The State of Smishing and Counter Measures

MACNICA, Inc.
Networks Company
Telecom Security Services Office
Kazumi Suzuki, General Manager
Ichiro Maruyama, Chief Engineering Specialist

Co.Tomorrowing
MACNICA

Table of Contents

Introduction

We have written this material with the hope that it will lead to a wider perspective and technical understanding for those working on anti-smishing measures. Unlike previous cybersecurity measures, anti-smishing measures require a perspective of cybercrime and background knowledge related to mobile phone and smartphone systems as living infrastructure. It's also a different challenge than IT security to protect information assets. With this in mind, we will explain the ins and outs of Smishing based on the knowledge obtained from MACNICA's support experiences for telecommunications infrastructure security measures and cybercrime investigation activities.

About Smishing

Smishing is a variant of phishing, a term devised from SMS Phishing. It uses the Short Message Service (SMS) on mobile phones to send fraudulent messages that take recipients to fake websites to steal personal information. The main targets are account information of banking and e-commerce, and information related to electronic payments and credit card usage. The information obtained will be used for criminal activities such as making fraudulent transfers or withdrawals of money in the guise of the person, purchasing goods on EC sites, or making fraudulent credit payments.

Smishing has a characteristic that stems from the fact that SMS is tied to mobile phone number associating to the subscriber. This can be appeared in the trends and extent of crimes, as well as in the methods of attacks (fraud techniques), the characteristics of victims and criminals, and the counter measures of the issues. That's the point of this paper.

Trends of threat and financial losses caused by Smishing

Smishing has become a major social problem in the last few years. As of 2022, phishing, including smishing, is the No. 1 threat to individuals in the “10 Major Security Threats 2022” published by the Information-technology Promotion Agency, Japan (IPA). Also, there are threats closely related to phishing/smishing, such as credit card fraud (4th rank), smartphone payment fraud (5th), and malicious apps damaging smartphone users (7th) in the ranking (Figure 1).

Smartphones have become daily necessities, linking individuals to various services and forming a platform for economic activities. This economic zone also has become an area of activity for criminals as well as in the physical world. It causes leading to widespread scams targeting individuals such as Smishing.

The amount of financial losses caused by unauthorized use of credit cards continues to increase year by year. According to the Japan Credit Association, the amount of losses caused by credit card fraud in 2021 was 33.01 billion yen (an increase of 30.5% from previous year), the record high in statistics. Within this, 31.17 billion yen (an increase of 39.4%) was related to the credit card number theft, accounting for 94% of total losses (Figure 2).

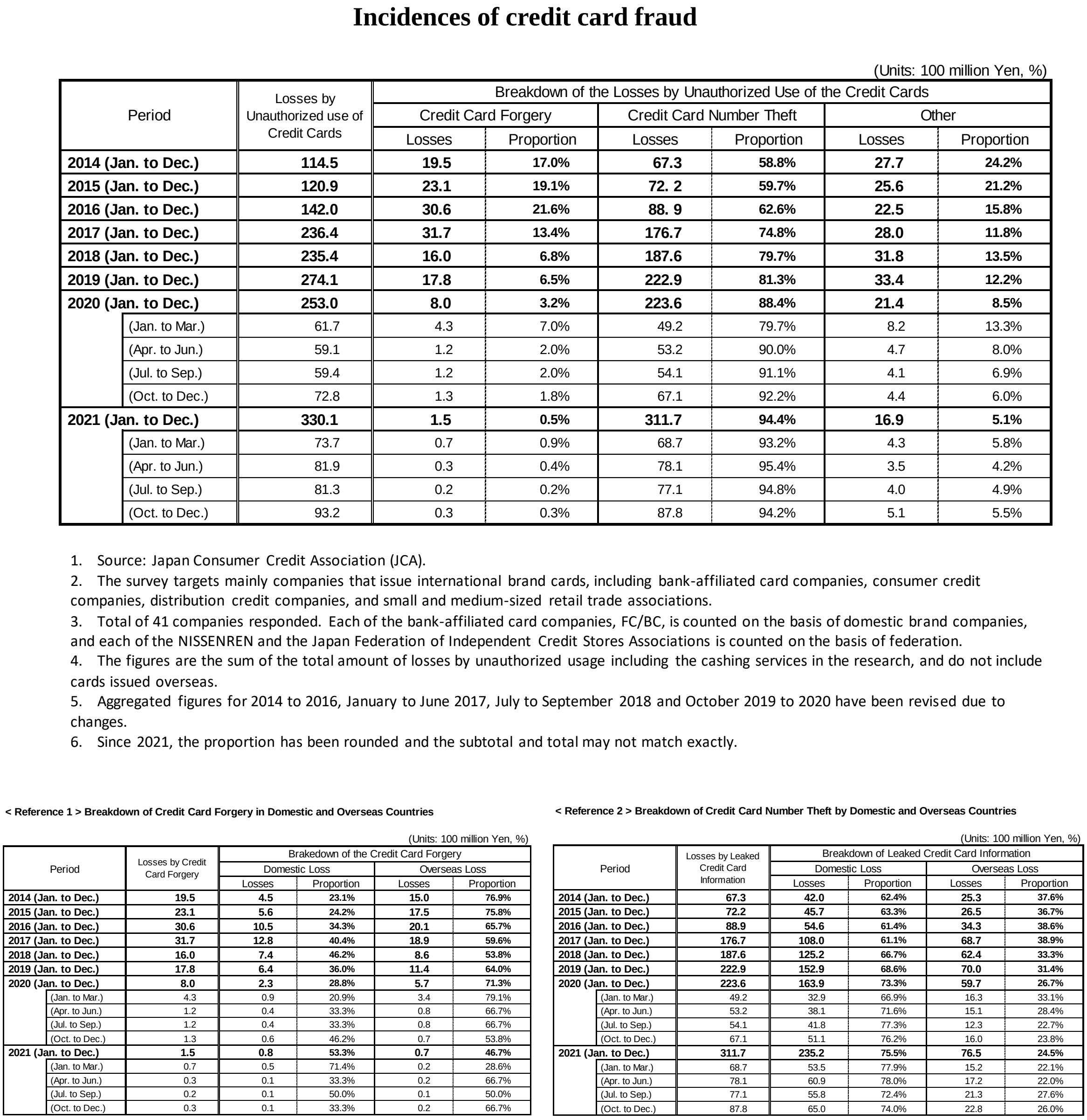
As it will be discussed in more details later, in recent years, targets of the Smishing became focusing to the credit card number thefts, and from the point of the amount of financial losses, phishing, including smithing, is an important issue to be addressed.

NEW: Threads ranked for the first time

Last year Rank	Threats for Individuals	Rank	Threats for Organizations	Last year Rank
2nd	Phishing fraud for Personal Information	**1st**	Financial Loss by Ransomware	1st
3rd	Cyberbullying and fake News	**2nd**	Confidential Information Theft by APT	2nd
4th	Extortion of Money by Blackmail or fraudulent Methods with E-mail, SMS, etc.	**3rd**	Attacks Exploiting Supply Chain Weaknesses	4th
5th	Unauthorized use of Leaked credit card information	**4th**	Attacks on Telework and other new Normal Ways of Working	3rd
1st	Unauthorized Use of Smartphone Payments	**5th**	Information Leakage by Internal fraudulent Acts	6th
8th	Internet Fraud by Fake Warnings	**6th**	Increase in Abuse following Disclosure of Vulnerability Information	10th
9th	Malicious Smartphone Applications	**7th**	Attacks targeting the Release of Software Fixes (Zero-Day Attacks)	NEW
7th	Personal Information Theft from Services on the Internet	**8th**	Financial Loss by Business E-mail Compromise	5th
6th	Unauthorized Use of Internet Banking Credentials	**9th**	Suspension of Business due to Unexpected IT Infrastructure Failure	7th
10th	Unauthorized Login to Services on the Internet	**10th**	Careless Information Leakage	9th

Figure 1. From IPA Japan, “10 Major Security Threats 2022”

https://www.ipa.go.jp/security/vuln/10threads2022.html



Incidences of credit card fraud

(Units: 100 million Yen, %)

Period	Losses by Unauthorized use of Credit Cards	Breakdown of the Losses by Unauthorized Use of the Credit Cards					
		Credit Card Forgery		Credit Card Number Theft		Other	
		Losses	Proportion	Losses	Proportion	Losses	Proportion
2014 (Jan. to Dec.)	**114.5**	**19.5**	**17.0%**	**67.3**	**58.8%**	**27.7**	**24.2%**
2015 (Jan. to Dec.)	**120.9**	**23.1**	**19.1%**	**72. 2**	**59.7%**	**25.6**	**21.2%**
2016 (Jan. to Dec.)	**142.0**	**30.6**	**21.6%**	**88. 9**	**62.6%**	**22.5**	**15.8%**
2017 (Jan. to Dec.)	**236.4**	**31.7**	**13.4%**	**176.7**	**74.8%**	**28.0**	**11.8%**
2018 (Jan. to Dec.)	**235.4**	**16.0**	**6.8%**	**187.6**	**79.7%**	**31.8**	**13.5%**
2019 (Jan. to Dec.)	**274.1**	**17.8**	**6.5%**	**222.9**	**81.3%**	**33.4**	**12.2%**
2020 (Jan. to Dec.)	**253.0**	**8.0**	**3.2%**	**223.6**	**88.4%**	**21.4**	**8.5%**
(Jan. to Mar.)	61.7	4.3	7.0%	49.2	79.7%	8.2	13.3%
(Apr. to Jun.)	59.1	1.2	2.0%	53.2	90.0%	4.7	8.0%
(Jul. to Sep.)	59.4	1.2	2.0%	54.1	91.1%	4.1	6.9%
(Oct. to Dec.)	72.8	1.3	1.8%	67.1	92.2%	4.4	6.0%
2021 (Jan. to Dec.)	**330.1**	**1.5**	**0.5%**	**311.7**	**94.4%**	**16.9**	**5.1%**
(Jan. to Mar.)	73.7	0.7	0.9%	68.7	93.2%	4.3	5.8%
(Apr. to Jun.)	81.9	0.3	0.4%	78.1	95.4%	3.5	4.2%
(Jul. to Sep.)	81.3	0.2	0.2%	77.1	94.8%	4.0	4.9%
(Oct. to Dec.)	93.2	0.3	0.3%	87.8	94.2%	5.1	5.5%

1. Source: Japan Consumer Credit Association (JCA).
2. The survey targets mainly companies that issue international brand cards, including bank-affiliated card companies, consumer credit companies, distribution credit companies, and small and medium-sized retail trade associations.
3. Total of 41 companies responded. Each of the bank-affiliated card companies, FC/BC, is counted on the basis of domestic brand companies, and each of the NISSENREN and the Japan Federation of Independent Credit Stores Associations is counted on the basis of federation.
4. The figures are the sum of the total amount of losses by unauthorized usage including the cashing services in the research, and do not include cards issued overseas.
5. Aggregated figures for 2014 to 2016, January to June 2017, July to September 2018 and October 2019 to 2020 have been revised due to changes.
6. Since 2021, the proportion has been rounded and the subtotal and total may not match exactly.

