. This Code does not apply to electronic commercial messaging, as dealt with via the Spam Act, unless this is also Spam as defined in this Code.

SPF

means Sender Policy Framework an email validation system designed to prevent email spam by detecting email spoofing.

Trojan

means a type of Malware which gains access to the operating system of a device, typically to steal confidential information or harm the host's device or computer system.

NOTE: Derived from the Trojan Horse story in Greek mythology because Trojan horses employ a form of "social engineering," presenting themselves as harmless, useful gifts, in order to persuade potential victims to install them on their devices.

Virus

means Malware which attaches itself to a program or file.

NOTES:

1. A Virus can be spread by users sharing infected files or sending emails with Viruses as attachments.

2. A worm is similar to a Virus but can spread without the need for any human action.

Wired Equivalent Privacy (WEP)

means an encryption protocol originally developed for wireless network security in the original IEEE 802.11 standard.

NOTE: As its name implies, WEP was designed to provide an equivalent level of security as wired networks. However, WEP has many well-known security flaws and should no longer be used as it has been superseded by WPA and subsequently the most recent and recommended WPA2 standard.

Wi-Fi Protected Access (WPA)

means an interim security enhancement for wireless networks, introduced to replace WEP, while the IEEE 802.11i wireless security standard was being further developed.

Wi-Fi Protected Access II (WPA2)

has the meaning given by IEEE 802.11.

NOTE: As at the end of 2013, WPA2 is the most recent and recommended wireless security standard, as it includes the Advanced Encryption Standard (AES) which was not available in WPA.

Wi-Fi Protected Setup (WPS)

means Wi-Fi Protected Setup is a feature established to assist end users in the easy setup of a secure wireless home network.

NOTE: It is recommended that you turn-off the WPS feature after setup in order to protect your modem/router's WPS PIN and WPA2 password from unauthorised access.

2.3 Interpretations

In the Code, unless the contrary appears:

(a) headings are for convenience only and do not affect interpretation;

(b) a reference to a statute, ordinance, code or other law includes regulations and other instruments under it and consolidations, amendments, re-enactments or replacements of any of them;

(c) words in the singular includes the plural and vice versa;

(d) words importing persons include a body whether corporate, politic or otherwise;

(e) where a word or phrase is defined, its other grammatical forms have a corresponding meaning;

(f) mentioning anything after include, includes or including does not limit what else might be included;

(g) words and expressions which are not defined have the meanings given to them in the Act;

(h) a reference to a person includes a reference to the person's executors, administrators, successors, agents, assignees and novatees; and

(i) 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.

3 RECOMMENDED ACTIONS FOR ISPS

3.1 Education, Detection, Action, Reporting

In order to comply with this Code, ISPs must undertake at least one of the items noted under each of the headings within this Part of the Code – Education, Detection, Action and Reporting – except where otherwise specified in this Part B. It is recognised that each ISP will implement cyber security programs that accord with their infrastructure, network and systems capabilities, their position as a retail or wholesale ISP, their resources, policies, contractual arrangements, customer base and so on.

3.1.1 **Educating customers**

(a) **Objective**: to reduce incidence of security violations due to customer behaviour.

(b) It is recommended that customers should be provided with information, or links to information, which provides them with simple steps they can take to better protect themselves online. ISPs should consider providing this information both to new customers and also to existing customers when the need or opportunity arises. For example, information could be provided:

(i) to new customers in their 'welcome' information;

(ii) when new online accounts are created;

(iii) to existing customers via articles in newsletters or updates on the provider's website;

(iv) to customers who call to discuss security concerns; and.

(v) on occasions when the ISP may contact a customer to deal with a security issue identified in relation to that customer's service or device.

ISPs can comply by providing such information to their customers (e.g. on their website) and/or by providing links to such information on the Communications Alliance cyber security pages at http://www.commsalliance.com.au/Activities/ispi and the Government's cyber security website Stay Smart Online www.staysmartonline.gov.au.

(c) An example of the information referred to in clause 3.1.1(b) is included at Schedule 1.

(d) Where ISPs have not contacted customers with compromised devices before taking action as referred to in clauses 3.1.3(b) and (c) below, ISPs should have previously informed their customers under the terms and conditions on which they supply the service:

(i) that the ISP may take action to address compromises without first contacting customers; and

(ii) what those actions may be.

