International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series X

Supplement 29

(09/2017)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

ITU-T X.1242 – Supplement on guidelines on countermeasures against short message service phishing and smishing attacks

ITU-T X-series Recommendations – Supplement 29

International Telecommunication Union

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 (1)	
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 (1)	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 (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed legder technology security	X.1400–X.1429
Security protocols (2)	X.1450–X.1459
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

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

Supplement 29 to ITU-T X-series Recommendations

ITU-T X.1242 – Supplement on guidelines on countermeasures against short message service phishing and smishing attacks

Summary

Supplement 29 to Recommendation ITU-T X.1242 provides universal guidelines on short message service (SMS) phishing which is a fraudulent technique through mobile phones by causing phishing frauds with smartphones, acquiring personal information on the smartphones, or by enabling small amounts of money to be approved and paid while the account holder is not aware of the approval.

The purpose of this Supplement is to universalize the guideline for countermeasures against SMS phishing incident by defining a security guideline about security technology against SMS phishing incident and method, and specification of report contents.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X Suppl. 29	2017-09-06	17	11.1002/1000/13409

Keywords

Measures, phishing, smishing, short message service.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

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/.

Table of Contents

		Page
1	Scope	1
2	References	1
3	Definitions	1
	3.1 Terms defined elsewhere	1
	3.2 Terms defined in this Supplement	1
4	Abbreviations and acronyms	2
5	Conventions	2
6	Overview	2
7	Countermeasures against SMS phishing attacks	3
	7.1 Typical SMS phishing attack scenario	3
	7.2 Recommendations for end users	3
	7.3 Recommendations for service providers	3
8	Countermeasures against SMS smishing attacks	3
	8.1 Smishing attack scenario	3
	8.2 Recommendations for end users	4
	8.3 Recommendations for service providers	5
Bibliography		6

Supplement 29 to ITU-T X-series Recommendations

ITU-T X.1242 – Supplement on guidelines on countermeasures against short message service phishing and smishing attacks

1 Scope

This Supplement provides guidelines on countermeasures against short message service (SMS) based phishing and smishing attacks from the perspective of the user side and the network operator side.

2 References

[ITU-T X.1242] Recommendation ITU-T X.1242 (2009), *Short message service (SMS) spam filtering system based on user-specified rules.*

3 Definitions

3.1 Terms defined elsewhere

This Supplement uses the following terms defined elsewhere:

3.1.1 malware [b-ISO/IEC 27033-1]: Malicious software designed specifically to damage or disrupt a system, attacking confidentiality, integrity and/or availability.

NOTE – Viruses and Trojan horses are examples of malware.

3.1.2 short message (SM) [b-ETSI TS 102 507]: Information that is conveyed from a sending user to a receiving user via an SM-SC.

3.1.3 short message service centre (SM-SC) [b-ETSI TS 102 507]: Function unit, which is responsible for the relaying and store-and-forwarding of a short message (SM) between two SM-TEs.

NOTE – The SM-SC can functionally be separated from or integrated in the network.

3.1.4 spam [ITU-T X.1242]: The electronic information delivered from senders to recipients by terminals such as computers, mobile phones, telephones, etc., which is usually unsolicited, unwanted, and harmful for recipients.

3.1.5 short message service (SMS) [ITU-T X.1242]: The services in telecommunication networks, which provide mobile phones, telephones and other SMEs to transfer and receive text messages through SMSCs that store messages if the receiving terminal cannot be contacted.

3.1.6 SMS spam [ITU-T X.1242]: Spam sent via SMS.

3.2 Terms defined in this Supplement

This Supplement defines the following terms:

3.2.1 phishing: An attack to acquire sensitive information such as usernames, passwords, and credit card details for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.

3.2.2 smishing: An attack in which the user is tricked into downloading a Trojan horse, virus or other malware onto his cellular phone or other mobile device.

3.2.3 uniform resource locator (URL): A reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it.

3.2.4 caller ID spoofing: The process of changing the caller ID to any number other than the calling number.

3.2.5 caller identification: A telephone service that transmits a caller's telephone number to the called party's telephone equipment when the call is being set up.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

FMD Filtered Messages Database

SCM Service Control Module

SM Short Message

SMS Short Message Service

SM-SC Short Message Service Centre

SM-TE Short Message Technical Equipment

SSFM SMS Spam Filtering Module

URD User-specified Rules Database

URL Uniform Resource Locator

USMM User Service Management Module

5 Conventions

None.