< Reference 1 > Breakdown of Credit Card Forgery in Domestic and Overseas Countries

(Units: 100 million Yen, %)

Period	Losses by Credit Card Forgery	Brakedown of the Credit Card Forgery			
		Domestic Loss		Overseas Loss	
		Losses	Proportion	Losses	Proportion
2014 (Jan. to Dec.)	**19.5**	**4.5**	**23.1%**	**15.0**	**76.9%**
2015 (Jan. to Dec.)	**23.1**	**5.6**	**24.2%**	**17.5**	**75.8%**
2016 (Jan. to Dec.)	**30.6**	**10.5**	**34.3%**	**20.1**	**65.7%**
2017 (Jan. to Dec.)	**31.7**	**12.8**	**40.4%**	**18.9**	**59.6%**
2018 (Jan. to Dec.)	**16.0**	**7.4**	**46.2%**	**8.6**	**53.8%**
2019 (Jan. to Dec.)	**17.8**	**6.4**	**36.0%**	**11.4**	**64.0%**
2020 (Jan. to Dec.)	**8.0**	**2.3**	**28.8%**	**5.7**	**71.3%**
(Jan. to Mar.)	4.3	0.9	20.9%	3.4	79.1%
(Apr. to Jun.)	1.2	0.4	33.3%	0.8	66.7%
(Jul. to Sep.)	1.2	0.4	33.3%	0.8	66.7%
(Oct. to Dec.)	1.3	0.6	46.2%	0.7	53.8%
2021 (Jan. to Dec.)	**1.5**	**0.8**	**53.3%**	**0.7**	**46.7%**
(Jan. to Mar.)	0.7	0.5	71.4%	0.2	28.6%
(Apr. to Jun.)	0.3	0.1	33.3%	0.2	66.7%
(Jul. to Sep.)	0.2	0.1	50.0%	0.1	50.0%
(Oct. to Dec.)	0.3	0.1	33.3%	0.2	66.7%

< Reference 2 > Breakdown of Credit Card Number Theft by Domestic and Overseas Countries

(Units: 100 million Yen, %)

Period	Losses by Leaked Credit Card Information	Breakdown of Leaked Credit Card Information			
		Domestic Loss		Overseas Loss	
		Losses	Proportion	Losses	Proportion
2014 (Jan. to Dec.)	**67.3**	**42.0**	**62.4%**	**25.3**	**37.6%**
2015 (Jan. to Dec.)	**72.2**	**45.7**	**63.3%**	**26.5**	**36.7%**
2016 (Jan. to Dec.)	**88.9**	**54.6**	**61.4%**	**34.3**	**38.6%**
2017 (Jan. to Dec.)	**176.7**	**108.0**	**61.1%**	**68.7**	**38.9%**
2018 (Jan. to Dec.)	**187.6**	**125.2**	**66.7%**	**62.4**	**33.3%**
2019 (Jan. to Dec.)	**222.9**	**152.9**	**68.6%**	**70.0**	**31.4%**
2020 (Jan. to Dec.)	**223.6**	**163.9**	**73.3%**	**59.7**	**26.7%**
(Jan. to Mar.)	49.2	32.9	66.9%	16.3	33.1%
(Apr. to Jun.)	53.2	38.1	71.6%	15.1	28.4%
(Jul. to Sep.)	54.1	41.8	77.3%	12.3	22.7%
(Oct. to Dec.)	67.1	51.1	76.2%	16.0	23.8%
2021 (Jan. to Dec.)	**311.7**	**235.2**	**75.5%**	**76.5**	**24.5%**
(Jan. to Mar.)	68.7	53.5	77.9%	15.2	22.1%
(Apr. to Jun.)	78.1	60.9	78.0%	17.2	22.0%
(Jul. to Sep.)	77.1	55.8	72.4%	21.3	27.6%
(Oct. to Dec.)	87.8	65.0	74.0%	22.8	26.0%

Figure 2, Japan Card Association, Aggregate Results of Credit Card Misuse (News Release)
https://www.j-credit.or.jp/information/statistics/download/toukei_03_g_220331.pdf

Overall view of the Smishing modus operandi

An overview of the actual Smishing techniques observed in the field is shown in Figure 3. This view has not fundamentally changed since the Smishing has emerged.

- **SMS delivery and inducing to fake sites**

A fraudulent SMS is sent to a mobile phone or a smartphone. It contains a URL in the message, and just clicking on it, recipient will find a fake website of a famous brand. When this happens, it can lead to one of the following:

(1) The site asks the user to input user account (ID and password) and personal information such as the credit card number, bank account, security code, etc... with impersonated entry forms of the official brand site.

(2) It asks the user to install a mobile application, which is a malware and infects the phone.

- **Keep a “stepping-stone”**

The primary purpose of a malware infection is to provide the attacker with an SMS sending platform (stepping-stone) for further Smishing. The malware has remote control functionality, where an attacker remotely controls an infected smartphone to send SMSs to desired destinations. Malware infections shouldn't be as important as phishing in nature, but since SMS could not be sent as freely as email, it probably has a “stepping-stone” as a source. In fact, many cases of Smishing that appear to originate from malware-infected smartphones have been identified in Japan.

- **Execution**

Actors will get financial gain by unauthorized access to the target sites with IDs and passwords exploited by fake sites. Similarly, fraudulent payments using exploited credit card information on on-line shops are another modus operandi. The brands targeted by Smishing vary, but the targeted information is almost the same such as bank accounts, EC website accounts, electronic payments, and credit card information. In addition, the purpose of the exploited information is not only to be misused, but also to be sold (bought) on black markets. Credit card information, in particular, is targeted and will be discussed in more detail later in this article.

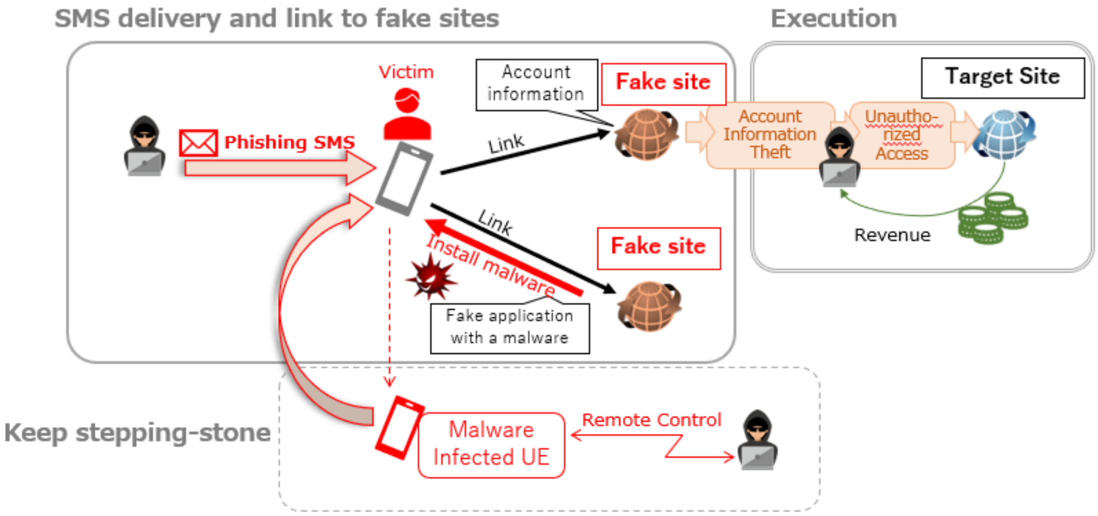


Figure 3. Smishing techniques

The role and characteristics of SMS in phishing

SMS, which has developed as a basic feature of mobile phones, has different characteristics from email and messaging apps, and this is evident in the features of scams.

1. SMS is delivered directly to the phone you carry every day
2. The address is a phone number associated with an individual.
3. Using control signals instead of the data transmission so that always reliably be delivered to subscribers.
4. Subscribers tend to open the SMS in a reflective action.
5. Tend to be believed, hard to distinguish and easy to click.

We will explain details of each items.

1. SMS is delivered directly to the phone you carry every day

SMS (Short Messaging Service) began to be commercialized in the 1990s as GSM Standard [1] and was adopted as a basic feature of mobile phones worldwide. It spread in Europe and the United States as a short-form communication tool, and in Japan since 2001, when the WCDMA standard was adopted in 3G, it became popular. Even when smartphones become mainstream, SMS will continue to be implemented as standard features. Although it is an old technology that has been in development for 30 years, it is still being used in the latest 5G devices and is expected to continue to be used.

Smartphones have a level of penetration equal to the necessities of life, and almost everyone in the economy always carries them around. Therefore, SMS is an effective way for criminals to reach a wide range of people to receive their scam messages, delivered, and opened.

2. The address is a phone number associated with an individual

The phone number, also known as MSISDN[2], is issued through a line contract with a telephone carrier ("carrier"). And, in effect, phone number means subscriber (specific individual). Especially, since mobile phones are owned by individuals, the link between a phone number and an individual is strong. Since SMS is sent to a phone number, it is more certain to reach the specific person targeted than by email. This feature is used for phone identity verification, multi-factor authentication using SMS, etc., but unfortunately it is also used for Smishing crimes.

Although there are fewer opportunities to be aware of phone numbers on a daily basis, such as the spread of talk and chat through apps, and the ability to make phone calls by simply tapping on the name in the address book, the strength of this "phone number = specific individual" association needs to be understood in terms of anti-smishing measures (Figure 4).

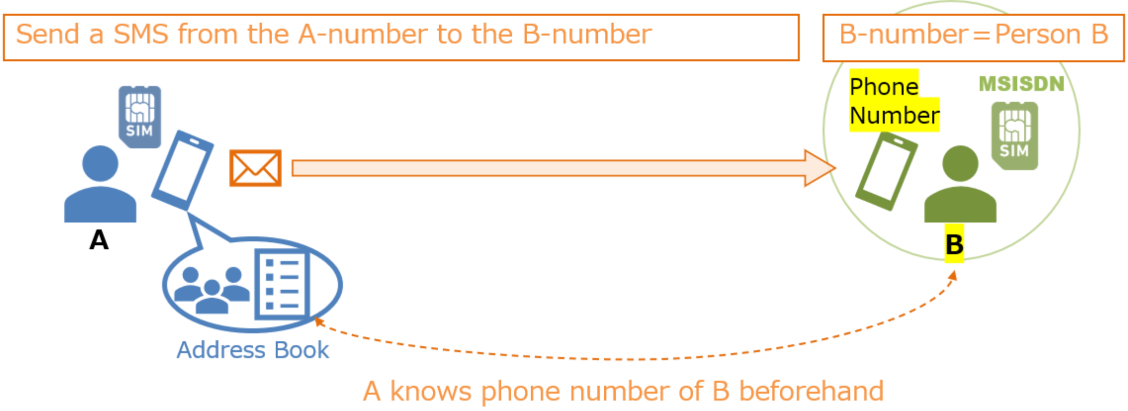

Send a SMS from the A-number to the B-number
B-number＝Person B
SIM
A
Phone Number
MSISDN
SIM
B
Address Book
A knows phone number of B beforehand

