

International Telecommunication Union

**ITU-T**

TELECOMMUNICATION  
STANDARDIZATION SECTOR  
OF ITU

**X.1240**

(04/2008)

SERIES X: DATA NETWORKS, OPEN SYSTEM  
COMMUNICATIONS AND SECURITY

Telecommunication security

---

## **Technologies involved in countering e-mail spam**

Recommendation ITU-T X.1240

ITU-T X-SERIES RECOMMENDATIONS  
DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

|                                               |                |
|-----------------------------------------------|----------------|
| <b>PUBLIC DATA NETWORKS</b>                   |                |
| 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    |
| <b>OPEN SYSTEMS INTERCONNECTION</b>           |                |
| 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    |
| <b>INTERWORKING BETWEEN NETWORKS</b>          |                |
| General                                       | X.300–X.349    |
| Satellite data transmission systems           | X.350–X.369    |
| IP-based networks                             | X.370–X.379    |
| <b>MESSAGE HANDLING SYSTEMS</b>               | X.400–X.499    |
| <b>DIRECTORY</b>                              | X.500–X.599    |
| <b>OSI NETWORKING AND SYSTEM ASPECTS</b>      |                |
| 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    |
| <b>OSI MANAGEMENT</b>                         |                |
| 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    |
| <b>SECURITY</b>                               | X.800–X.849    |
| <b>OSI APPLICATIONS</b>                       |                |
| 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    |
| <b>OPEN DISTRIBUTED PROCESSING</b>            | X.900–X.999    |
| <b>TELECOMMUNICATION SECURITY</b>             | <b>X.1000–</b> |

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

# **Recommendation ITU-T X.1240**

## **Technologies involved in countering e-mail spam**

### **Summary**

Recommendation ITU-T X.1240 specifies basic concepts, characteristics and effects of e-mail spam, and technologies involved in countering e-mail spam. It also introduces the current technical solutions and related activities from various standards development organizations and relevant organizations on countering e-mail spam. It provides guidelines and information to users who want to develop technical solutions on countering e-mail spam. This Recommendation will be used as a basis for further development of technical Recommendations on countering e-mail spam.

### **Source**

Recommendation ITU-T X.1240 was approved on 18 April 2008 by ITU-T Study Group 17 (2005-2008) under the WTSA Resolution 1 procedure.

## 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/>.

© ITU 2009

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

# CONTENTS

## Page

|      |                                                                                |    |
|------|--------------------------------------------------------------------------------|----|
| 1    | Scope .....                                                                    | 1  |
| 2    | References.....                                                                | 1  |
| 3    | Definitions .....                                                              | 1  |
| 4    | Abbreviations and acronyms .....                                               | 1  |
| 5    | Conventions .....                                                              | 2  |
| 6    | Introduction to countering e-mail spam.....                                    | 2  |
| 6.1  | Concept and Characteristics of spam .....                                      | 2  |
| 6.2  | Approaches to countering e-mail spam .....                                     | 3  |
| 7    | Anti-spam technologies .....                                                   | 3  |
| 7.1  | Overview .....                                                                 | 4  |
| 7.2  | The importance of tool/technology context.....                                 | 4  |
| 7.3  | Combining tests .....                                                          | 5  |
| 7.4  | Types of anti-spam technologies .....                                          | 5  |
| 7.5  | Existence of the sender's domain and eliciting a response .....                | 6  |
| 7.6  | Existence of a pointer record (PTR).....                                       | 6  |
| 7.7  | Blacklists/whitelists.....                                                     | 7  |
| 7.8  | Address of the sending server treated as either "dynamic" or "residential" ... | 7  |
| 7.9  | Filtering .....                                                                | 8  |
| 7.10 | HELO/CSV.....                                                                  | 9  |
| 7.11 | Greylisting .....                                                              | 10 |
| 7.12 | Tokens/passwords.....                                                          | 10 |
| 7.13 | Various techniques .....                                                       | 10 |
| 7.14 | How to use this review of technologies and factors to consider .....           | 11 |
| 7.15 | Rejection in the SMTP session.....                                             | 12 |
| 7.16 | Silent rejection.....                                                          | 12 |
| 7.17 | Rejection by sending a DSN (delivery status notification or "bouncing").....   | 12 |
| 7.18 | Delivery to a spam box.....                                                    | 12 |
| 7.19 | Marking .....                                                                  | 12 |
|      | Appendix I – Activities on countering e-mail spam .....                        | 13 |
| I.1  | Introduction .....                                                             | 13 |
| I.2  | International activities on countering spam.....                               | 13 |
| I.3  | Development of technical specifications for countering spam.....               | 15 |
| I.4  | List of industry alliances and initiatives for countering spam.....            | 16 |
|      | Bibliography.....                                                              | 20 |

