International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1207

(04/2008)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Telecommunication security

Guidelines for telecommunication service providers for addressing the risk of spyware and potentially unwanted software

Recommendation ITU-T X.1207

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	
Services and facilities	X.1–X.19
Interfaces	X.20–X.49
Transmission, signalling and switching	X.50–X.89
Network aspects	X.90–X.149
Maintenance	X.150–X.179
Administrative arrangements	X.180–X.199
OPEN SYSTEMS INTERCONNECTION	
Model and notation	X.200–X.209
Service definitions	X.210–X.219
Connection-mode protocol specifications	X.220–X.229
Connectionless-mode protocol specifications	X.230–X.239
PICS proformas	X.240–X.259
Protocol Identification	X.260–X.269
Security Protocols	X.270–X.279
Layer Managed Objects	X.280–X.289
Conformance testing	X.290–X.299
INTERWORKING BETWEEN NETWORKS	
General	X.300–X.349
Satellite data transmission systems	X.350–X.369
IP-based networks	X.370–X.379
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	
Networking	X.600–X.629
Efficiency	X.630–X.639
Quality of service	X.640–X.649
Naming, Addressing and Registration	X.650–X.679
Abstract Syntax Notation One (ASN.1)	X.680–X.699
OSI MANAGEMENT	
Systems Management framework and architecture	X.700–X.709
Management Communication Service and Protocol	X.710–X.719
Structure of Management Information	X.720–X.729
Management functions and ODMA functions	X.730–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	
Commitment, Concurrency and Recovery	X.850–X.859
Transaction processing	X.860–X.879
Remote operations	X.880–X.889
Generic applications of ASN.1	X.890–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
TELECOMMUNICATION SECURITY	**X.1000–**

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1207

Guidelines for telecommunication service providers for addressing the risk of spyware and potentially unwanted software

Summary

Recommendation ITU-T X.1207 provides guidelines for telecommunication service providers (TSPs) for addressing the risks of spyware and potentially unwanted software. This Recommendation promotes best practices around principles of clear notices and user's consents and controls for TSP web hosting services. This Recommendation develops and promotes best practices to users on personal computer (PC) security, including use of anti-spyware, anti-virus, personal firewall and security software updates on client systems.

Source

Recommendation ITU-T X.1207 was approved on 18 April 2008 by ITU-T Study Group 17 (2005-2008) under the WTSA Resolution 1 procedure.

Keywords

Deceptive software, internet safety, potentially unwanted software, spyware.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

Recommendation ITU-T X.1207

Guidelines for telecommunication service providers for addressing the risk of spyware and potentially unwanted software

1 Scope

This Recommendation forms part of the set of guidance developed in ITU-T to improve the state of cybersecurity. It covers the baseline safety and security practices requirements for the telecommunication service providers (TSPs) and end-users, focusing on addressing the issue of spyware and other potentially unwanted software, which may be malicious and/or deceptive. Telecommunication service providers (TSPs), in the context of this Recommendation, refers to TSPs that are providing internet-related services, in particular, web hosting services to business organizations and internet access to end-users.

2 References

None.

3 Definitions

The term spyware has been used loosely to include numerous forms of software that exhibit certain privacy-intrusive behaviours that are uncalled for by the end-users. To ensure consistent use of the term and a common understanding, a working definition of spyware and related deceptive software is therefore provided here.

3.1 deceptive software: Software which performs activities on a user's computer without: 1) first notifying the user as to exactly what the software will do on the user's computer; or 2) asking the user whether he consents to the software doing these things. Examples of deceptive software include programs which hijack user configurations, or programs which cause endless pop-up advertisements which cannot be easily clicked out of by the user.

3.2 potentially unwanted software: Potentially unwanted software refers to various forms of deceptive software, including malicious software such as viruses, worms and trojans, and non-malicious software that exhibit the characteristics of deceptive software and spyware.

3.3 spyware: Spyware is defined in this Recommendation as a particular type of deceptive software that collects personal information from a user's computer. The personal information may include matters such as websites most frequently visited or more sensitive information such as passwords.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CERT	Computer Emergency Response Team
CIRT	Computer Incident Response Team
ICT	Information and Communication Technology
ISMS	Information Security Management System
ISMS-T	Information Security Management System – Requirements for Telecommunications
ISV	Independent Software Vendor

SQL	Structured Query Language
TSP	Telecommunication Service Provider
URI	Uniform Resource Identifier

5 Conventions

None.

