International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series X

Supplement 6

(02/2009)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

ITU-T X.1240 series – Supplement on countering spam and associated threats

ITU-T X-series Recommendations – Supplement 6

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339

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

Supplement 6 to ITU-T X-series Recommendations

ITU-T X.1240 series – Supplement on countering spam and associated threats

Summary

Supplement 6 to ITU-T X-series Recommendations states that in order to deal effectively with spam, governments need to employ a variety of approaches, including effective laws, technological tools, and consumer and business education. This supplement reviews the international forums where the issue of spam is being addressed. As a case study, for illustrative purposes, it provides some information about the way the U.S. has approached the spam problem.

Source

Supplement 6 to ITU-T X-series Recommendations was agreed on 20 February 2009 by ITU-T Study Group 17 (2009-2012).

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

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the publication 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 publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication 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 publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. 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

Supplement 6 to ITU-T X-series Recommendations

ITU-T X.1240 series – Supplement on countering spam and associated threats

1 Scope

The topic of this supplement is spam and associated threats. This supplement is intended for national administrators who are newcomers to the concept of spam and would like some basic information about it.

This supplement looks at the tools that need to be employed to combat spam effectively and describes the work that some international forums are doing in this area. It provides, as a case study and for illustrative purposes, a description of what is the U.S. doing to combat spam.

2 References

None.

3 Definitions

This supplement defines the following terms:

3.1 phishing: An attempt to fool an individual into going to the wrong website with the intent of stealing that individual's private information.

3.2 spam: Although there is no universally agreed definition of spam, the term is commonly used to describe unsolicited electronic bulk communications over e-mail or mobile messaging (SMS, MMS).

4 Abbreviations and acronyms

This supplement uses the following abbreviations:

APEC TEL	Asia-Pacific Economic Community – Telecommunication and Information Working Group
CAN-SPAM	Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (U.S.)
CNSA	Contact Network of Spam Authorities (European Union)
FCC	Federal Communications Commission (U.S.)
FTC	Federal Trade Commission (U.S.)
LAP	London Action Plan
MAAWG	Messaging Anti-Abuse Working Group
MMS	Multimedia Messaging Service
MSCM	Mobile Service Commercial Messages
OECD	Organization for Economic Co-operation and Development
SMS	Short Messaging Service

5 Conventions

None.

6 Background

6.1 **Spam** has gone from being nuisance communications containing commercial advertisements to a facilitator of a more serious cybersecurity problem. For example, spam can be a vehicle for deception, spreading malware such as viruses and spyware, and inducing consumers to provide confidential information that can later be used to commit identity theft (i.e., phishing). Spammers take advantage of the fact that they can send their messages from anywhere in the world to anyone in the world at an extremely low cost to themselves. This makes spam an international problem that must be addressed through international cooperation.

6.2 **Phishing** takes advantage of the fact that, due to a basic characteristic in the Internet's e-mail system[1], anyone can send e-mail to anyone with almost no form of authentication. Phishing is an attempt to fool someone into going to the wrong website with the intent of stealing that individual's private information. Phishing exists in large part because sometimes people expect to receive e-mail from a popular site and they simply do not realize that the mail is not from the legitimate site. Because there is little authentication in e-mail, it is difficult to determine whether a message is legitimate without careful inspection of the message. Such careful inspection requires substantial knowledge of the underlying mechanisms used on the web.

Phishing also exists because most people find it difficult to verify that the websites they are going to are legitimate. Sometimes we do not look closely at the URL of a web page before entering sensitive information, and sometimes we just do not know what the correct URL should be.

The web servers used to "phish" sensitive information are often themselves the victims of malware, making it again extremely difficult to track phishers.

6.3 **Malware**, or malicious software that is made to run on a device without the knowledge or permission of the owner, is also a substantial problem.

7 National approaches to deal effectively with spam and associated threats

7.1 **National strategy and spam**: With respect to a national strategy, countries should develop and maintain a combination of effective laws, law enforcement authorities and tools, technological tools and best practices, and consumer and business education to effectively deal with spam.

7.2 **Legal and regulatory foundation and spam**: With respect to a legal foundation and regulatory framework, authorities that have jurisdiction over spam must have the necessary authority to investigate and take action against violations of laws related to spam that are committed from their country or cause effects in their country. Authorities that have jurisdiction over spam should also have mechanisms to cooperate with foreign authorities. Requests for assistance from foreign authorities should be prioritized based on areas of common interest and in cases where significant harm occurs.

7.3 **Government-industry collaborations and promotion of national awareness of spam and associated threats**: All interested persons, including enforcement authorities, businesses, industry groups, and consumer groups should cooperate in pursuing violations of laws related to spam. Government enforcement agencies should partner with industry and consumer groups to educate users and promote information sharing. Government enforcement agencies should cooperate with the private sector to promote the development of technological tools to fight spam, including tools to facilitate the location and identification of spammers.