ISPs may choose the appropriate method by which to inform their customers. This could be, for example, via their website (including via the page referred to in clause 3.1.1(b) above); via a message on a bill; by email or newsletter; in the customer contract; or by specifying the details as part of the process by which the security incident is being managed by the ISP. If a customer's device is compromised the ISP will carefully manage communications to the customer regarding this issue to:

(a) ensure that the customer is certain that the communication is made by the customer's ISP;

(b) communicate to the customer the action or activity that may have caused the compromise of the device; and

(c) direct the customer to online resources that may assist the customer to prevent further successful attacks.

3.1.2 **Detection of compromised devices and other malicious activity**

(a) **Objective**: increase awareness of and minimise malicious activity. ISPs are strongly encouraged to find out about malicious activity and compromised devices in the following ways:

(i) by participating in the AISI and receiving the free reports provided under this program;

(ii) by undertaking network management practices to help identify abnormal traffic patterns from an IP address that may indicate that a customer's device has been compromised; and

(iii) by notification by trusted third party sources. (A sample list of sources is included in Schedule 2 of this Code).

(b) ISPs can help prevent the delivery of fraudulent messages by implementing Domain-based Message Authentication, Reporting & Conformance (DMARC, described at www.dmarc.org) to standardise email authentication using SPF and DKIM mechanisms.

(c) ISPs can help protect their networks and customers devices connected to their networks by implementing appropriate security strategies, which can be referenced from a

number of trusted sources. Examples of information available to ISPs can be found at Schedule 2 of this Code.

3.1.3 **Actions to be taken in respect to compromised devices**

(a) **Objective**: to optimise the response by ISPs to information regarding a compromised device on a network.

(b) Should an ISP become aware of a compromised device on its network, for the protection of its customers and its network integrity it is recommended the ISP take action to address the problem.

(c) Actions that ISPs can take when they become aware of a compromised device include, for example:

(i) contacting the customer directly (by phone, email, SMS or other means);

(ii) regenerating the customer's account password to prompt customers to call the ISP's helpdesk so they can be directed to resources to assist them to deal with the compromise;

(iii) applying an 'abuse' plan where the customer's internet service is temporarily speed throttled while the issue associated with the compromised device is addressed;

(iv) temporarily quarantining the customer's service, for example by holding them within a 'walled garden' with links to relevant resources that will assist them until they are able to restore the security of their device or to require the customer to acknowledge the compromise before they can connect to the internet;

(v) in the case of spam sources, applying restrictions to outbound email (SMTP); and/or

(vi) such other measures as determined by the ISP consistent with their terms of service.

ISPs may choose to take one or more of the above actions, and may choose different options depending on whether it is the first time a customer's IP address has appeared on the source lists (see Schedule 2.4 of this Code for examples of source lists) or whether they continue to appear on the lists and seem to have taken no remedial action.

ISPs that are Code compliant will maintain systems and procedures that aim to:

(a) contact its customers if the ISP becomes aware that a customer's device is likely to have been compromised;

(b) contact CERT Australia or the AISI if deemed necessary in accordance with Schedule 3 of this Code, if it becomes

aware that a device or network associated with a third party may have been compromised;

(c) upon customer's request, provide assistance to a customer whose device or network has been compromised or whose device or network has been compromised repeatedly using the ISPs own resources or by referring the customer to the Standardised Information for Customers in Schedule 1 of this Code; and

(d) upon customer's request, after any instance of compromise confirm that the customer was satisfied with the assistance provided and encourage the customer to review and consider the Standardised Information for Customers in Schedule 1 of this Code.

If the customer is unable to address the problem through the above actions, then the ISP should direct them to further information or technical support, which may be at the cost of the customer and may require the customer to seek assistance from a third party organisation.

3.1.4 **Reporting of malicious activity**

(a) **Objective**: to optimise shared information and guided response for each security incident.

(b) Where the ISP believes that the nature and extent of suspicious or malicious activity against its network may constitute a significant cyber security incident, the ISP should report the matter to the relevant government agencies as set out in Schedule 3 of this Code.

(c) In general terms, suspicious or malicious activity that could be reported to government agencies, includes, but is not limited to, activity that:

(i) is novel or not previously seen by the ISP; or

(ii) impacts well beyond the capacity of private enterprise to manage; or

(iii) involves serious malicious intent; and

(iv) involves serious threats to Australian telecommunications networks or other critical infrastructure.