6 Overview

The proliferation of the Internet has enabled new businesses and brought about many benefits to consumers at home and in the workplace. With the inherent openness of the Internet, and the interconnectivity and speed of access that it provides, it has also grown to be an effective platform for businesses' and consumers' communications, as well as mass commercial marketing purposes. In recent years, this openness and ease of communication and connectivity have increasingly being exploited by cyber criminals and rogue businesses through the use of various forms of malicious software for financial gains and other criminal purposes.

One of the safety and security challenges that are growing in significance is that of spyware and deceptive software, which are capable of compromising personal information, causing significant lost of productivity and undermining end-users' confidence and trust in legitimate businesses on the Internet.

Telecommunication service providers (TSPs) are often looked up to by various parties, in particular, regulators and enterprise customers, to provide safe and secure Internet services to the end-users (including consumers and enterprise users). When websites hosted in TSP networks and found to be hosting malicious contents, including spyware or deceptive software, and affecting the safety and security of end-user computer systems, TSPs are looked upon for assistance to address the issues, and any prolonged or frequent recurrences of such incidents would impact the trust and confidence of the TSP in providing safe and secure services. This would translate into customer dissatisfaction and result in migration of customers to other TSPs.

From a regulatory perspective, regulators in many countries are increasingly demanding assurances from TSPs of the security and safety measures they have taken, and requesting TSPs to do more in assisting consumers and end-users in safe and secure Internet computing.

In view of these changes in the Internet safety and security landscape, it is important for TSPs to adopt a set of standards of best practices that could be recognized across the industry as a minimum baseline[1] that would ensure the safe and secure provision of Internet services hosted through the TSP and also promote relevant practices to the end-users subscribing to their networks. Implementation of the baseline standard will also allow TSPs to demonstrate to regulators and end-users its conformance to industry best practices and to enhance, if not maintain, regulators' and end-users' confidence and trust over the safety and security of the TSP network and services.

[1] There is currently no such baseline, and this guideline Recommendation is a step towards providing such a minimum baseline.

7 Objectives

The objectives of this Recommendation are to:

1) Promote best practices around the principles of clear notices, user consents and user controls for web hosting services; and

2) Promote security best practices (via telecommunication service providers) to home users on safe and secure use of personal computers and the Internet, including the use of anti-virus, anti-spyware, personal firewall and automated security updates.

8 Deceptive software and spyware

The common element, shared by all deceptive software programs (including spyware), that distinguish them from legitimate applications is their lack of notice and choice at the user level. Importantly, it is commonly noted that with proper disclosure, user authorization and control, many of the software tasks performed by deceptive software/spyware, can provide benefits to users. For example, such programs may facilitate personalization, enable user-approved configuration changes and deliver approved advertising which in turn can subsidize the cost of a highly-valued service such as e-mail. In short, deceptive software is not predominantly a technology problem but largely a problem arising from deceptive or fraudulent behaviour.

At both a global and a local level, deceptive software and spyware has become one of the top-tier issues for government, industry and consumers in that they go beyond the parameters of an 'ICT policy' issue. While deceptive software obviously uses the Internet and the computer as its medium, it is fundamentally a consumer protection problem that stems from deceptive behaviour.

9 Why deceptive software and spyware matter

At the consumer level, such software degrades the computing and/or online experience of the user (sometimes to the point of rendering the computer unusable) and creates a sense of frustration and a perception that the user is not "in control". It is not an exaggeration to suggest that at the residential consumer level in particular there is a significant proportion of users for whom deceptive software threatens to completely undermine the extraordinary benefits available from the Internet and from computing *per se*.

While deceptive software is clearly having a substantial impact on consumers it is also a major problem for many ICT companies. At one level, many customers misattribute their computer operating problems to software manufacturers and developers, which detracts from their reputation and customer perceptions of their products. Clearly, problems arising from deceptive software also result in millions of dollars being spent on unnecessary support calls in both software and hardware sectors.

As noted in clause 6 above, TSPs are not spared from dealing with the challenges due to spyware and deceptive software, due to their hosting of websites that may be used directly by rogue businesses and cyber criminals to host them directly, and their subscribers experiencing the adverse impact directly, and hence calling on the TSP for support and assistance. On top of that, it is a common expectation of regulators and end-users that TSPs implement adequate safety and security measures that counter such problems. When TSPs relinquish the responsibility to deal with such challenges, their reputation and end-users' confidence and trust would naturally be undermined.