---

[1] The Internet e-mail system was designed in the 1970s when access to the Internet was limited to a very few researchers and government members. There was no need to authenticate the identity of individuals sending e-mail, and therefore no effort was made to design the system to do so. While the e-mail system has evolved since then, this basic omission has been present ever since.

Phishing is often a preventable crime. Governments should work together with the private sector to improve means of protecting citizens from phishing, and educating consumers and businesses on safe authentication methods.

Governments can also play a role in educating the public on the need to keep malware in check by making use of tools such as anti-virus software and by applying the latest operating system patches and trusted computing techniques.

8 International (multilateral) countering spam initiatives

Several multilateral fora are working on initiatives to combat spam. These include:

8.1 London Action Plan

The U.S. Federal Trade Commission (FTC) and U.K. Office of Fair Trading hosted an International Spam Enforcement Conference in London in 2004, which led to the creation of a London Action Plan on International Spam Enforcement Cooperation (LAP). As of July 2008, government agencies and private sector representatives from more than 25 countries have endorsed the plan. The LAP encourages interested parties, including spam enforcement agencies and private sector stakeholders, to consider applying for membership in the organization.

The purpose of the LAP is to promote international spam enforcement cooperation and address spam related problems, such as online fraud and deception, phishing, and dissemination of viruses. The LAP builds relationships among these entities based on a short document that sets forth a basic work plan for improving international enforcement and education cooperation against illegal spam. This document is non-binding, asking participants only to use best efforts to move the work plan forward. http://londonactionplan.org/

Since its inception, the LAP has held annual workshops, typically in conjunction with the European Union's Contact Network of Spam Authorities (CNSA). In October, 2007, the LAP and CNSA co-located their annual joint workshop with the messaging anti-abuse working group (MAAWG) conference in Arlington, Virginia, which facilitated increased law enforcement cooperation with the private sector. In October 2008, the LAP and CNSA are co-locating their annual joint workshop with Eco's 6th German Anti-Spam Summit in Wiesbaden, Germany.

8.2 OECD Spam Toolkit and Council Recommendation on Spam Enforcement Cooperation

In April 2006, the OECD Spam Task Force released an Anti-Spam "Toolkit", which contains recommendations to help policy makers, regulators and industry players orient their policies relating to spam solutions and restore trust in the Internet and e-mail. The Toolkit contains eight elements, including anti-spam regulation, industry driven solutions and anti-spam technologies, education and awareness, and global cooperation/outreach. Recognizing that international cooperation is key to combating spam, the OECD governments also approved a "Recommendation on Cross-Border Co-operation in the Enforcement of Laws against Spam", which urges countries to ensure that their laws enable enforcement authorities to share information with other countries and do so more quickly and effectively. http://www.oecd-antispam.org/sommaire.php3.

8.3 APEC TEL Symposium on spam

In April 2006, APEC TEL held a symposium on "Spam and Related Threats" that brought together thirty speakers and panelists to discuss the evolution of the spam problem and establish a common agenda of action for the TEL. The main topics addressed included:

1) the development and application of national anti-spam regulatory regimes, including enforcement and codes of practice;

2) the role of industry in combating spam, including government-industry collaboration;

3) technical responses to spam;

4) cross-border cooperation and enforcement, including the Council of Europe's Convention on Cybercrime and the OECD Council Recommendation on Enforcement Cooperation as primary tools for enhancing cooperation; and

5) the need for targeted consumer education and awareness raising.

Concrete steps the TEL agreed to take going forward included:

1) encouraging information sharing on regulation and policy, drawing on resources such as the OECD Spam Toolkit;

2) developing a contact list for APEC spam authorities to augment similar resources developed by the OECD and the ITU;

3) encouraging economies to apply for membership in voluntary cooperation forums such as the London Action Plan or the Seoul-Melbourne Agreement;

4) cooperating with the OECD on information sharing and guidance-related initiatives; and

5) supporting capacity building for developing economies to better deal with spam.

9 Case study of some activities in the United States to counter spam

The following is a summary of the spam laws in the United States.

9.1 Laws establishing requirements for those who send commercial e-mail (CAN-SPAM Act)

In 2003, the United States enacted the "CAN-SPAM Act", which establishes requirements for those who send commercial e-mail, spells out penalties for spammers and companies whose products are advertised in spam if they violate the law, and gives consumers the right to ask e-mailers to stop spamming them.

The main provisions of the CAN-SPAM Act include the following:

- **It bans false or misleading header information**: Your e-mail's "From", "To", and routing information – including the originating domain name and e-mail address – must be accurate and identify the person who initiated the e-mail.
- **It prohibits deceptive subject lines**: The subject line cannot mislead the recipient about the contents or subject matter of the message.
- **It requires that your e-mail give recipients an opt-out method**: You must provide a return email address or another Internet-based response mechanism that allows a recipient to ask you not to send future e-mail messages to that e-mail address, and you must honour the requests. You may create a "menu" of choices to allow a recipient to opt out of certain types of messages, but you must include the option to end any commercial messages from the sender. Any opt-out mechanism you offer must be able to process opt-out requests for at least 30 days after you send your commercial e-mail. When you receive an opt-out request, the law gives you 10 business days to stop sending e-mail to the requestor's e-mail address. You cannot help another entity send e-mail to that address, or have another entity send e-mail on your behalf to that address. Finally, it is illegal for you to sell or transfer the e-mail addresses of people who choose not to receive your e-mail, even in the form of a mailing list, unless you transfer the addresses so another entity can comply with the law.
- **It requires that commercial e-mail be identified as an advertisement and include the sender's valid physical postal address**: Your message must contain clear and conspicuous notice that the message is an advertisement or solicitation and that the recipient can opt out of receiving more commercial e-mail from you. It also must include your valid physical postal address.