4 REFERENCES

Publication	Title
Legislation	
Broadcasting Services Act 1992 (Cth) (BSA)	
Telecommunications Act 1997 (Cth)	
Telecommunications (Interception and Access) Act 1979 (Cth)	
Spam Act 2003	
Criminal Code Act 1995 (Cth) (particularly Part 10)	
Privacy Act 1988 (Cth)	
Industry Guidelines	
IETF BCP38	Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing http://tools.ietf.org/html/bcp38
IETF RFC6561	Recommendations for the Remediation of Bots in ISP Networks http://datatracker.ietf.org/doc/rfc6561/
IEEE 802.11™-2012	IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications http://standards.ieee.org/about/get/802/802.11.html

SCHEDULE 1 – STANDARDISED INFORMATION FOR CUSTOMERS

THE INFORMATION BELOW IS AN EXAMPLE OF THE TYPE OF INFORMATION THAT SHOULD BE INCLUDED IN INFORMATION PROVIDED TO CUSTOMERS BY THE ISP OR ON A RESOURCE CREATED BY COMMUNICATIONS ALLIANCE (THAT ISPs CAN LINK TO)

1. Internet security is an ongoing challenge and we are all required to play our part. As an internet user, there are steps you can take to protect yourself online and ensure your actions do not inadvertently impact others. This includes protecting any devices you use which connect to the internet (such as your computers, mobile phones and tablets) and also thinking carefully about what you do online (e.g. whether the links you click on are to legitimate websites, whether the sites you give financial information to are secure).

2. Communications Alliance recommends the following tips to help ensure that your device stays adequately protected for a safer and more secure online experience:

(a) **Take action immediately if you suspect your device 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.

(b) **Keep your anti-virus and other security software updated**.

(c) **Install a Firewall** and enable the security features with a strong password to prevent unauthorised access to your devices.

(d) **Turn on automatic updates for relevant security software** so that it can automatically receive the latest fixes and updates.

(e) **Use a strong password and change it regularly.** (Note: most websites or programs will have rules about what type of password you can use. Try to make it as strong as possible within that site or program's parameters, for example by using a combination of uppercase and lowercase letter, numerals and other characters. Don't use a password that would be easy for someone to guess if they had access to your personal information, e.g. if they'd stolen your wallet or could see the information on your Facebook page.)

Also try to use unique passwords for as many services as possible. Re-using passwords across multiple services carries a risk, as if the password is compromised on one service, access to your other accounts that use the same password could also be compromised. There are Password Manager Services available to help deal with having to remember multiple unique passwords.

The Australian Signals Directorate (ASD), an intelligence agency in the Australian Government Department of Defence, provides information on its top security tips for the home user (including passwords) at http://www.asd.gov.au/publications/csocprotect/home_computer_security.htm

(f) **Stop and think before you open emails or click on links or attachments contained in them.** Don't open suspicious emails or attachments from unknown sources. Don't click on links in emails requesting your personal

details – legitimate companies will generally not ask for your personal details via an email.

Also think carefully about the emails you are opening. Sometimes an email that appears to be from someone you know may just be the result of that person having a virus which is using their email address to send out spam or infect more devices with the virus. Pay close attention to the following:

- Is the sender address indicated in the "from" field an address the recipient recognises or would use?
- Is the text of the email unusually short or unlike the language or grammar the sender would commonly use or the recipient would recognise or are there spelling mistakes?
- Is the real subject of the email concealed until you click a link?

If the email has any of these features or it doesn't look like something the person would normally send you, think about contacting them via an alternate means to check if they really did send it to you.

(g) **Check your "sent items" file or "outgoing" email.** If you find unknown messages in your out box, it is a sign that your device may be infected with malware. (Note that this isn't foolproof: many spammers have learned to hide their unauthorised access and so this is not the only way to check if you have a virus.)

(h) **Stop and think before you share any personal or financial information** about yourself, your friends or family online. For example, letting your friends know on Facebook about your upcoming holidays and the dates you'll be away may seem like a good idea, but if other people can see that information they can tell when your home will be vacant for a period of time and use that for their own purposes.

It's important to understand the privacy and security settings on your social media services, that way you can restrict the information about things like your upcoming holidays only to people you trust, rather than to everyone you're "friends" with on social media.

(i) **Configure your wireless network securely**. If you are using a wireless router/modem, enable the security features with a strong password and use Wi-Fi Protected Access version 2 (WPA2) encryption on your Wi-Fi equipment (WPA and WEP are older standards and less secure. WEP in particular poses a larger security risk.). If your wireless router/modem has the Wi-Fi Protected Setup (WPS) feature, it's recommended that you turn-off the WPS feature after setup in order to protect your WPS PIN and router's WPA2 password from unauthorised access. Refer to your router/modem manual or contact your ISP for further details.