10 Recommendations

The most effective way to confront spyware is likely to involve a combination of multiple strategies involving the various stakeholders:

- industry best practices with collaboration of all key players to identify and address spyware and other unwanted software;
- broad consumer education, providing a trusted resource for how to remove and avoid spyware and other unwanted software;
- innovative technology solutions to help protect users from spyware and other potentially unwanted software, and to stay current against exploitation; and
- legislation and enforcement by government, with assistance from industry, to discourage the development of deceptive software and spyware.

This guideline focuses on providing industry best practices and broad consumer educations to assist TSPs in playing an active role in countering the deceptive software and spyware challenges.

11 Guidance for telecommunication service providers (TSPs)

To help address the issues of deceptive software and spyware, this guideline focuses on three main areas: namely, the internal security management of the TSP organization itself; security requirements that TSPs should specify for their web-hosting customers to implement; and security guidance useful for end-users (or subscribers) of Internet access services. The recommendations are structured into three respective sub-sections as follows:

a) Manage information security risk in the business.

b) Safety and security requirements for web hosting services.

c) Safety and security guidance for end-users.

11.1 Manage information security risk in the business

11.1.1 Information security management system

At the enterprise level, there should be a formal information security management system implemented to identify and manage related information security risk to the TSP business. [b-ITU-T X.1051] provides the required guidance and best practices for implementing such a system.

A key consideration for TSPs in implementing ISMS-T is to ensure that the TSP as an enterprise organization has a system to continuously identify, assess, treat and manage information security risk relating to its provision of services on the Internet, directly to end-users/subscribers, and indirectly via web hosting services to customers.

Through the ISMS-T continuous risk management processes, a TSP will gain visibility of its risk profile and be enabled to demonstrate to regulators and other interested parties the security of its network and services.

A TSP may also consider the formal certification of its compliance with the ISMS-T recommendations, under the ISO/IEC 27001 certification scheme.

As part of the implementation of ISMS-T or relevant information security management system, TSPs should also establish a security incident monitoring and response capability, and coordinate their incident response activities with external computer incident response team (CIRT) or computer emergency response team (CERT) organizations in the country. The incident and emergency response provision should include monitoring and assessing the security status of end-users and hosted websites on the TSP networks, and provide guidance to assist the affected parties in responding to security incidents effectively.

11.1.2 Provide safe and secure products

Some TSPs may develop[2] and release their own web browser toolbars, diallers or code of any kind to provide end-users value-added services or facilitate ease of access to Internet services. In such instance, there should be proper end-user agreement incorporating suitable language and statements about the TSPs coding policy, privacy policy and means whereby users may change their acceptance later or escalate any issues they might have regarding the policy and practices. When such agreement is used, TSPs should make sure that end-users sign and version it consistently.

TSPs should also document the code behaviour and make assessment as to whether their behaviour may fall into any potential areas that might be considered spyware or deceptive software. In the latter case, they should then engage a suitably qualified assessor to evaluate whether the code may fall within any anti-spyware vendor's objective criteria and adhere to the best practices so that TSP-provided software tools for the end-users would not be labelled as spyware/adware by the anti-spyware vendors. Many anti-spyware vendors publish the criteria by which they rate software.[3]

TSPs should implement digital code signing for their binaries so that anti-spyware vendors could easily determine the owner of a file, and independent software vendors (ISVs) who consistently produce software that follows best practices would be categorized as being likely safe even prior to analysis.

Should TSPs discover useful software techniques that could help reduce the spyware problem, TSPs should consider partnering and working with the vendor to make them broadly available.

11.1.3 Network monitoring and response

Network monitoring is common amongst TSPs to ensure reliability and quality of network services. At the same time, this capability can be leveraged to look for exceptional network traffic conditions and detect malicious activities emerging on the network. In general, TSPs should perform the following:

- Understand the traffic on the network – what is normal, what is not normal.
- Use network management tools to identify spikes in traffic, "unusual" traffic/ports and ensure that there are tools available to pinpoint and respond to the cause.
- Test the response capability before they are needed for an actual event. Refine the response techniques, processes and tools based on the result of regular drills.
- Understand the constituents on an individual basis – if someone who is normally an inactive user suddenly starts to use 100 percent of its available bandwidth, maybe they need to be isolated until the reason can be found. Network isolation can prevent the spread of malicious software (malware) though some implementations may require user consent or updates to the terms of service.