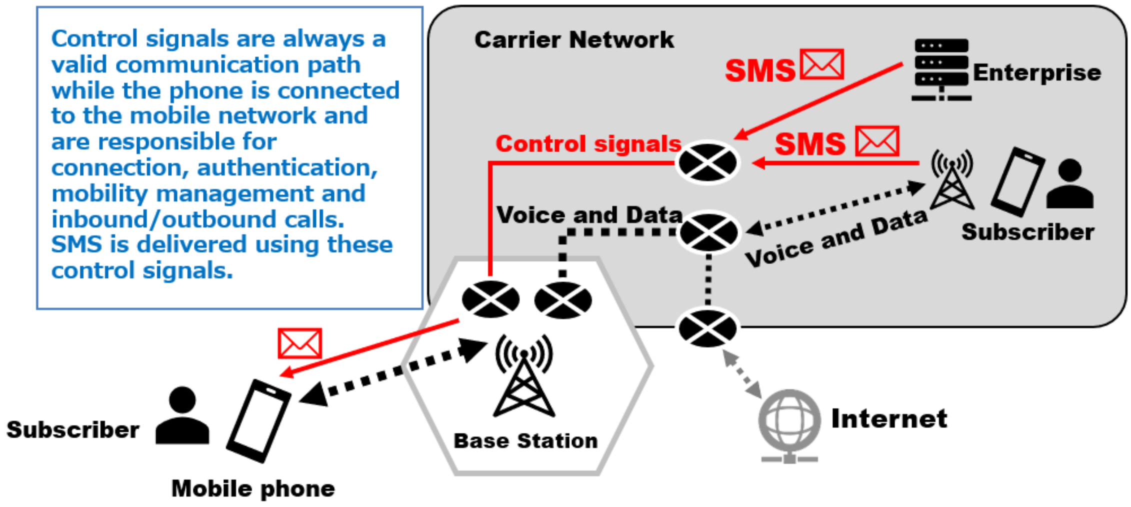
Figure 4. Phone number is associated with an individual

3. Using control signals instead of the mobile data transmission so that always reliably received

SMS is delivered using control signals instead of using normal data communications (so-called packet plans). Control signals are the basic mechanism of a mobile phone technology and are responsible for connecting to a carrier network through a base station - authentication, making and receiving calls, switching between connecting stations while the mobile phone moving (handover) -. (Figure 5)

Even if the user is not on a call nor using the Internet, control signals are always exchanged while the terminal is attached to the carrier network and SMS can be always received. In addition, SMS is delivered by a push method sent from the carrier network side instead of pulling it from the terminal side. Farther more, control signals are carried on a standard protocol called SS7/SIGTRAN[3], which connects to cellular networks around the world. This allows SMS to be delivered from anywhere in the world, if specifies a destination phone number.

By using SMS in this way, messages can be certainly delivered to specific individuals at the sender's preferred timing by mechanism of the mobile communication.



Control signals are always a valid communication path while the phone is connected to the mobile network and are responsible for connection, authentication, mobility management and inbound/outbound calls. SMS is delivered using these control signals.

Figure 5. SMS is using control signals and always receivable

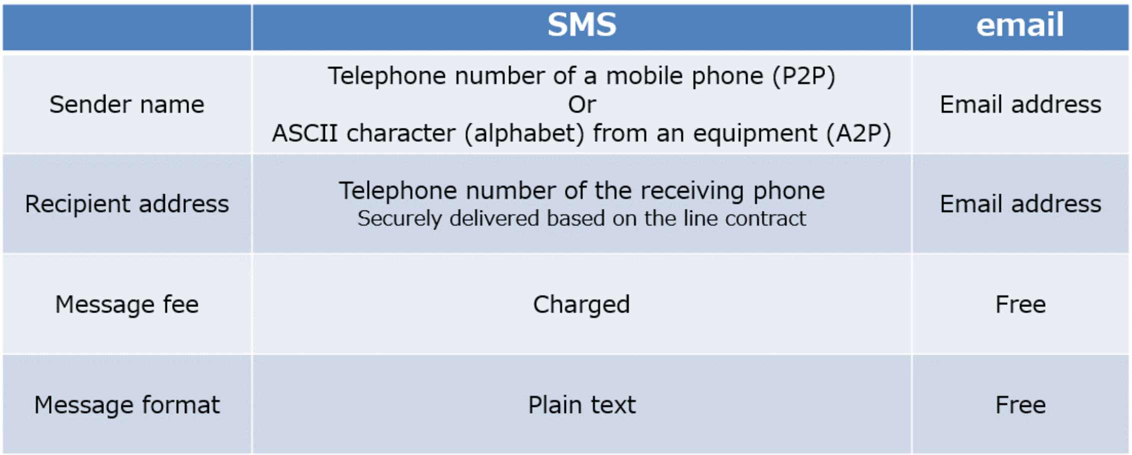
4. Subscribers tend to open the SMS in a reflective action

SMS is a basic feature of mobile phones, and like incoming calls, it provides a visual notification to the user at the moment of the SMS received.

Also, due to the limitation of the number of characters in a message by the specification (160 English and 70 Japanese characters in a message, basically), only short sentences can be sent. Inevitably, the message become simple and clear, and easier to react reflexively.

5. Tend to be believed, hard to distinguish and easy to click.

Even legitimate SMS from companies and public institutions are written in simple and clear texts due to message length constraints, and short URL is also used. Even if the message is uncomfortably short and abrupt for the E-mail, it is a common expression in SMS, and it is hard to suspect Smishing just from the text itself. Even if you look at the text closely with suspicion, it is difficult to discern a fraudulent message that is created by copying a legitimate message. What's more, the actual message for you to inform from both the Smishing and the legitimate message are written on the website you're directed to (a text that makes you feel like it), can lead to reflexive clicks.



	SMS	email
Sender name	Telephone number of a mobile phone (P2P) Or ASCII character (alphabet) from an equipment (A2P)	Email address
Recipient address	Telephone number of the receiving phone Securely delivered based on the line contract	Email address
Message fee	Charged	Free
Message format	Plain text	Free

Figure 6. Differences between SMS and E-mail

SMS sources and reach paths: Exploitation technique for Smishing

The source and route of SMS transmission are unique in cellular networks. Understanding it and knowing how it is misused for Smishing is important for planning countermeasures. The SMS source and reach path are shown in Figure 7. The source and route of the Smishing were also illustrated in it for better understanding.

• SMS Source and Reach Path

SMS is used for communication between mobile phone users as well as for corporate advertising and announcements. As with telephone calls, you can send and receive SMS messages to and from another carrier subscribers, and you can also receive SMS messages from overseas carrier users and corporations. Technically, it can be organized as follows:

○ Home network and other networks

From the viewpoint of the SMS recipient Mr. A, "Home network" refers to the network of the domestic carrier company A to which Mr. A belongs. Other networks are networks of other companies other than Company A.

SMS sources are divided into two types: local (e.g., senders on the home network) and remote (e.g., senders on the other networks). No matter where the SMS comes from, each SMS is always delivered to A through the home network.

○ P2P/A2P

SMS exchanged between subscriber terminals is called "P2P (Person to Person)". On the other hand, SMS sent from applications other than subscriber terminals for purposes such as advertising is called

"A2P (Application to Person)". P2P comes from another user on your home network and from another user on another network. A2P comes from corporate connections on your home network and from overseas carriers.

○ Corporate connections

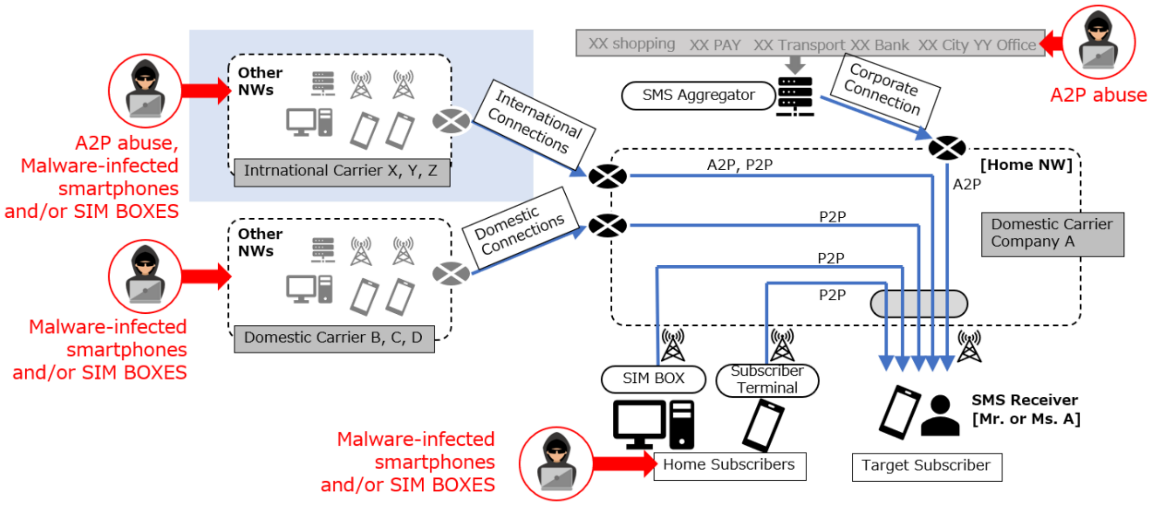
This is a special interface for businesses to send ads, notifications, etc., via A2P SMS. Also referred to as corporate connection service or A2P service, it can send SMS from a computer such as a server. Companies that send SMS either sign an individual contract with the carrier for corporate connection or use SMS delivery service of SMS Aggregators.

○ Domestic connections

Interconnection with domestic carriers. The control signals described in Fig.5 are exchanged between carriers so that calls and SMS can be received no matter where the other party is. For SMS, it is basically responsible for P2P exchanges with subscribers to other networks. In Japan, carriers do not transfer A2P SMS to other networks through domestic connections, with each carrier having separate corporate connections (except for individual special contracts between carriers).

○ International connections

Interconnection with overseas carriers. Sending and receiving SMS messages to and from users of overseas carriers. A2P SMSs are also transferred through these connections as well as P2P. For this reason, A2P SMS targeting to Japanese users can arrive from international connections. A typical example of legitimate use of this case are SMS notifications and multi-factor authentication.



XX shopping XX PAY XX Transport XX Bank XX City YY Office
A2P abuse
SMS Aggregator
Corporate Connection
Other NWs
Intrnational Carrier X, Y, Z
International Connections
A2P abuse, Malware-infected smartphones and/or SIM BOXES
A2P, P2P
[Home NW]
A2P
Domestic Carrier Company A
Other NWs
Domestic Connections
P2P
P2P
P2P
Domestic Carrier B, C, D
Malware-infected smartphones and/or SIM BOXES
SIM BOX
Subscriber Terminal
SMS Receiver [Mr. or Ms. A]
Malware-infected smartphones and/or SIM BOXES
Home Subscribers
Target Subscriber

Figure 7. SMS sources and Reach Paths

Modus operandi of Smishing transmission

The sources of the Smishing are also shown in Figure 7. Any legitimate means of SMS transmission can be used for Smishing, but in addition, there are informal/fraudulent methods of transmission. Those transmission methods are as follows:

A2P abuse: To use official route to send SMS from computer

Since the use of a computer to send SMS gives a high degree of flexibility, therefore, A2P official service is also subject to malicious use for Smishing. Similar mechanisms exist around the world for A2P services and SMS aggregators, and there are variation of the service content, flexibility, quality, and administration. For example, there exist some sites overseas where you can easily send SMS messages to Japan from the website screen. There are also some overseas SMS delivery services that allow you to freely set the SMS sender name (that is, to disguise the sender).

Unauthorized connections: some unofficial routes to send SMS from computer

An unofficial route is to send an SMS by illegally connecting to the carrier network. It is widely known among carriers as a security threat and appears in the GSMA Security Guidelines. Articles about trading of illegal connections on the dark web are also available on the Internet.