6 Overview

Short message service (SMS) phishing is the attempt to acquire sensitive information such as usernames, passwords and credit card details (and sometimes, indirectly, money) for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.

SMS smishing is an attack that tricks the user into downloading a Trojan horse or other malicious software through SMS. It can also be used to infect users' phones and related networks with destructive viruses or eavesdropping software and uses SMS technology to phish for a user's sensitive personally identifiable information, such as social security numbers or user names and passwords for online banking.

The framework for countering phishing and smishing in this Supplement is based on the SMS spam filtering system, which includes the following logical modules: service control module (SCM), SMS spam filtering module (SSFM), user service management module (USMM), user-specified rules database (URD) and filtered messages database (FMD). The structure of the SMS spam filtering system is given in Figure 1 of [ITU-T X.1242].

Most spammers and smishing attackers send texts via an Internet text relay service in order to hide their identity. Many cellar service providers can provide a feature to end-users that will block texts that come in from the Internet. This is another easy way to filter out spam and smishing SMS.

This Supplement provides a guideline on countermeasures against both SMS-based phishing and smishing attacks.

7 Countermeasures against SMS phishing attacks

7.1 Typical SMS phishing attack scenario

The objective of SMS phishing is for spammers to acquire sensitive information such as usernames, passwords and credit card details for malicious reasons, by masquerading as a trustworthy entity in an electronic communication. SMS phishing exploits mobile phone text messages to deliver the bait to trick users into divulging their personal information.

This clause describes a typical attack scenario for an SMS phishing attack as follows:

- An attacker sends a text message to end users's mobile device.
- This message asks end users to provide sensitive personal or financial information via a web link and false website, or via a telephone number.
- An attacker uses the user's information for further fraudulent activities by masquerading as a trustworthy entity.

7.2 Recommendations for end users

This clause describes recommendations for end users to prevent them from falling victim to a phishing attack.

- End users should not respond to text messages that request private or financial information.
- If users receive a message that appears to be from an organization, financial institution or other entity that users do business with, the end users should contact that organization or entity directly to determine if the message they receive is a legitimate request, and ascertain that entity's policy on sending text messages to users with regard to requests for private or financial information.
- End users should stop and think about it, if a text message is urging them to act or respond quickly.
- End users should not reply to a suspicious text message without doing their research and verifying the source.
- End users should not call a phone number from an unknown sender.
- End users should keep its web browser up to date.
- End users should use antivirus software.

7.3 Recommendations for service providers

This clause describes recommendations for cell service providers to prevent phishing attacks.

- Cell service providers should provide "calling identification display" feature to end-users.
- Cell service providers should provide "caller ID spoofing prevention" feature of end-users.
- Cell service providers should provide measures to block SPAM messages from Internet.

8 Countermeasures against SMS smishing attacks

8.1 Smishing attack scenario

This clause describes a typical attack scenario for smishing attacks as shown in Figure 1.

1. A malicious application is uploaded to the distribution site.
2. An attacker sends a text message to end users.
3. An end user clicks on the uniform resource locator (URL) that downloads a malicious application.

4. The malicious application is downloaded to the end-user's phone.
5. The malicious application is installed in the mobile phone.
6. The malicious application sends sensitive financial information to the relay server without the user's knowledge.
7. The relay server forwards the information to the attacker.