(j) **Know what your children are doing online.** Make sure they know how to stay safe and encourage them to report anything suspicious. Understand how to avoid scams online. Consider implementing Phishing protection and optional content filtering on your home network or device. For further information about online safety go to the Australian Government's Cybersafety website at http://www.cybersmart.gov.au.

3. More Information and tools for ongoing security

Learn more about securing your device at http://www.commsalliance.com.au/Activities/ispi. This site offers practical tips from the internet industry to help safeguard against Internet fraud, 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:

(a) The Australian Government's cyber security website www.staysmartonline.gov.au

(b) The Stay Smart Online email alert service.

(c) An annual National Cyber Security Awareness Week.

(d) The Budd:e cyber security education package for Australian schools. The Package consists of two self-learning, interactive modules, one for year primary and one for secondary students. The modules are available online http://www.staysmartonline.gov.au/school or on compact disc which can be ordered online.

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

The ACMA 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.

NOTE: Terms capitalised and acronyms or terminology used in this Code are as defined in the Code or have the meaning as shown in Section 2 of this Code. This Schedule 1 or other Schedules should not be removed from the Code without providing reference to the meanings defined in the Code.

SCHEDULE 2 – SOURCES OF INFORMATION FOR ISPS RELATING TO COMPROMISED DEVICES

1. ISP Network Management Activities

It is recommended that ISPs use current best practice standards and resources in determining whether a customer's device is compromised. Examples include, but are not limited to:

(a) review mail queues and network traffic patterns for anomalies or known patterns of Bot/malicious activity;

(b) "ingress" and "egress" address validation and spam checking;

(c) gateway IPS/IDS (Intrusion Prevention System/Intrusion Detection System);

(d) internal Firewall systems;

(e) internal systems used to identify well known Trojans/viruses using well known TCP and UDP port numbers; and

(f) reports from customers.

2. The ACMA Australian Internet Security Initiative (AISI)

The ACMA developed the Australian Internet Security Initiative (AISI) to help address the problem of Botnets, which are a network of malware infected devices, or Bots. These devices become compromised through the secret installation of malicious software, such as a Trojan, that enables the device to be controlled remotely for illegal and harmful activities.

The AISI collects data on computing devices that are operating as bots, analyses this data, and provides daily reports to AISI participants (predominantly ISPs and universities) identifying bots operating on their networks. AISI participants are expected to then inform their customers that their device is compromised and provide advice on how they can disinfect it.

As of August 2012, approximately 98% of allocated Australian IP address ranges are covered by AISI participants. For additional information on the AISI, visit the ACMA's website at www.acma.gov.au/aisi.

3. CERT Australia

CERT Australia is Australia's national computer emergency response team. It is Australia's initial point of contact for cyber security threats or incidents impacting upon Australian networks. CERT Australia is managed by the Australian Government Attorney-General's Department.

CERT Australia provides Australian ISPs with access to information on cyber security threats and vulnerabilities and how to better protect their security and that of their customers. CERT Australia assists with the correlation of seemingly isolated incidents for the early identification of potentially significant cyber security incidents. It also has a central role in the Government's response to significant cyber security incidents in the Australian private sector.

Further information can be found at https://www.cert.gov.au/.

4. Other sources of information

There are also other sources of information available on compromises / malicious activity and security initiatives which an ISP may choose to reference and/or use, such as:

(a) Spamcop reports;

(b) Domain Name System Blackhole List (DNSBL) reports;

(c) Domain Name System (DNS) security which can be found on the ASD website at http://www.asd.gov.au/publications/csocprotect/dns_security.htm

(d) America Online (AOL) reports;

(e) Hotmail reports;

(f) Spam and Open Relay Blocking System (SORBS) reports;

(g) Real-time Blacklist notification subscription (RBLS);

(h) Internal Spamassassin scanning and reporting of outbound mail destined to popular spam target domains like Hotmail, Yahoo, BigPond;

(i) Reports from other organisations such as CERT Australia, My Net Watchman, SpamCop, RoadRunner, JunkMail Filter, other ISPs and external individuals;

(j) The Internet Engineering Task Force (IETF) document RFC6561: *Recommendations for the Remediation of Bots in ISP Networks* March 2012 (see http://datatracker.ietf.org/doc/rfc6561/); and

(k) Phishing reports from http://www.fraudwatchinternational.com/phishing-alerts.