(Reference: DEEP WEB)

https://www.deepweb-sites.com/dark-web-service-claimed-track-phone-read-text-messages-500-using-ss7/

In addition, suspicious behaviors of unauthorized connections have been observed on international connections among the security surveillance operations supported by Macnica. It is hard to imagine from a Japanese sense of the mobile phone business, but the level of operation, management, and governance execution varies greatly from country to country and region, and in the extreme case, the operation can be done by a system like a small amateur station. In addition to malicious unauthorized connections, there exist other points of connection that can be used for unauthorized connections, either for maintenance or monitoring purposes or due to misconfiguration, and it is currently difficult to completely block those unofficial routes.

Signaling operations of the SS7 protocol can be done via these unauthorized connection points, so not only sending impersonated SMS freely, but other SMS abuses are also possible by interweaving acquisition of subscriber information from the network and abuse of the node equipment. More on this later, as it falls under the category of Telecom Signaling Security, we will explain it at another time, but please be aware that there are unofficial routes that allow attackers to send spoofed SMS freely.

Mobile phone abuse and Sending from malware-infected terminals

It is possible to send a fraudulent SMS from a mobile phone. There are two scenarios.

1. Sending a fraudulent SMS from a mobile phone owned by a criminal

2. Remotely control a malware-infected mobile phone to send a fraudulent SMS

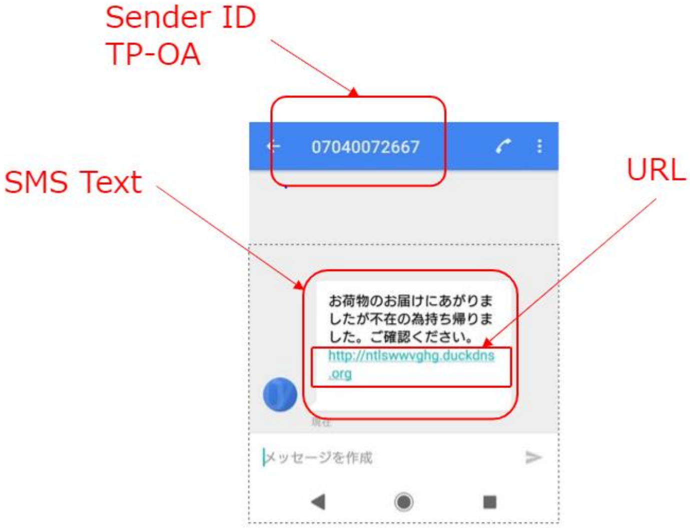
We have observed that malware-infected cases are recently raising, and this is becoming serious.

○ Use of SIM boxes

There is a device called “SIM box” to hold multiple SIM cards within it and connecting to a cellular network. There are small models that can hold 4 or so SIMs, and large models that can hold more than 16 SIMs and can operate as a mobile terminal by themselves, and models that connect to a PC via a USB connection. A typical example is a SIM box installed in Japan that bypasses international roaming charges by sending a signal via the Internet from overseas. But it is also believed to be used to initiate Smishing.

Identification of Smishing delivery routes

We have explained the SMS sources and the route of arrival. By combining this with the SMS sender name constraint, it is possible to identify the route of arrival for incoming Smishing (and SMS in general). Once a route is identified, it can be used to distinguish Smishing from legitimate SMS in the countermeasures described later. It is explained below.



07040072667

お荷物のお届けにあがりましたが不在の為持ち帰りました。ご確認ください。 http://ntlswwvghg.duckdns.org

現在

Figure 8. Names of Smishing SMS parts

- ### SMS sender name constraints

When you receive a SMS, the brand name or phone number information appears in the SMS sender name field (Figure 8). The information contained in the TP-OA field of the signaling protocol is exactly displayed here. The SMS sender name looks seemingly free but not so much actually. The restrictions are as follows:

○ Protocol specifications

By design, the Sender Name field (TP-OA) can contain an ASCII string (3 GPP TS 23.040 9.1.2.4 Alphanumeric representation). In practice, the following operational restrictions apply, and the characters that can be used (characters that can be delivered) are further limited depending on the transmission method.

○ Sending SMS from a mobile phone (P2P message)

For P2P case, the caller ID (phone number/MSISDN) is automatically embedded as the sender name. It is impossible for the user to change it arbitrarily, but the phone number recorded in the SIM card will be adopted.

The notation is only by numbers and follows the phone numbering system (0 -9 combination to within 12 digits, see 3 GPP TS 23.040). For this reason, SMS messages sent from domestic subscribers are always sent with a domestic number in the sender name, and those sent from overseas subscribers are sent with an international number. All other patterns of the phone number notations appear only by the impersonation of the sender name, but those patterns cannot be sent from mobile phones.

○ Sending from a computer, etc. (A2P message)

As per the protocol specification, any ASCII character, including alphabets, can be used for the sender name. It is common to use a company name or brand name as the sender name, but operational restrictions such as the type of words and letters that can be used vary by country, region and carrier.

All SMS messages received in Japan which have sender names other than the mobile phone number are sent from A2P. You can use alphabets and numbers, but in particular, only official SMS's agreed with your carrier in advance are allowed to use alphabetic company names (such as "NTT DOCOMO"), short numbers and specific phone numbers, and you can send such SMS only through official channels (such as aggregators) that you have contracted in advance. Conversely, any SMS with an alphabetic, symbolic, or numeric sender name that is not in agreement with the carrier considered to be flowing in from an international connection.

• Route identification using sender name constraints

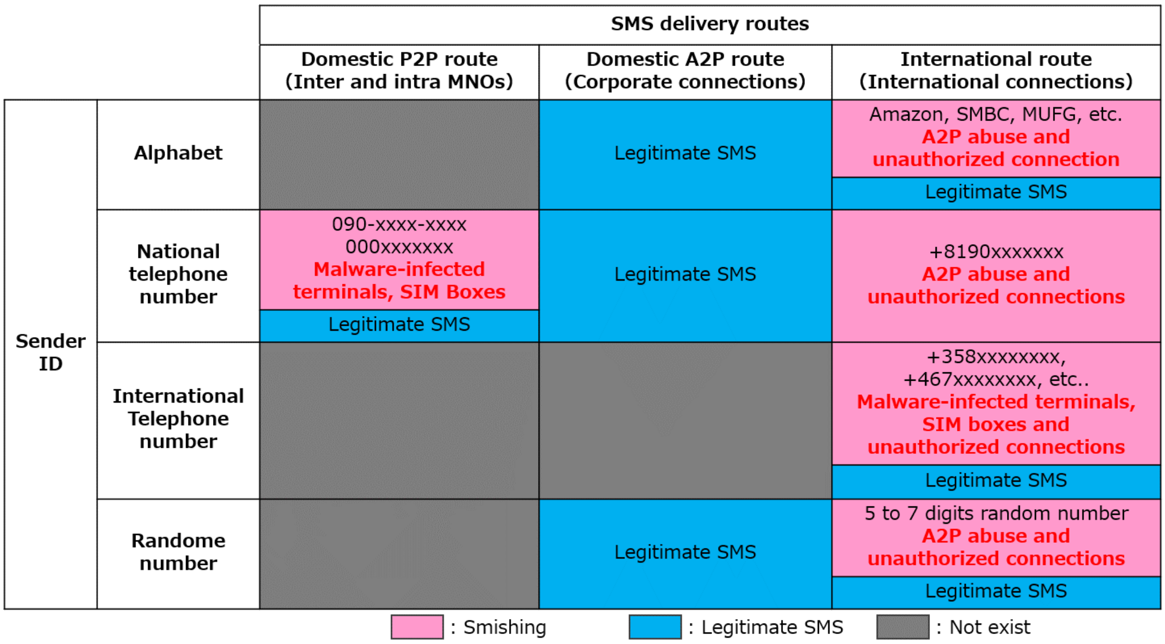
Based on the above, it is possible to identify the route of the Smishing by sender name - the main source (Fig. 9). The actual observed Smishing cases are shaded in pink.

Domestic A2P is strictly controlled, and malicious use such as Smishing is quite difficult: For companies spoofed their names (alphabets) in sender name of Smishing, it is unlikely to think those SMS are sent from the domestic A2P route.

Within the country, it is possible to send subscriber number initiated (P2P) Smishing. From the observed trend, most of them seemed to send from malware-infected terminals. Well-known case is the home-delivery Smishing (described later).

On the other hand, there is always a large amount of Smishing coming from international connection routes, and they have wide variety of sender names. Following types of sender names are often observed.

- alphabet
- International phone numbers
- Random digits (not phone numbers)



		SMS delivery routes		
		Domestic P2P route (Inter and intra MNOs)	**Domestic A2P route (Corporate connections)**	**International route (International connections)**
Sender ID	**Alphabet**	⬛	🟦 Legitimate SMS	🟪 Amazon, SMBC, MUFG, etc. **A2P abuse and unauthorized connection** 🟦 Legitimate SMS
	National telephone number	🟪 090-xxxx-xxxx 000xxxxxxx **Malware-infected terminals, SIM Boxes** 🟦 Legitimate SMS	🟦 Legitimate SMS	🟪 +8190xxxxxxx **A2P abuse and unauthorized connections**
	International Telephone number	⬛	⬛	🟪 +358xxxxxxxx, +467xxxxxxxx, etc.. **Malware-infected terminals, SIM boxes and unauthorized connections** 🟦 Legitimate SMS
	Randome number	⬛	🟦 Legitimate SMS	🟪 5 to 7 digits random number **A2P abuse and unauthorized connections** 🟦 Legitimate SMS

🟪 : Smishing 🟦 : Legitimate SMS ⬛ : Not exist

Figure 9. Relationship between SMS sender name and Smishing route

- Existence of SMS aggregators

As mentioned above, the SMS aggregator is used to deliver SMS via A2P. Even for SMS aggregators with Japanese nationality, the actual delivery route may include overseas carriers. Even if a company uses those SMS aggregator to deliver SMS to domestic users, the SMS sender name displayed on the smartphone will be the pattern of the international connection because it flows from the overseas carrier to the Japanese carrier through the international connection (such as overseas phone number or alphabets). Therefore, unlike domestic A2P, which is strictly controlled, it becomes difficult to distinguish between legitimate corporate SMS and Smishing in this case.

Smishing Trends and Technical Considerations

We have been discussing the delivery of Smishing from a technical perspective in so far. Based on these understandings, we will reveal the actual trend of the Smishing.

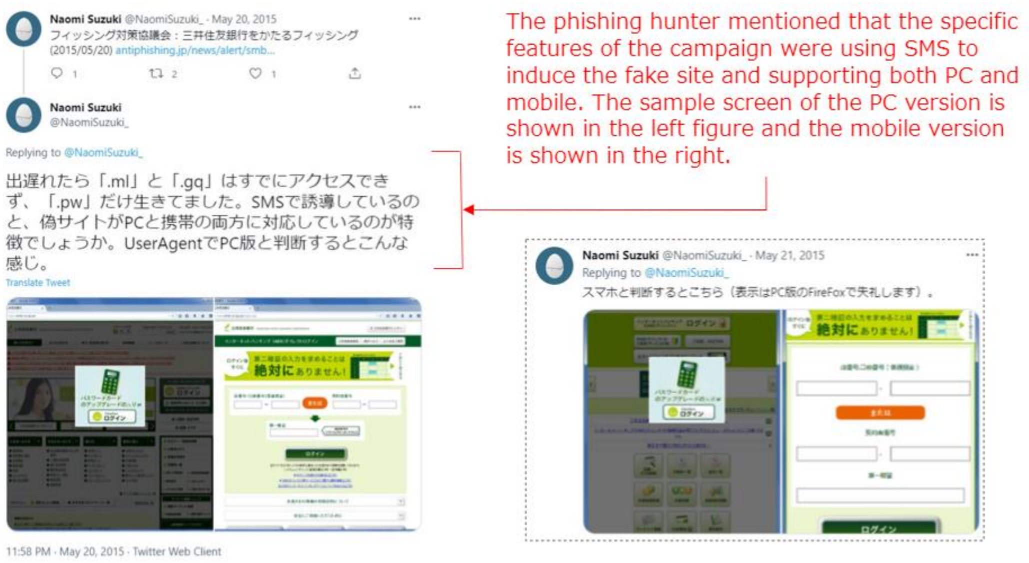
• Trend of modus operandi

○ Dawn of Smishing: Internet banking

While email phishing is rampant, bank phishing has tended to spoof more banks since around 2014. Each bank for attention on its website and news is frequently featured in online articles. You can check out the News Archive of the Council of Anti-Phishing Japan at

https://www.antiphishing.jp/news/alert/.