11.1.4 Support and escalation

TSPs normally have a support service to answer customers' queries and provide technical assistance and support to address end-users' problems. With the escalation of malware on the Internet, TSPs will receive reports relating to malware and spyware infections and issues. Such information is important and useful for relevant vendors to risk assess the malware situation and provide updates to necessary tools to ensure that any new malware or spyware detected can be removed or disabled effectively. In this regard, TSPs should establish contact with security vendors and submit relevant reports and malware samples to the vendors for follow-up, particularly if there appears to be a spike

---

[2] Either internally or through a third party provider.

[3] The AntiSpyware Coalition, which represents multiple industry players, also has a set of definitions and criteria published at their website. For more information, see Appendix I.

in prevalence. Most vendors maintain an e-mail list for receiving such report/samples for analysis and following. For example, see Table I.1.

11.1.5 Keeping up-to-date with latest developments

As part of the ISMS-T implementation to manage the enterprise information security risk, and also ensure that TSPs continue to follow industry best practices and keep pace with the latest vulnerabilities and exploits/attacks situation, TSPs should participate in relevant community or industry forums to share their best practices and learn from fellow providers.

NOTE – For more information, see Appendix I.

11.2 Safety and security requirements for web hosting services

Most TSPs provide web hosting services on their networks and data centres as part of their business services. These services will reach the end-user/consumers and/or small businesses when they are re-packaged by the web hosting subscribers and re-sold to the end-users. Should the web hosting subscribers set up an insecure server, or host malicious content in their websites, the safety and security of the end-users will be adversely affected. As such, it is important for TSPs to establish a minimum safety and security best practices standard for the web-hosting subscribers to comply with as part of the terms of agreement.

The terms of agreement should cover the following:

a) Clear notices, describing the website security and privacy practices, data collection practices and the behaviour of any code (e.g., browser helper object) that the website may distribute and execute in the end-users' desktop or web browser environment.

b) User consent, facilitating users' agreement or disagreement with the terms of services described in the notices. This would allow users to exercise discretion and determine whether they can accept the terms of services accordingly.

c) User controls, facilitating users to change their settings or otherwise terminate their acceptance any time in the future after the initial agreement.

The terms are important to ensure that the end-users are clear about the behaviour and practices of the website in relation to the end-users' safety, privacy and security. The terms should be developed with the aid of a legal professional to ensure that they will also indemnify the TSP from potential legal charges from end-users as a result of specific losses or harm incurred due to malicious contents or unclear policies and practices on the website.

In addition to the data protection and personal privacy and safety provisions on the website, TSPs should require websites hosted on their network to implement a set of best practices security measures at the application level before they could go live. This should include, but not be limited to, the following:

a) Guidance for secure website development and web page coding practices, including:

   i) Display of short privacy notices, which provide a clear, concise one-page summary (in layman's terms) of the company's essential online privacy practices. With this, users are able to make more informed choices about sharing their information online. The short notices should conform to all regulatory requirements and provide links to full legal statements and other relevant information, so customers who want more detail can easily click through to read the longer version. With a single notice, customers can have a more consistent experience across all of the company's properties, with the same privacy standards and expectations extended to many sites.

   ii) Secure handling of cookies.

iii) Secure input validation and handling to prevent common attack such as SQL injection. Based on the fact that increasingly frequented websites are used for malicious code distribution, input and output validations have to be carried out by active content as well as by dynamic content.

iv) Secure web page scripting to prevent common attack such as cross-site scripting.

v) Code security review and testing.

As part of TSP web hosting infrastructure, the following security measures should also be undertaken to protect the web servers against unauthorized access, and compromised to host malicious contents such as deceptive software and spyware:

b) Configure the web server, including underlying operating systems in accordance with a baseline security configuration guide. This should include proper definition of web-server users versus administrators, enforce access controls on program and systems directories and files, and enabling of audit trails, in particular, for security and other failure events on the system. Furthermore, it is recommended to install a minimal system on the server in order to reduce the attack vector.

c) Implement a system to test and deploy security updates and ensure web server operating systems and applications are kept up-to-date promptly when new security updates are available.

d) Monitor security performance of the web server through regular review of the audit trails.

e) Run both anti-virus and anti-spyware on the server.

f) Scan all hosted and uploaded content regularly using up-to-date definitions. Recognize that a file may still be spyware or malware even if not detected by the current definitions due to the constraints of imperfect information.

g) Perform regular security penetration testing for the websites to ensure that their security is adequately maintained and have not been compromised by perpetrators.