SCHEDULE 3 – NOTIFICATION TO GOVERNMENT AGENCIES

A cyber security incident involving unauthorised access to or impairment of electronic communications, for example a denial of service attack, will constitute an offence under the Commonwealth *Criminal Code Act 1995* and/or State and Territory criminal laws.

Law Enforcement

Where an ISP suspects that criminal activity has occurred against their infrastructure or customers, or that their customers are involved in criminal activity, the ISP should report the matter to the relevant State or Territory police.

Where an ISP suspects that criminal activity has occurred against national critical infrastructure, the ISP should report the matter to the Australian Federal Police. Such incidents might include, but are not limited to, attacks that significantly compromise the integrity of: Australia's financial system; the control systems used by electricity, water and other infrastructure; telecommunications networks or the Internet infrastructure (such as the domain name system).

The Australian Federal Police can be contacted at:
Phone: (02) 6126 7133
Fax: (02) 6126 7900
Email: AOCC-Client-Liaison@afp.gov.au

Regardless of whether law enforcement indicates the matter will be pursued by them or not, CERT Australia should also be given visibility of the issue, as described below.

CERT Australia

ISPs should report any **significant** cyber security incident to CERT Australia, irrespective of whether criminal activity is suspected or not. If an ISP has also reported an incident to a law enforcement agency, the ISP should (to the extent permitted by law) include all information provided by the agency (such as incident or call numbers) when notifying CERT Australia. Ensuring that CERT Australia is aware of such incidents will:

(a) help build broad situational awareness of cyber threats to Australian systems that CERT Australia can share with ISPs;

(b) provide early warning of specific threats that CERT Australia can then disseminate to all ISPs;

(c) provide information that CERT Australia and other Australian Government agencies can use to help ISPs and the Internet community mitigate potential attacks; and

(d) assist CERT Australia to coordinate Australia's response to cyber security incidents of national significance.

As well as giving CERT Australia visibility of significant cyber security incidents, ISPs are encouraged to also provide periodic information about threats and attacks on their networks. This aggregated and de-identified information, in conjunction with information from other sources, will help the Australian Government develop and maintain a broad picture of the threat to the Australian cyber environment.

CERT Australia is able to facilitate requests from Australian ISPs for Australian Government assistance in responding to cyber security incidents on a case by case basis. CERT Australia can assist by:

(a) engaging with other Australian organisations and International CERTs to facilitate requests to 'takedown' malicious websites or the blocking of overseas based internet addresses;

(b) providing general alerts and advisories on an incident; or

(c) facilitating targeted advice and assistance from other Government agencies or international partners.

Any direct assistance provided by CERT Australia would not normally involve technical advice or services that are readily available from specialist IT security firms or elsewhere in the private sector. ISPs should therefore consider whether they may need to access such services during an incident and develop contingency arrangements accordingly.

ISPs seeking Australian Government assistance in responding to a significant cyber security incident should make this request through CERT Australia.

If urgent or an emergency, CERT Australia can be contacted at the CERT Australia Hotline on:

1300 172 499 (24-hour hotline)

Otherwise please email CERT Australia at info@cert.gov.au

Email and phone are monitored twenty four hours, seven days a week.

Communications Alliance was formed in 1997 to provide a unified voice for the Australian communications industry and to lead it into the next generation of converging networks, technologies and services.

In pursuing its goals, Communications Alliance offers a forum for the industry to make coherent and constructive contributions to policy development and debate.

Communications Alliance seeks to facilitate open, effective and ethical competition between service providers while ensuring efficient, safe operation of networks, the provision of innovative services and the enhancement of consumer outcomes.

It is committed to the achievement of the policy objective of the *Telecommunications Act 1997* - the greatest practicable use of industry self-regulation without imposing undue financial and administrative burdens on industry.

Published by:
COMMUNICATIONS
ALLIANCE LTD

Level 12
75 Miller Street
North Sydney
NSW 2060 Australia

Correspondence
PO Box 444
Milsons Point
NSW 1565

T 61 2 9959 9111
F 61 2 9954 6136
E info@commsalliance.com.au
www.commsalliance.com.au
ABN 56 078 026 507

Care should be taken to ensure the material used is from the current version of the Standard or Industry Code and that it is updated whenever the Standard or Code is amended or revised. The number and date of the Standard or Code should therefore be clearly identified. If in doubt please contact Communications Alliance