At that time, there was still no generally recognized way to induce people to malicious site using SMS. In 2015, SMS messages leading to fake sites of mega banks were observed (Figure 10). This campaign brought the line on the issue, however the very use of SMS is still a long way off from becoming a major issue as "Smishing."



Naomi Suzuki @NaomiSuzuki_ · May 20, 2015
フィッシング対策協議会：三井住友銀行をかたるフィッシング (2015/05/20) antiphishing.jp/news/alert/smb...

Naomi Suzuki
@NaomiSuzuki_

Replying to @NaomiSuzuki_

出遅れたら「.ml」と「.gq」はすでにアクセスできず、「.pw」だけ生きてました。SMSで誘導しているのと、偽サイトがPCと携帯の両方に対応しているのが特徴でしょうか。UserAgentでPC版と判断するとこんな感じ。

Translate Tweet

11:58 PM · May 20, 2015 · Twitter Web Client

The phishing hunter mentioned that the specific features of the campaign were using SMS to induce the fake site and supporting both PC and mobile. The sample screen of the PC version is shown in the left figure and the mobile version is shown in the right.

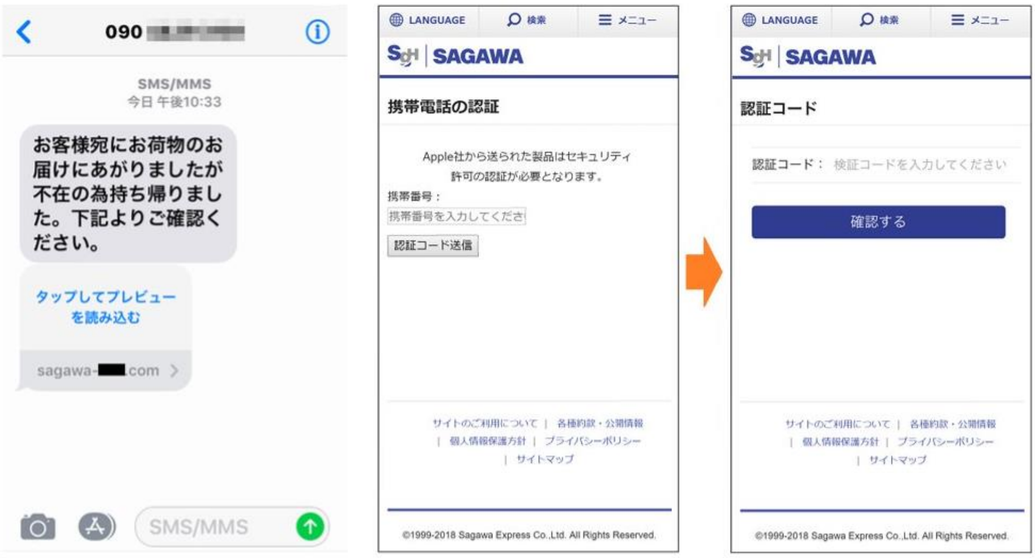
Naomi Suzuki @NaomiSuzuki_ · May 21, 2015
Replying to @NaomiSuzuki_
スマホと判断するとこちら（表示はPC版のFireFoxで失礼します）。

Figure 10. 2015: SMS banking phishing observed (twitter, @NaomiSuzuki_)
https://twitter.com/NaomiSuzuki_/status/601039199291060224

○ Year 2018 -- Home-delivery Smishing

Around this time, the Smishing, both quantitative and topical, became apparent. In addition to exploiting personal information on the fake site by sending SMS impersonated as a home-delivery service, there were methods of inducing recipients to download malware infected applications to their smartphones. Infected smartphones were used as a source of malicious SMS messages, which would lead to more damage in the future.

In the early days, home-delivery Smishing arrived from overseas routes (the sender's name is an overseas phone number, etc.). Later, as the number of infected terminals increased and terminals located in Japan became a stepping-stone for sending SMS, a large number of SMS messages were observed using domestic mobile phone numbers (090~, for example) as the sender's name, and this has continued to the present day. In addition to the SMS text that says, "Your package has been taken home due to your absence," the sender's name is a mobile number, so it is easy to assume that the SMS was sent by a home-delivery driver. Most of them originate from malware-infected devices in the country, but it is also possible to come from SIM boxes or legitimate terminals.



090 [redacted]

SMS/MMS
今日 午後10:33

お客様宛にお荷物のお届けにあがりましたが不在の為持ち帰りました。下記よりご確認ください。

タップしてプレビューを読み込む

sagawa-[redacted].com

The SMS to induce the fake site.

携帯電話の認証

Apple社から送られた製品はセキュリティ許可の認証が必要となります。

携帯番号：携帯番号を入力してくださ

認証コード送信

サイトのご利用について | 各種約款・公開情報 | 個人情報保護方針 | プライバシーポリシー | サイトマップ

©1999-2018 Sagawa Express Co.,Ltd. All Rights Reserved.

The fake site requests the victim to send the phone number for the authentication.

認証コード

認証コード： 検証コードを入力してください

確認する

サイトのご利用について | 各種約款・公開情報 | 個人情報保護方針 | プライバシーポリシー | サイトマップ

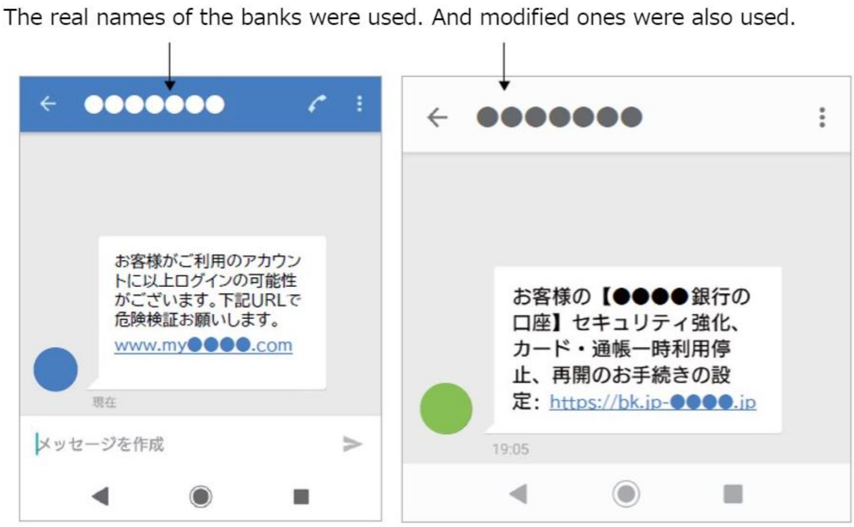
©1999-2018 Sagawa Express Co.,Ltd. All Rights Reserved.

Verification code was sent and the site requests to input the code.

Figure 11. Reported cases of home-delivery smishing reported in 2018 (from News on Phishing archive, Anti-Phishing Council)
https://www.antiphishing.jp/news/alert/sagawa_20180810.html

- ### Year2019: Mobile carriers and bankers Smishing

In 2019, there was a lot of talk about Smishing campaigns to pretend mobile carrier's payments such that charging unpaid fees, and campaigns to pretend banks to steel account information. Fake sender names as "NTT DOCOMO" and "SMBC" increased rapidly. These alphabetic sender names flew from international connections because they were not freely available to third parties in Japan and there was no way to send those spoofed SMSs from inside the country.



The real names of the banks were used. And modified ones were also used.

●●●●●●●

お客様がご利用のアカウントに以上ログインの可能性がございます。下記URLで危険検証お願いします。
www.my●●●●.com

現在

メッセージを作成

●●●●●●●

お客様の【●●●●銀行の口座】セキュリティ強化、カード・通帳一時利用停止、再開のお手続きの設定：https://bk.jp-●●●●.jp

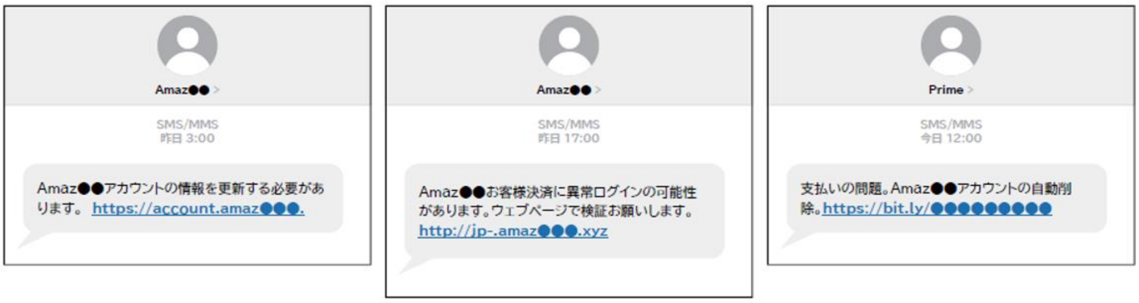
19:05

Figure 12. Example of carrier and bank Smishing observed in 2019

○ Year 2020~: EC and home-delivery Smishing

After that, it calmed down for a while, but flared again around the end of 2020, and from 2021 to 2022, an unprecedented amount of Smishing was observed and continues till now. The contents were mainly about E-commerce companies that pretend major online shopping sites and home-delivery notice. The increase in online shopping demand due to the COVID-19 pandemic was thought to be behind this.

E-commerce sender names were commonly spoofed by EC brands such as "Amazon" around 2020 but have since changed (see below). Delivery services continue to be dominated by SMS originating from domestic mobile phones, and many thoughts to be originated from malware-infected terminals in Japan, and SIM boxes and legitimate terminals could be also the source of them.



Amaz●●

SMS/MMS
昨日 3:00

Amaz●●アカウントの情報を更新する必要があります。 https://account.amaz●●●.

Amaz●●

SMS/MMS
昨日 17:00

Amaz●●お客様決済に異常ログインの可能性があります。ウェブページで検証お願いします。
http://jp-.amaz●●●.xyz

Prime

SMS/MMS
今日 12:00

支払いの問題。Amaz●●アカウントの自動削除。https://bit.ly/●●●●●●●●●

The SMS requests you to update the account information.

The SMS noticed the abnormal log-in on the payment system and ask you to check it on the web page.

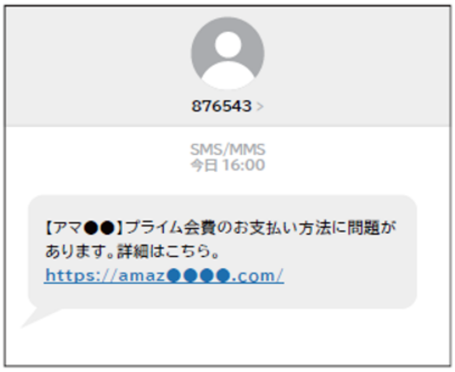
The SMS mentioned there was a problem on your payment and the account will be automatically deleted.