The U.S. Federal Trade Commission (FTC) is authorized to use its civil law enforcement authority to enforce the CAN-SPAM Act and to obtain civil penalties of up to USD 11'000 per violation. Since 1997, when the FTC brought its first enforcement action targeting unsolicited commercial e-mail, or "spam", the FTC actively has pursued deceptive and unfair spam practices through 94 law enforcement actions, 31 of which targeted violators of the CAN-SPAM Act.

CAN-SPAM also gives the Department of Justice the authority to enforce its criminal sanctions. The CAN-SPAM Act provides for significant criminal penalties, including jail time for spammers. Other federal and state agencies can enforce the law against organizations under their jurisdiction, and companies that provide Internet access may sue violators, as well.

9.2 Rules prohibiting sending commercial e-mail to wireless devices

The United States also has adopted rules to protect consumers from receiving unsolicited commercial messages (spam) on their wireless devices. With some exceptions, the rules prohibit the sending of commercial electronic mail messages, including e-mail and certain text messages, to wireless devices such as cell phones. The rules apply only to messages that meet the definition of "commercial" used in the CAN-SPAM Act – and to those messages where the main purpose of the message is a commercial advertisement or to promote a commercial product or service. Non-commercial messages, such as messages about candidates for public office or messages to update an existing customer about his or her account, are not subject to the rules.

Mobile service commercial messages (MSCMs) include any commercial message sent to an e-mail address that has been provided by a mobile service provider of a subscriber's wireless device. MSCMs are prohibited unless the individual addressee has given the sender express prior authorization (known as an "opt-in" requirement). The rule prohibits sending any commercial messages to addresses that contain domain names that have been listed on the FCC's list for at least 30 days or at any time prior to 30 days if the sender otherwise knows that the message is addressed to a wireless device. To assist senders of commercial messages to know which addresses belong to wireless subscribers, the rules require that wireless service providers supply the Federal Communications Commission (FCC) with the names of the relevant mail domain names. Short messaging service (SMS) messages transmitted solely to phone numbers are not covered by these protections. Auto-dialed calls are already covered by other laws.

Under the FCC's rules, the FCC can impose monetary forfeitures against spammers ranging from up to USD 11'000 per violation for non-licensees and to up to USD 130'000 per violation for common carrier licensees. In addition to monetary penalties, the FCC can issue a cease and desist order against a spammer that has violated any provision of the Communications Act or any FCC rule authorized by the Act. In addition, under the Communications Act, anyone who violates a provision of the Act is subject to criminal prosecution by the Department of Justice (in addition to a monetary penalty), and may face imprisonment for up to 1 year (up to 2 years for repeat offenders). To date, the FCC has not initiated any enforcement proceedings related to such commercial messages.

9.3 Approaches to limit phishing

As was discussed above, a basic premise that spammers and phishers count on is the lack of knowledge regarding who the sender is. Participants within the Internet Engineering Task Force have finalized a proposed standard, [b-IETF RFC 4871] that would improve a recipient's ability to identify senders. Vendors have begun to make implementations available to customers. There is also at least one free[2] implementation of the standard available. A source for assistance is the Anti-Phishing Working Group (APWG), an industry association focused on eliminating the identity theft and fraud that result from the growing problem of phishing and e-mail spoofing. The

[2] "Free" here refers to the ability to implement this feature royalty-free under conditions specified by the patent holder.

organization provides a forum to discuss phishing issues, trials and evaluations of potential technology solutions, and access to a centralized repository of phishing incidents http://www.antiphishing.org.

This standard enables "white list validation", or the ability to verify that, for example, it really is your bank or your friends or associates that are trying to reach you. This standard in and of itself will limit some forms of phishing, but not all.

Bibliography

[b-IETF RFC 4871] IETF RFC 4871 (2007), *Domainkeys Identified Mail (DKIM) Signatures*. <http://www.ietf.org/rfc/rfc.4871.txt>

[b-contr-spam] Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (United States Code). This Act is documented in the following laws: 15 U.S.C. §§ 7701-7713; 18 U.S.C. § 1037; 28 U.S.C. § 994; 47 U.S.C. § 227. <http://www.gpsaccess.gov/uscode/index.html>

[b-ITU-T cyb] Messaging Anti-Abuse Working Group Conference reports: http://www.itu.int/ITU-D/cyb/cybersecurity/spam.html.

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, 2009