## Introduction

As requested by WTSA-2004 Resolution 52 'Countering spam by technical means', standardization work was undertaken to develop ITU-T Recommendations that help countering spam by technical means. This Recommendation is one of a series of ITU-T Recommendations for countering e-mail spam which consist of guidelines, requirements, a technical framework and technical strategies. Other ITU-T Recommendations on countering spam for IP multimedia applications such as IP telephony, instant messaging and conference will be developed as separate documents.

...

# Recommendation ITU-T X.1240

## Technologies involved in countering e-mail spam

### 1 Scope

This Recommendation specifies the technologies involved in countering e-mail spam. It introduces the current technical solutions and related activities from various standards development organizations and relevant organizations for countering e-mail spam. The purpose of this Recommendation is to provide useful information to users who want to develop technical solutions for countering e-mail spam. This Recommendation will be used as a basis for further development of technical Recommendations on countering e-mail spam.

NOTE – The use of the term "identity" in this Recommendation does not indicate its absolute meaning. In particular, it does not constitute any positive validation.

### 2 References

None.

### 3 Definitions

This Recommendation defines the following terms:

**3.1 phisher:** An entity or a person launching phishing attacks.

**3.2 phishing:** Phishing attacks use both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. Social-engineering schemes use 'spoofed' e-mails to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as credit card numbers, account usernames, passwords and social security numbers. Hijacking brand names of banks, e-retailers and credit card companies, phishers often convince recipients to respond. Technical subterfuge schemes plant crimeware onto PCs to steal credentials directly, often using trojan keylogger spyware.

**3.3 spam:** The meaning of the word "spam" depends on each national perception of privacy and what constitutes spam from the national technological, economic, social and practical perspectives. In particular, its meaning evolves and broadens as technologies develop, providing novel opportunities for misuse of electronic communications. Although there is no globally agreed definition for spam, this term is commonly used to describe unsolicited electronic bulk communications over e-mail or mobile messaging for the purpose of marketing commercial products or services.

**3.4 spammer:** An entity or a person creating and sending spam.

### 4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

|      |                                   |
|------|-----------------------------------|
| API  | Application Programming Interface |
| DKIM | DomainKeys Identified Mail        |
| CSV  | Certified Server Validation       |
| DNS  | Domain Name System                |
| DSN  | Delivery Status Notification      |

|      |                                                        |
|------|--------------------------------------------------------|
| HTML | HyperText Markup Language                              |
| IM   | Instant Messaging                                      |
| ISP  | Internet Service Provider                              |
| META | Message Enhancements for Transmission Authorization    |
| MMS  | Multimedia Messaging Service                           |
| MTA  | Mail Transfer Agent                                    |
| OECD | Organization for Economic Co-Operation and Development |
| OPES | Open Pluggable Edge Services                           |
| PGP  | Pretty Good Privacy                                    |
| PTR  | Pointer Record                                         |
| SMS  | Short Message Service                                  |
| SMTP | Simple Mail Transfer Protocol                          |
| SPF  | Sender Policy Framework                                |
| TEOS | Trusted Email Open Standard                            |

## 5 Conventions

None.