Figure 13. Example of EC Smishing reported in 2020

○ 2021~：More SMS with random number of sender names

The observed trend since 2021 was a sudden increase in the use of random numbers of 5 to 8 digits in sender names. The majority of SMS texts deceive brand names such as EC have been dominant for a long time, and the sender names were changed from alphabetic notation to random numbering. While spoofed brand names are more persuasive, they are also more likely to be blocked by security software and the like, so the intention seemed to use a different number each time to circumvent defenses.

Sender names in random number sequences that do not follow the rules for phone number notation cannot be sent from P2P channel, so A2P seemed to be used, but domestic A2P is not free to use random sequences, so this type should be flew into Japan through international connections.

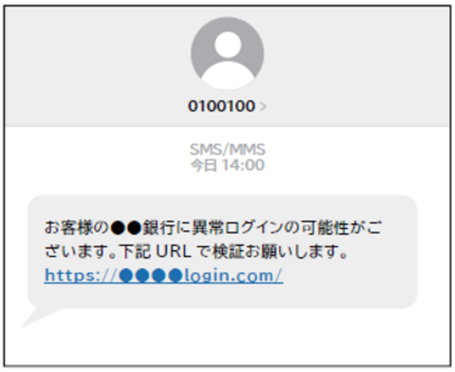


876543 >

SMS/MMS
今日 16:00

【アマ●●】プライム会費のお支払い方法に問題があります。詳細はこちら。
https://amaz●●●●.com/

The SMS mentions a problem with the payment of your prime member’s fee. The sender's name “87654” is an example and it was changed with each SMS message.



0100100 >

SMS/MMS
今日 14:00

お客様の●●銀行に異常ログインの可能性がございます。下記 URL で検証お願いします。
https://●●●●login.com/

The SMS alerts the abnormal log-in to your bank account with strange number of the sender.

Figure 14. Example of a Sender Name with Random Numbers

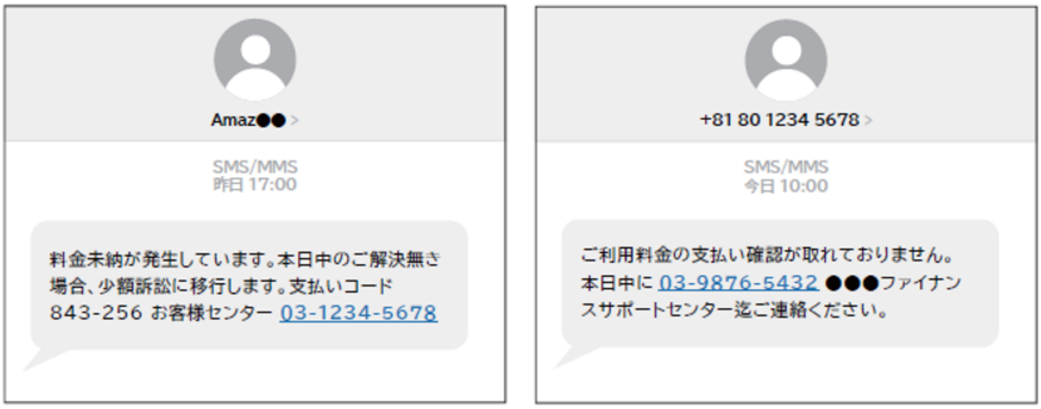
• Transition of the destination domain name

There was also a transition in the domain names used by the fake sites to which the Smishing message directing. From 2018 to 2019, there was a lot of domain names that looked like legitimate brand sites or added letters onto legitimate domains. Also, .xyz, .top and .shop were often used for TLD (Top Level Domain).

Later, when Smishing became a social problem and people started to be cautious about domains that pretend the real ones, shortened URLs (bit.ly, etc.) that were difficult to determine whether they were legitimate or not increased. In addition, the use of DDNS (dynamic DNS), which makes domain tracking difficult, has also increased to avoid take-down of the destination domain. For example, ****.duckdns.org which frequently appeared mainly in the home delivery type of Smishing.

- **Cases of guiding to a phone number**

There is also a type of scam SMS in which the massage includes a phone number instead of a URL and to insist you to call to it. They are classified as so-called “Tokushu-Sagi” meaning special fraud in Japan, and if you call the number within the text, you will be tricked into falling victim to fraud by a clever conversation. This type of fraud has existed since before 2018 and is still prevalent, but it requires a coordinated response, such as setting up a call center. The hurdles for new entrants are high, and it is thought that a conventional special fraud group, which is different from Smishing, is involved. (For example, fraud groups of “Wangiri”)



Amaz●● >

SMS/MMS
昨日 17:00

料金未納が発生しています。本日中のご解決無き場合、少額訴訟に移行します。支払いコード843-256 お客様センター 03-1234-5678

+81 80 1234 5678 >

SMS/MMS
今日 10:00

ご利用料金の支払い確認が取れておりません。本日中に 03-9876-5432 ●●●ファイナンスサポートセンター迄ご連絡ください。

The SMS alerts the unsettled debt and ask you to call the customer center immediately.

The SMS mentioned they cannot find the payment and ask you to call the support center by today.

Figure 15. Case leading to phone number (image)

Changes in attackers, widening the base of crime

We can assume that various attackers (fraudsters, also called Phishers) are behind Smishing. Since its earliest days, bank affiliated Smishing has demonstrated a high level of knowledge, operation, and organization in terms of targeted banks and regions, as well as methods for making illegal withdrawals through certification. It was also estimated that there were more than one group, based on each Smishing’s modus operandi.

In recent years, there has been an increase in the number of Smishings resembling e-commerce and home delivery companies targeting information for credit cards and electronic payments. The total amount of Smishing is increasing, but at the same time, the following types of Smishing are being seen here and there.

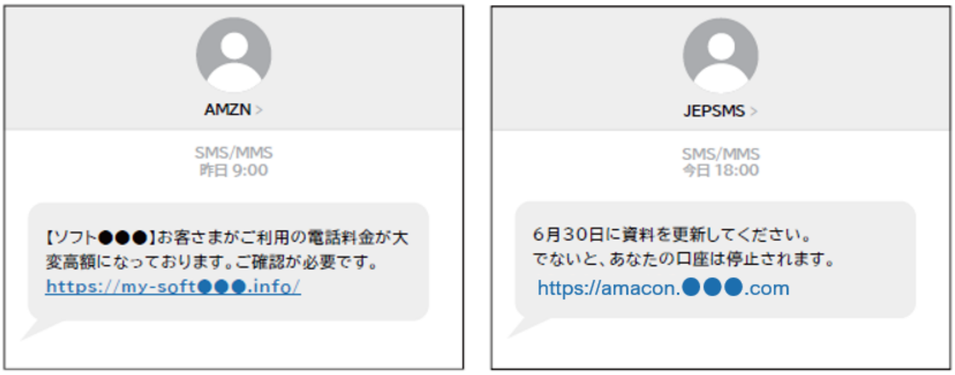
1. The sender name and the impersonated brand in the SMS text do not match

2. The brand of the fake site and the brand of the SMS text do not match

3. Japanese in SMS text is unnatural

In other words, we can infer that there has been a shift in the entry of people with a lower operational level compared to the past or using outsources for operation. We think the background to this is related to the circumstances described in following section.

Figure 16. Low level of operations reported



AMZN >

SMS/MMS
昨日 9:00

【ソフト●●●】お客さまがご利用の電話料金が大変高額になっております。ご確認が必要です。
https://my-soft●●●.info/

JEPSMS >

SMS/MMS
今日 18:00

6月30日に資料を更新してください。
でないと、あなたの口座は停止されます。
https://amacon.●●●.com

Mismatch case of the sender's name and the SMS text.
The sender seams EC site but the contents mentioned about telephone fee.

Unnatural Japanese case.
It asked to update the document on Jun 30th with unnatural Japanese.

- ## Illegal information circulating on the Internet

Information for Smishing is exchanged online and spread as a means of easy money acquisition. In the past, a lot of information related to cybercrime could be observed on the dark web, but now those information flows on the surface web, which can be easily accessed from search sites, etc. SNS and communication apps are also used, and Telegram is a typical example.

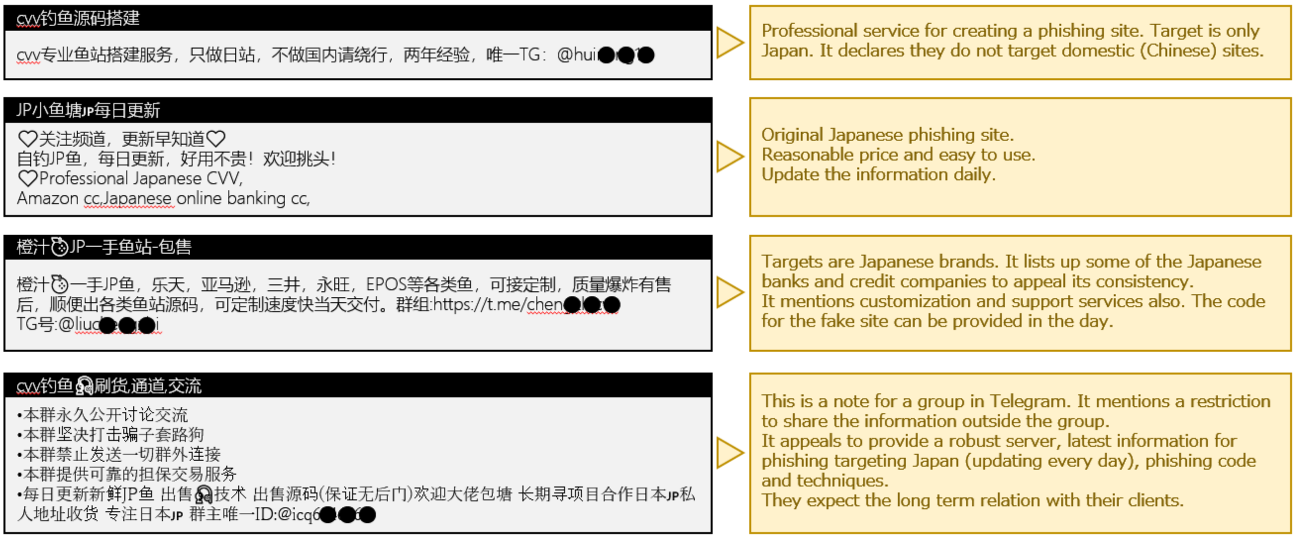
Although Telegram is a chatting tool available on Google Play and the App Store, it is often pointed out in the country that it is used to exchange and solicit information on crime and illegal job offer, while it is characterized by high anonymity. It has been pointed out that Telegram played a major role in a massive SMS phishing campaign in Iran from September to December 2021 resembling the Iranian government.

We won't mention the good or bad of Telegram itself since it is out of the scope of this paper. Any communication tool can be used to commit crimes. The point we want to make here is the reality that information about the crime (or being part of it) is flowing in a place that is accessible to everyone, using widely available means.