To permit the enforcement of these security measures, in particular, those relating to website security, TSPs should consider incorporating these provisions in the terms of services agreement.

11.3 Safety and security guidance for end-users

11.3.1 User guidance and education

Provide guidance on how to stay safe online. TSPs may either create the guidance directly or refer the users to available guidance sites that could provide the contents. It is critical to educate the end-users on how they can contribute to a safe Internet. Examples of guidance campaigns or activities may include:

a) Periodic (for example, monthly) security newsletter to advise on specific security techniques (for example, how to choose a good password); updates on security trends; and notices of security webcasts and other on-demand videos, audio broadcasts, and security information that are available from the TSP web portal or other security content providers.

b) Direct broadcast of on-demand security education videos and/or webcasts covering a variety of security topics to improve end-users' security practices and awareness.

c) Incorporate a security column in the TSP hard-copy newsletter that is sent to the end-users' resident or office address to highlight key security events or contents.

d) Annual or other periodic end-user security seminars or road shows, possibly in partnership with other industry players, vendors and governments.

11.3.2 End-user technical security measures

As part of the user security education and guidance against deceptive software and spyware, TSPs should advise the end-users on the use of suitable technical security measures to protect their systems against known exploits and attacks. The minimum protective measures should include:

a) Use latest operating systems with the most updated security patches installed.

b) Use anti-virus and anti-spyware tools. If feasible, TSPs should partner with trusted security vendors[4] to offer them as part of the TSP subscription package so that the security measures are made available upon signing-up for the subscription or upon renewal.

c) Enable pop-up blocker. Common web browser and browser toolbars have now incorporated this capability, which will prevent malicious websites from displaying windows that contain spyware or deceptive software that could exploit system or browser weaknesses or use social engineering to trick users into downloading and installing them onto their systems. A list of recommended pop-up blocker tools should be collated and recommended, and their use should be encouraged with guidance on their enablement and how to allow pop-ups from websites that users' allow.

d) Enable personal firewall. Personal firewall is another important tool for controlling network services accessing the user systems, and vice versa. A number of newer operating systems have personal firewalls incorporated. While they are enabled by default, users or other applications might disable them, resulting in undesirable network security exposure. TSPs should encourage the use of the personal firewall functions, and/or suggest other third-party personal firewall products that TSPs have evaluated as trusted, and educate and help users in enabling basic network security at the end-user system level.

e) Enable automated updates. While the above technical security measures are capable of dealing with most malicious software at their respective operating levels, they are not very effective against exploitation of vulnerabilities that exist in operating systems and application products. To prevent such exploitation, updating functions available at the operating system, and also provided by user-trusted applications (for example, trusted third-party evaluated anti-spyware and anti-virus products), should be enabled for automated updates to be performed. This would then ensure that systems are updated with the latest security patches whenever they are available, closing the time gap for exploitation to take place.

Appendix I provides a list of references and online resources that could be used to support the implementation of the above recommendations.

---

[4] Trusted security vendors may be the TSP's business partners and/or vendors that provide products and services have been evaluated to meet the TSP security policies and requirements.

Appendix I

Additional resources

(This appendix does not form an integral part of this Recommendation)

I.1 Online security and anti-spyware references

There are a number of websites that can be referenced and leveraged for more information relating to Internet safety and security. These include:

- **Anti-Spyware Coalition** (http://www.antispywarecoalition.org/) – A group dedicated to building a consensus about definitions and best practices in the debate surrounding spyware and other potentially unwanted technologies. Composed of anti-spyware software companies, academics and consumer groups, the ASC seeks to bring together a diverse array of perspective on the problem of controlling spyware and other potentially unwanted technologies.
- **Be Web Aware** (http://www.bewebaware.ca) – National, bilingual public education program on Internet safety designed to ensure that young Canadians benefit from the Internet while being safe and responsible in their online activities.
- **Center for Safe and Responsible Internet Use** (http://csriu.org) – Organization providing outreach services addressing the issues of the safe and responsible use of the Internet.
- **Childnet International** (http://www.childnet-int.org) – Non-profit organization that works in partnership with others around the world to help make the Internet a great and safe place for children.
- **ECPAT International** (http://www.ecpat.net) – Network of organizations and individuals working together to eliminate the commercial sexual exploitation of children.
- **GetNetWise** (http://www.getnetwise.org) – Public service offered by a coalition of Internet industry corporations and public interest organizations that want users to be only "one click away" from the resources they need to make informed decisions about their and their families' use of the Internet.
- **Global Infrastructure Alliance for Internet Safety (GIAIS)** (http://www.microsoft.com/security/msra/default.mspx) – An alliance of service providers, which have organized to improve security and safety on the Web, manage threats consistently across a broad spectrum, and identify and mitigate existing vulnerabilities.
- **INHOPE** (http://www.inhope.org) – International association that supports Internet hotlines in their aim to respond to reports of illegal content to make the Internet safer.
- **Internet Safety Group** (www.netsafe.org.nz) – The NetSafe website is the online home of the Internet Safety Group of New Zealand (ISG) and Hector the Protector.
- **International Centre for Missing & Exploited Children** (http://www.icmec.org) – Global agency that promotes the safety and well-being of children through activism, policy development and multinational coordination.
- **Interpol** (http://www.interpol.int) – International police organization that facilitates cross-border police cooperation and supports and assists all organizations, authorities and services whose mission is to prevent or combat international crime.
- **iSafe** (http://www.isafe.org) – Worldwide leader in Internet safety education; incorporates classroom curriculum with dynamic community outreach to empower students, teachers, parents, law enforcement and concerned adults to make the Internet a safer place.

- **Microsoft Security At Home** (http://www.microsoft.com/protect) – Information and resources to help the public protect their computers, protect themselves and protect their families.
- **National Council for Motherhood and Childhood** (http://www.nccm.org.eg) – Egyptian organization dedicated to supporting childhood and motherhood from a rights-based approach.
- **Net Family News** (http://netfamilynews.org) – Non-profit public service providing a forum and "kid-tech news" for parents and educators in more than 50 countries.
- **NetAlert Limited** (http://www.netalert.gov.au) – Non-profit community organization established by the Australian government to provide independent advice and education on managing access to online content.
- **NetSmartzKids** (http://www.netsmartzkids.org) – NetSmartz is an interactive, educational safety resource from the National Center for Missing & Exploited Children (NCMEC) and Boys & Girls Clubs of America (BGCA) for children aged 5 to 17, parents, guardians, educators and law enforcement that uses age-appropriate, 3-D activities to teach children how to stay safer on the Internet.
- **Safe Kids Worldwide** (http://www.safekids.org) – Global network of organizations whose mission is to prevent accidental childhood injury, a leading killer of children 14 and under.
- **SafeKids.com** (http://www.safekids.com) – Resources to help families make the Internet and technology fun, safe and productive.
- **StaySafe.org** (http://www.staysafe.org) – Educational site intended to help consumers understand both the positive aspects of the Internet as well as how to manage a variety of safety and security issues that exist online.
- **UNICEF** (http://www.unicef.org) – Global advocate for the protection of children's rights dedicated to providing long-term humanitarian and developmental assistance to children and parents in developing countries.
- **WebSafe Crackerz** (http://www.websafecrackerz.com) – Interactive games and puzzles designed to help teenagers and offer strategies for dealing with different situations online including spam, phishing and scams.

I.2 Sample list of incident escalation contacts

Table I.1 below provides a sample list of Internet safety and security incident escalation contacts:

Table I.1 – Sample list of security escalation contact information

Organizations	Contact
Cisco Systems Inc.	mailto:safetyandsecurity@cisco.com http://www.cisco.com/security
Forum of Incident Response and Security Teams (FIRST)	http://www.first.org/about/organization/teams/
Microsoft Corporation	mailto:avsubmit@submit.microsoft.com mailto:secure@microsoft.com
Telecom-ISAC Japan	https://www.telecom-isac.jp/contact/index.html

Bibliography

[b-ITU-T X.1051] Recommendation ITU-T X.1051 (2004), *Information security management system – Requirements for telecommunications (ISMS-T).*

[b-ISO/IEC 27001] ISO/IEC 27001:2005, *Information Technology – Security techniques – Information Security Management Systems – Requirements*. http://www.iso.org/iso/catalogue-detail?csnumber=42103

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2008