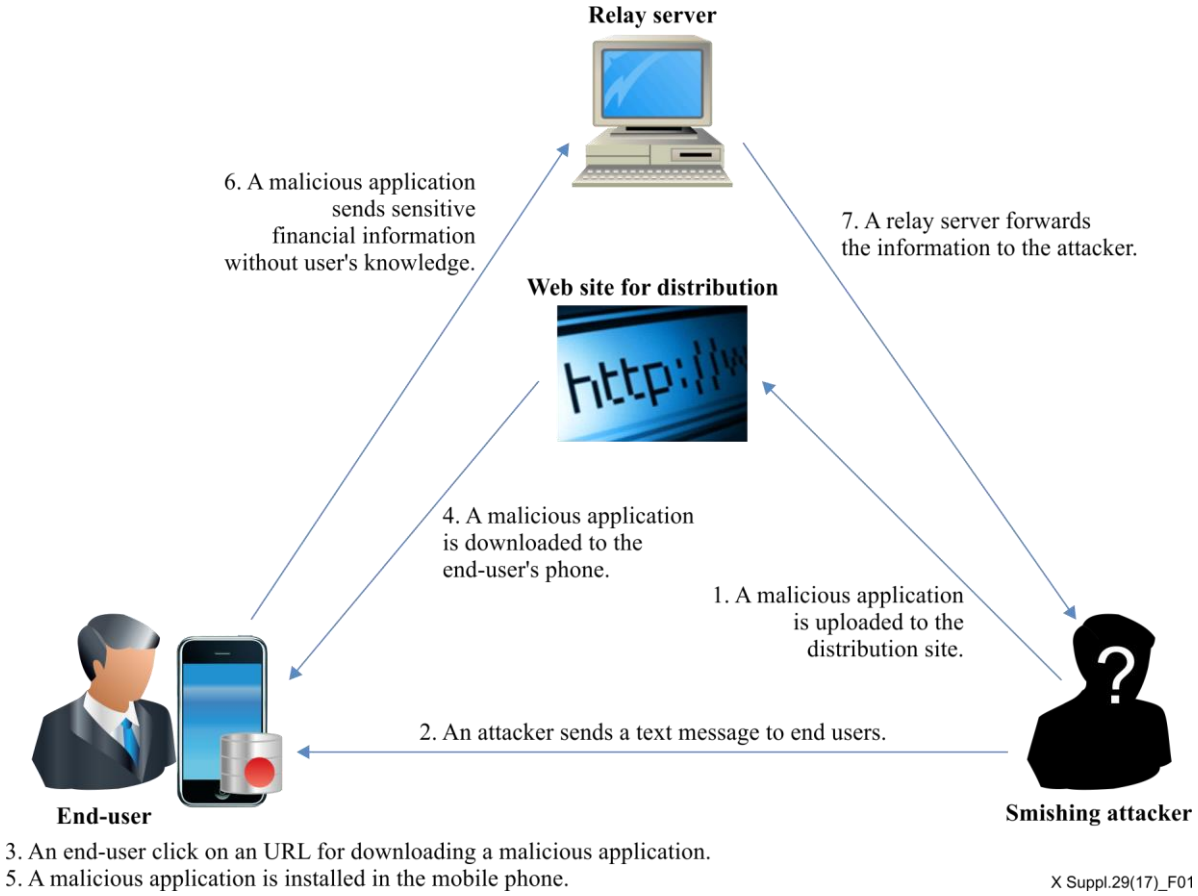

Figure 1 – Typical smishing attack scenario

8.2 Recommendations for end users

This clause provides recommendations for end users to prevent them from falling victims to smishing attacks.

- End users should use the "block texts from the internet WEB-SMS" feature, if available from their cellular service provider.
- End users should not respond to text messages that request them to disclose credentials or financial information.
- End users should not click on URLs within text messages, especially if they are sent from someone unknown, and should also be cautious to even click on URLs within text messages received from someone they know, since attack messages can appear to come from someone known.
- Even if a message that is received appears to come from the user's bank, financial institution or other entity with which business is conducted, end users should contact the entity directly to determine if the request is legitimate, and should also review the entity's policy on sending text messages to customers.

- End users should be aware of messages from a known smishing source number indicating that some other number is not a cell phone number. Scammers often mask their identity by using email-to-text services, so as not to disclose their real cellular phone number.
- End users should stop responding to messages if a text message is urging them to act or respond quickly, and to keep in mind that attackers use text messages to lure users into doing what they want.
- End users should not reply to a suspicious text message without verifying the source.
- End users should not call a phone number from a person that is unknown to them.

8.3 Recommendations for service providers

This clause describes recommendations for cell service providers to prevent smishing attacks.

- Cell service providers should provide end users with the feature "block texts from the internet WEB-SMS".
- Cell service providers should provide a countering system for preventing smishing attacks.

Bibliography

[b-ETSI TS 102 507] ETSI TS 102 507 V1.1.1 (2006), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Fixed network Short Message Service (F-SMS) for IP networks; Service description.*

[b-ISO/IEC 27033-1] ISO/IEC 27033-1:2015, *Information technology – Security techniques – Network security – Part 1: Overview and concepts.*

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
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	Environment and ICTs, climate change, e-waste, energy efficiency; 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, and associated measurements and tests
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, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2019