- ## Japan is a target

  - ### From Telegram's findings

Information for Smishing targeting Japan is being exchanged on Telegram. There are many channels involved, but with the help of a phishing hunter (@KesagataMe), Macnica investigated and confirmed the contents of 17 channels related Phishing and Smishing targeting Japan (as of the end of 2021). Channel - The purpose and nature of the channel can be read from the blurb presented by the owner. Here are some examples (Figure 17):



cvv钓鱼源码搭建

cvv专业鱼站搭建服务，只做日站，不做国内请绕行，两年经验，唯一TG：@hui[redacted]

Professional service for creating a phishing site. Target is only Japan. It declares they do not target domestic (Chinese) sites.

JP小鱼塘JP每日更新

♡关注频道，更新早知道♡
自钓JP鱼，每日更新，好用不贵！欢迎挑头！
♡Professional Japanese CVV,
Amazon cc,Japanese online banking cc,

Original Japanese phishing site.
Reasonable price and easy to use.
Update the information daily.

橙汁JP一手鱼站-包售

橙汁一手JP鱼，乐天，亚马逊，三井，永旺，EPOS等各类鱼，可接定制，质量爆炸有售后，顺便出各类鱼站源码，可定制速度快当天交付。群组:https://t.me/chen[redacted]
TG号:@liuc[redacted]i

Targets are Japanese brands. It lists up some of the Japanese banks and credit companies to appeal its consistency.
It mentions customization and support services also. The code for the fake site can be provided in the day.

cvv钓鱼刷货,通道,交流

•本群永久公开讨论交流
•本群坚决打击骗子套路狗
•本群禁止发送一切群外连接
•本群提供可靠的担保交易服务
•每日更新新鲜JP鱼 出售技术 出售源码(保证无后门)欢迎大佬包塘 长期寻项目合作日本JP私人地址收货 专注日本JP 群主唯一ID:@icq6[redacted]

This is a note for a group in Telegram. It mentions a restriction to share the information outside the group.
It appeals to provide a robust server, latest information for phishing targeting Japan (updating every day), phishing code and techniques.
They expect the long term relation with their clients.

Figure 17. Example of Telegram channel targeting Japan

- There are Major Japanese e-commerce sites, city banks and card brands listed.
- Source code of the fake sites are available and can be handed over on the day. Supports and customization services are also available.
- There are some sites dedicated to exploit card information, and Japan is targeted.
- They claim the freshness, low price, and quality of information.

In contact with the channel owners, we also got the following information (only part is shown):

- The source code of a certain major bank's phishing site is available for less than 1,000 Chinese yuan.
- The 24-hour unlimited SMS sending offer is 100 Chinese yuan or less.
- Illegally purchased products can be sold (ex. Japanese gaming consoles, Apple products and branded clothes and shoes).

- **On other websites**

In addition to Telegram, a significant amount of information about Smishing is circulated on the website and can be reached by searching the Internet. Some examples include:

- Information for the sale, purchase or misuse of credit card information (called "Carding").

Example) "Sell cvv US-UK-US-CA-EU-ASIA-dump 12 2022 FULL fresh all country"
hxxp://scandinavian-va[.]net/forums/index-.php?/topic/12551-sell-cvv-us-uk-aus-ca-eu-asia-dump12-2022-full-fresh-all-country/

- A list of Japanese mobile phone numbers with related information. It claims freshness and is likely updated frequently.

Example) “Japan Phone Number List”
hxxps://www.latestdatabase[.]com/japan-phone-number-list/

- There are also video contents on how to do phishing and carding.

Example)"BEST SPAMMING TUTORIAL 2021 | SMS SPAMMING 2021 | CARDING TUTORIAL 2021"
hxxps://www[.]youtube[.]com/watch?v=eza3S0pUxGg

Thus, information is circulating on the Internet to carry out the elements of crime, such as Smishing, credit card fraud payments arising from it, and resale of goods. Since anyone can make money by being involved in Smishing, we can assume that the criminal community is expanding, as is real-world fraud.

Ecosystem of the Smishing

Based on information from a series of surveys, we have provided a graphic representation of the Smishing crime ecosystem (Figure 18). Here's an example of a case where credit card information theft is particularly prominent these days.

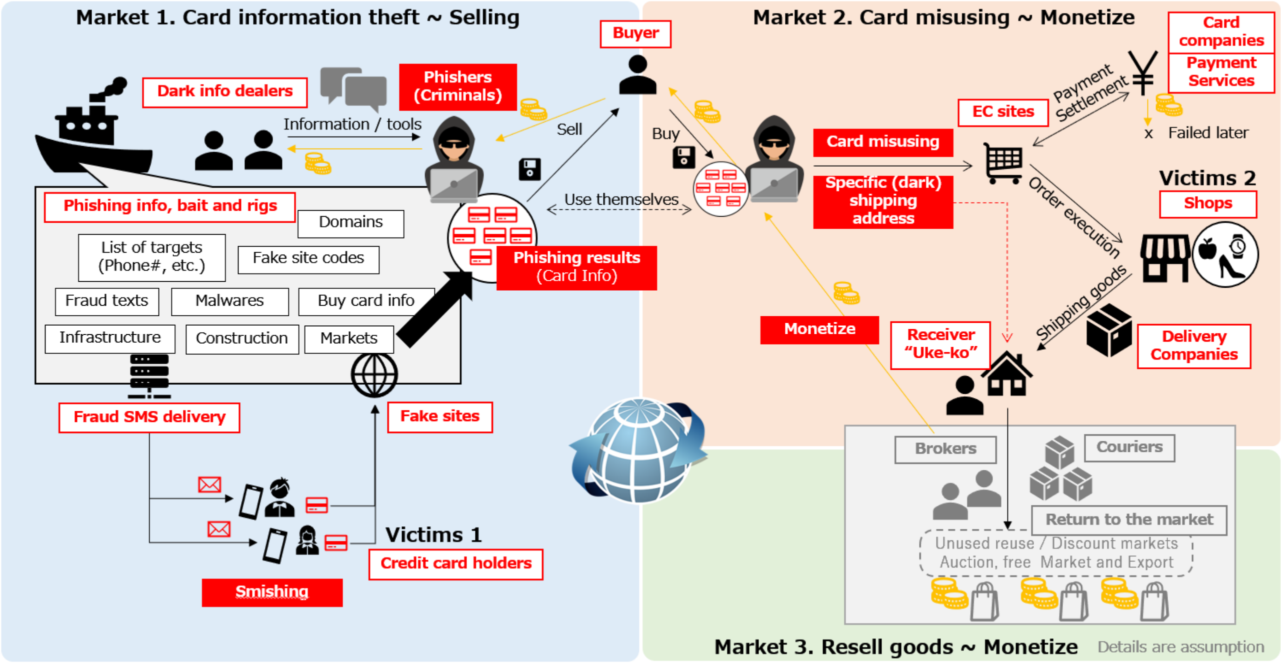


Figure 18. The Smishing Crime Ecosystem

○ Three criminal markets

The ecosystem can be broken down into three major markets.

Market 1: A fraud scheme called Phishing and/or Smishing is used to convert exploited card information into money.

Market 2: Exploited credit card information is misused to resell purchases and convert them into money.

Market 3: Purchase goods and distribute them to the consumer market to earn money.

○ Phishing fraudsters

They are also called Phishers. While there are some high operational level of groups found in banking Smishing, research from Telegram and others shows that credit card Smishing has much wider criminal base and more people are entering Phishing scams for money.

- **Preparing for Smishing**

You'll have instructions on how to create a fake site, source code for the fake site, SMS delivery, a place to sell card information, and where to send items bought by fraudulently using the card. The black market where these trades take place is accessible through Telegram and other means of communication.

You can also buy a list of phone numbers for SMS destinations (targets). Japanese mobile phone lists are sold on foreign websites. The phone number is just a sequence of number, so a brute force attack can be possible, but we don't see brute force or random transmission as a fact observed by Macnica. Basically, they use the listed information for distribution.

- **Execution of Smishing**

Launch a fake site and spread SMS. Depending on the tool, the information entered by the target on the fake site will automatically arrive at a pre-set email address, etc., so the Phishers can catch the card information while they are waiting. Harvesting is likely to depend on the cleverness of the scam and the duration it takes for the fake site to be discovered and be took down. Victims of fraud are individuals who receive SMS and have their card information stolen through fake sites (Victim 1). However, because no real harm can be done just by exploiting the information, and because they are not aware that they have been exploited, it is likely that "Victim 1" is unaware at this stage.

- **Buying and selling information**

Sell credit card information (and credentials required for authentication or payment) that was exploited by Smishing. Phishers earn incomes at this stage. This is where the goal of economic activity in Market 1 to be achieved. It is conceivable that Phishers themselves might go to Market 2 and abuse the card.

- **Credit card fraud ~ purchasing goods**

Credit card information stolen through Phishing is misused here. In real cases, it is a purchasing goods on an EC site, followed by the conversion of the goods into cash. The attacker does not pay for the item at all because the purchase is made using the other person’s credit card stolen. Items should be eligible for purchase if they provide enough gain to cover the cost of obtaining card information. Popular gaming consoles, smartphones, tablets, bags and clothing were recommended in our research. When purchasing goods, attacker's preferred address is specified as the shipping destination.

- **Shipping goods to designated addresses to cash**

Once the payment is settled on the EC site, the purchased goods will be shipped from the shop. The shipping address is not the buyer, but the shipping address obtained from Telegram etc. There are many addresses (receiving points) in Japan those are dedicated for receiving such goods. There is a person who receives packages, commonly called "Uke-ko" in Japanese, meaning “Receiver.” We found that when the pick-up point becomes unavailable due to exposure, such information also flows on Telegram.

After the delivery of the item is completed, the purchaser (fraudster) of the item is expected to receive the payment after some sort of confirmation, but as we are just investigating them, we hold explanation to this point.

If credit card fraud is found after the item is shipped, the card user is protected, but instead, the card company does not settle the payment to the shop where the product was sold. The shop will lose the product with no sales. This is also the problem, and they are the "Victims 2".

- **To flow back goods to the consumer market**

We believe that products are being returned to the consumer market in some form and are being cashed out (Market 3). This area is not investigated by Macnica, but we believe it has something to do with the traditional mechanism proceeding to the era of Smishing that allows disposals, stolen goods and other ill-gotten goods obtained through other channels to flow back to the market.

Countermeasure approach

A better understanding and consideration of the criminal ecosystem around Smishing (Fig. 18) will enable us to take action in a holistic way. Until now, early detection of phishing sites and take-downs (or virtually detoxifying by access blocking) have been the focus of anti-phishing efforts. These will continue to be effective, but it will also be important to combine upstream and downstream measures to break the chain of criminal activity. The following are our thoughts of consideration.

Anti-Smishing Framework

When considering countermeasures, we define a framework that follows the flow of Smishing (Figure 19). The center icons represent the order of the Smishing crime from left to right. The boxes on them indicate measures that companies in the ecosystem can take individually, and the boxes on the bottom indicate measures that companies can take together. Each measure is explained below.