## 6 Introduction to countering e-mail spam

### 6.1 Concept and Characteristics of spam

Although there is no universally agreed definition of spam, the term is commonly used to describe unsolicited electronic communications over e-mail, mobile messaging (SMS, MMS) and instant messaging services, usually with the objective of marketing commercial products or services.

While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media, e.g., mobile phone messaging spam, IP-based telephony spam, instant messaging spam, Usenet newsgroup spam, web search engine spam and blog spam. The content of the spam messages ranges from advertisement of goods to offensive pornographic material. E-mail spam has various kinds of harmful effects to e-mail service users and internet service providers:

- Spam recipients and ISPs spend a lot of time, money and effort to identify, delete and filter spam.
- E-mail spam may include deceptive contents alluring to spam recipients, or adult content inappropriate for children.
- E-mail service users and ISPs suffer from the waste of network resources and storage.
- Spread of virus and spyware can be a threat to the network security.
- E-mail spam decreases the visibility of normal and important e-mails.

A recent and growing phenomenon is the use of spam to support fraudulent and criminal activities, including attempts to capture financial information (e.g., account numbers and passwords) by masquerading messages as originating from trusted companies ("brand-spoofing" or "phishing"), as well as a vehicle to spread viruses and worms.

Phishing attacks use both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. Social-engineering schemes use 'spoofed' e-mails to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as credit card numbers, account usernames, passwords and social security numbers. Hijacking brand names of banks, e-retailers and credit card companies, phishers often convince recipients to respond. Technical subterfuge schemes plant crimeware onto PCs to steal credentials directly, often using trojan keylogger spyware. Pharming crimeware misdirects users to fraudulent sites or proxy servers, typically through domain name system (DNS) hijacking or poisoning.

Spammers have proven themselves to be highly creative in avoiding detection, including falsification of origin of e-mail and randomization of content to bypass spam filters. The scale of the problem has grown to such an extent that anti-spam laws are being rapidly enacted in a number of countries, although different national approaches and remedies are used. At the same time, there is increasing recognition that countering spam is an issue requiring international coordination and cooperation.

## **6.2 Approaches to countering e-mail spam**

Since e-mail spam does great damage to e-mail service users, ISPs and network operators, technologies have been developed and regulations have been adopted in many countries to help counter spam. However, it is difficult to counter spam effectively through a single countering measure such as filtering or legal punishment since countering spam is not a simple problem. For that reason, various methods should be applied simultaneously to counter spam effectively:

- Regulation: Anti-spam regulations should be adopted to facilitate the appropriate response of service users for e-mail spam and to increase the effect of anti-spam technologies such as filtering. In addition, regulation can help protect service users and ISPs from illegal spam.
- Technology: Anti-spam technology development is essential for countering large quantities of e-mail spam effectively. It is required to develop various technologies to prevent sending spam, and to identify and filter spam effectively.
- Industrial action: Various kinds of anti-spam technologies, including blacklist or whitelist and filtering functions, are appropriate to be developed and installed by industry participants such as ISPs or network operators. It is also possible for ISPs to adopt policies for countering e-mail spam.
- International cooperation: International cooperation is required, since telecommunication networks are borderless, and the generation and effect of spam are not domestic. International cooperation is also useful for information sharing about effective regulation adoption, anti-spam technology development, and education of service users and providers.
- Education: To minimize the damage caused by e-mail spam, education of service users and ISPs is important. The education is expected to help e-mail users take appropriate actions for e-mail spam, and ISPs to adopt anti-spam policies and technologies.

Among various anti-spam measures introduced above, this Recommendation focuses on technical means for countering spam such as development and application of anti-spam technologies.

## **7 Anti-spam technologies**

The report of the OECD Task Force on Spam [b-OECD TF] provides several elements for countering e-mail spam including regulatory approaches, enforcement concerns and technical solutions. This Recommendation includes a reference to a part of the report (Element IV – Anti-spam technologies) in this clause. Consideration is required because the anti-spam toolkit was published in May 2006 and has not been updated since.