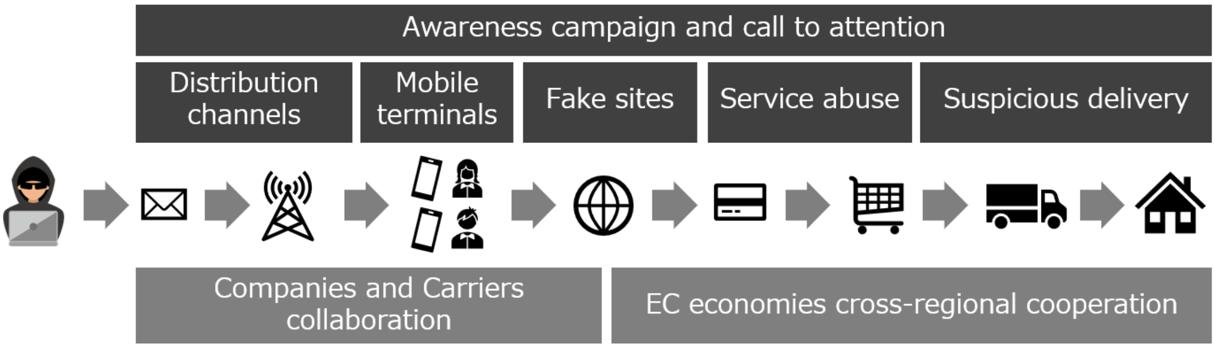

Awareness campaign and call to attention
Distribution channels
Mobile terminals
Fake sites
Service abuse
Suspicious delivery
Companies and Carriers collaboration
EC economies cross-regional cooperation

Figure 19. Anti-Smishing Framework

○ Measures against distribution channels

The SMS delivery network provider will take measures to prevent fraudulent SMS from reaching the recipient. Make rigorous rule to use SMS services and/or implement Smishing detection and filtering techniques are effective. The route from SMS transmission to reception is operated by the telecommunication carrier and for this reason, most of the distribution channel measures will be carried out by carriers. However, there are challenges in practice.

Personal rights - Secrecy of communications for privacy purposes (Article 21 of the Constitution and the Telecommunications Business Act in Japan) greatly limits how carriers can distinguish and filter Smishing on the delivery network side. Carriers clearly fall under the category of "telecommunications carriers" in the above laws, and therefore, they are not able to identify and distinguish SMS in an easy way to screen and block Smishing. In addition, communications reachability is a carrier's mission. Unless malicious SMS can be accurately identified, it can lead to poor reachability due to excessive filtering, leading to claims and service failures. In this way, it is important to understand the roles and responsibilities that are placed on careers in order to consider effective countermeasures.

Japanese carriers have a high level of awareness of the issue of Smishing and have conducted various discussions and exchanges of views. Due to the tremendous efforts of carriers and the consultations with ministries, we have started to do a little more these days. Major carriers in Japan are promoting the introduction of SMS firewall filtering, and some of them have been effective since March 2022. This is a highly effective method if properly operated because it blocks Smishing before it reaches the user's terminal.

To increase the effectiveness of filtering, we need to accumulate operational know-how in the future. It is also important for legitimate brands, SMS users, SMS aggregators, and carriers to work together to improve accuracy so that they can filter accurately and avoid false blockages (see below). Macnica will work with related companies to promote distribution channel measures.

○ Mobile Terminal measures

There are two type of measures that can be implemented on the mobile terminal.

(1) Measures against leading victims to fake sites

(2) Anti-Malware

Currently, measures mainly on Safe Browsing are in progress for (1). It identifies dangerous sites from domain names and URLs and blocks (and warns) access. Reports and declarations from each company regarding such dangerous sites are useful for this purpose. It is important to input information from the company side along with the domain abuse declaration. However, it is not effective for a large number of domains containing random strings.

There is also a smartphone app that identifies unwanted calls/SMS from the sender's name and displays a warning when receiving an SMS. In addition, improvements to the SMS app make it technically possible to disable links or not jump to URLs in text or call phone numbers in a single operation. To popularizing these apps themselves, features improvements, DB enhancements, and more can help.

(2) includes antivirus software and security packs provided by carriers. Their improvements in functionality and detection performance are important. In addition to the measures to be taken on the terminal in use, there are also measures that can be taken by the company. There are technologies that can automatically detect the distribution of fake apps that impersonate specific

company's official apps. These technologies can be used for Smishing measure (anti-malware) while increasing brand credibility.

From the point of view of developing mobile apps, measures on the terminal should also be considered, such as improving functions (such as the API of the OS) that are likely to be exploited as malware, tightening the execution authority, and tightening the method of distributing apps and installation. However, balancing safety with ease and flexibility of app development and the impact on freedom and fairness in the app market is likely to be a debate.

○ Countermeasures against fake sites

Thanks in part to the efforts of the phishing hunters, new patterns of Smishing are being detected and shared early. And from there, fake sites are quickly taken down, and quickly applied to safe browsing. It is vital that we continue to promote these.

Fishers are trying to avoid countermeasures. Domain names they use for fake sites are becoming more diverse and short-lived, with shortened URLs, dynamic DNS (DDNS), and mass generation, including random strings. It is important to speed up and automate the findings to take-down (detoxification) cycles. Some companies are already working on finding fake sites that duplicate their own brands, and others are working on automation, including take-down requests to the site administrators. It is hoped that more companies and organizations will use these examples and experiences to promote measures.

It is also technically possible to block access to fake sites at the DNS level. When accessing a site from a terminal, we use a mechanism (name resolution by DNS) that links URL notation (just a string of characters) to the real IP address, but when accessing a fake site, do not solve the name to IP translation, for example. Discussions need to be made in terms of public nature and transparency, but it is worth considering as a measure to induce fake sites. The EU is studying "DNS4EU," which is expected as a security measure such as filtering in the DNS resolver area in addition to privacy protection. This kind of movement by other countries can be helpful.

https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/cef-dig-2021-cloud-dns-works

○ Measures against unauthorized use

Fail the attempt of the criminals to misuse victim's account or card information. It can be divided into two major categories to realize them.

(1) Measures against unauthorized logins

(2) Measures against malicious behavior (including fraud account creation)

The login authentication is being enhanced nowadays, and it should be required to work on continuously. In addition, in recent years, behavior-based detection technologies have been refined. Even if the user-ID and password match, it is also possible to detect differences of behavior from when the actual person logs in with other factors and, if something detected, request additional authentication steps. Authentication itself has also begun without passwords. It is a challenging topic to balance user experience and security, but technology development will likely to be continued. It is also worth considering the introduction of such new technologies.

To find malicious behavior on the site are also effective. For example, a criminal's failure to create a new account to use illegally obtained information can lead to crime prevention. It is possible to assess the risk of multiple accounts being created with the same information, and to assess the similarity between the information registered at the time of account creation and past unauthorized users. You can consider measures such as additional identity verification according to the level of risk or deleting accounts if necessary.

Even though an actor successfully impersonated and logged-in, it is possible to detect abuse of service based on the behavior. Even if we could not identify the fraud completely, we can add stricter procedures for checking out or making payments, and/or requiring additional authentication when a suspicious user behavior found, etc.

In this way, criminals are more likely to abandon the activity by adding unpredictable elements in the middle of the act of them. It is also a challenge for this type of measure to balance user convenience and comfort with security when using the site.

○ Measures on suspicious delivery

Items ordered through credit card fraud are shipped to addresses linked to criminals. The recipient, commonly called "Uke-ko," in Japanese, receives the goods. There are cases where such an address is given on the EC site when purchasing, or where the address is given after the shipment through procedures such as redirecting/forwarding. For the delivery persons, we heard the cases where they feel uncomfortable, such as packages from shops arriving quite frequently, recipients changing frequently, or no one seems to live there. It is possible to translate these findings into measures against crime. In 2021, a case in which the post office noticed an anomaly and arrested a man for burglary of a mansion also made news (Asahi Shimbun Digital, August 7, 2021).

There may not be many things that a shipping company can do on its own, but it is possible to start by sharing information about delivery sites within the company, which can lead to measures such as information exchange between local shipping companies, between delivery companies and post offices, or consultation with local police. In addition, measures can be considered in conjunction with EC sites and shops. The increased risk of detection and the rising cost of crime to establish new delivery destinations can be deterrents for the crime.

○ Awareness campaign and Call to attention

Unlike traditional IT security, there are many victims who have no connection to the IT world, so simply listing cautions on the HP does not raise enough awareness. We should have to be careful to select mediums which can be seen by the potential victims to write a caution. Also, some of the cautions may not be valid claims (e.g., explanation of how to distinguishes fake sites, which is not sufficient and sometimes quite dangerous.) So, it is necessary to reduce such variation in understanding and countermeasures among related companies/specialists. For example, it is effective to share good examples and develop guidelines so that companies that are newly tricked into using their own brand can carry out appropriate cautions.

We also believe that the improvement of people's literacy through awareness campaign will lead to crime deterrence in the medium term. While taking on the role of both awareness and attentions, Macnica will proactively support the awareness campaign of subjects which are difficult for individual companies to deliver.

○ Collaboration between companies and carriers

By combining official services and information of companies and organizations with measures for distribution channels of SMS on the carrier side, more precise identification to filtering can be performed. It will also speed up countermeasures when the company's brand name or organization name is deceived in Smishing. The following types of collaborations can be effective for this purpose.

(1) Limit the "distribution route" of official SMS to domestic corporate routes only.

(2) Limit and clarify the "SMS sender name" used in the official SMS to identifiable patterns.

(3) Limit and clarify the entire URLs and domain names used in the SMS text.

(4) Do not embed URLs in the official SMS. And make it clear to users.

(5) Make it clear whether your brand will use SMS or not in the first place and share the information with carriers in advance.

SMS aggregators also play an important role. For (1) and (2), there are variations in what aggregators can do. It is important to have a good understanding of the SMS delivery routes, sender name characteristics, and Smishing methods described in this paper so that to consider in advance how the company's official SMS delivery is distinguishable from Smishing, and to devise measures to prevent Smishing from using them.

For such collaboration, B2B collaboration window and collaboration schemes will become very important. Macnica will continue to support these efforts.

○ Cross-sector cooperation among EC economies

It is also technically possible to exchange risk information about criminal misuse and wrongdoing online between companies and services. For example, if an EC site can refer to suspicious delivery destination information held by a shipping company, it may be possible to deter and prevent illegal transactions by adding risk assessment in the process of purchase and settlement and alerting before an order is completed, adding authentication, and limiting delivery method options. Similarly, from technical aspects, it is possible to put additional authentication based on a risk score from EC site while card payment approval process. As well, also possible to use the credit status like abuse to evaluate risk score by EC site or payment gateway services.

• Stakeholder collaboration and in-depth discussions are important

The above is a countermeasure approach from a technological perspective. There are many factors that need to be discussed and examined, including industry regulations and legal regulations, before they can be considered in practice. For example, to what extent and how to utilize registration and input information provided by users for security measures. What can be done with the real-time data that can be collected on the site? These directly tie into non-security issues such as privacy issues. But we think it's important not to stop thinking there, but to make an effort to build consensus from the smallest things possible. To this end, it is important not only to think individually, but also to exchange ideas and issues among companies, and to hold in-depth discussions while referring to various practical examples. In fact, carriers have made such efforts that led to the introduction of SMS firewalls in Japan. Even if it is difficult to get a 100% effect, if it is effective to some extent, the cost of cybercrime execution will go up and it will be a deterrent of crimes.

We can say that Anti-Smishing measures are still on the threshold. From now on, Macnica will cooperate in various ways so that we can pool our wisdom and implement more effective measures.

We sincerely hope that in the future we will become a society where citizens can enjoy the convenience of the Internet with peace of mind.

Co.Tomorrowing
MACNICA

Macnica is a technology trading company that partners with many international businesses. We leverage our expertise and research to offer advanced solutions in areas such as security, network infrastructure, AI, and DX. From product implementation to operation and support, we provide comprehensive services to government agencies, educational institutions, and various enterprises. We also have a dedicated research institution focused on studying cyber attacks and countermeasures targeting Japanese companies.

https://www.macnica.com/globalportal/en/home.html