THE CHANGE IN THE METHODS OF SMISHING IN SOUTH-KOREA AFTER THE ONSET OF COVID-19

Yeon-Jun Choi, Kwangju Women's University
Julak Lee, Chung-Ang University

ABSTRACT

This study aims to figure out the change in the techniques of smishing in South Korea after the onset of COVID-19 by identifying smishing modus operandi. Smishing is a serious SMS fraud in which criminals achieve profits by deceiving victims through SMS. Even though the damage of smishing is increasing each day after the onset of COVID-19, there are few papers on the change in the smishing methods after COVID-19. To fill this gap, the researchers collected smishing cases online and employed content analysis and crime script analysis to figure out the modus operandi of smishing in detail. The researchers classified the types of smishing after the start of COVID-19 by utilizing content analysis and identified the progress of smishing through crime script analysis. The findings demonstrated that the modus operandi of smishing in South Korea after COVID-19 consists of pre-preparation, preparation of smishing attack, sending of smishing message, downloading of malicious application onto victims' smartphone & theft of victims' information and storing it, attempt at financial gain through utilization of attained victims' information, charging of transaction/payments to the victims.

Keywords: Smishing, Modus Operandi, Content Analysis, Crime Script Analysis, COVID-19.

INTRODUCTION

With the extension of the COVID-19 pandemic, the whole globe is implementing various policies in order to stop the dissemination of it. For example, the 'Emergency Alert Message Service' is utilized in South-Korea to notify the citizens COVID-19 related information (Institute of Information & Communications Technology Planning & Evaluation, 2021). "Smishing" can be defined as a crime that uses SMS (Short Message Service) to spread malicious code followed on by financial theft from the victims (Park & Ryu, 2018). The percentage of people possessing smartphones is close to 100% in South-Korea (Silver, 2019) and the ratio of the citizens checking their messages is 98% (Kim, 2020). In other words, South-Korea is in an environment that is extremely vulnerable to smishing.

In reality, smishing cases are at a rapid rise because of the abuse of the COVID-19 situation by those with an ill-intention (Jeon, 2020) and with the disperse of the disease, non-physical economic activities have become more common which has contributed towards the sharp increase in the cases of smishing (Hong, 2021; Jeon, 2021; Jung & Chang, 2020; Kim, 2021; Shin, 2021). With the combination of COVID-19 related issues and smishing attacks, it has led to a new type of smishing and these methods have become the norm as a new trend.

Citation Information: Choi, Y.J., & Lee, J. (2021). The change in the methods of smishing in South-Korea after the onset of covid-19. *Journal of Legal, Ethical and Regulatory Issues, 24*(S5), 1-12

According to Choi (2020), in reaction to this phenomenon, the South-Korean government has established and is running a smishing-counteractive team- an indication that the attention on COVID-19 related smishing has risen. Taking all of this into account, it can be said that the need for a research on the change of smishing methods after COVID-19 has increased. However, even with the necessity on the interest and research, the current situation is that there is none as such in the world that has conducted a research professionally on the change in methods with regards to smishing after COVID-19.

Therefore, this paper focuses on the change in smishing criminal methods in South-Korea after the onset of the COVID pandemic. Rather than doing a simple comparison of the smishing methods, the researchers have identified the overall process of how smishing attacks are conducted and through it, find out the effects of COVID-19 on smishing which would allow for a worthwhile research result as well as being effective in reaching the research goals. With this in mind, this research has utilized content analysis and crime scrip analysis as the preferred analysis method in order to identify the change in methods in smishing modus operandi.

LITERATURE REVIEW

Smishing

Smishing is the combination of the word "*SMS*" and "*phishing*" (Joo & Yoon, 2014), which means fraud via SMS. Smishing is a crime where the perpetrator sends content via SMS that catches the victims' attention, thereby luring them to click on the link which results in the installation of a malicious application onto the victims' smartphone (National Police Agency, 2016). This is done with the purpose of stealing the victims' personal information (e.g., ID number, contact number), financial information (e.g., digital accredited certificate, security card) or inflicting financial damage (e.g., loss from minor transaction payments) (National Police Agency, 2016). In addition to this, according to Korea Communications Commission (2021), the number of smishing that KISA (Korea Internet & Security Agency) has investigated in South-Korea in 2020 amounts to 950,843 which is an increase by 2.6 times compared to 2019's 364,000 cases. Even in 2021, an increasing trend was spotted with 7,264 cases in February, 25,710 cases in March, 24,951 cases in April, 40,004 cases in May (Infinigru, 2021).

Phishing is one of the most common forms of method for fraud in this age with the purpose of stealing sensitive information such as credit card information and is increasingly affecting all areas of the industry (Banu & Banu, 2013). Especially, phishing via SMS- smishing- starts by sending SMSs to its targets and in order to lure its victims to click on the link within it, it also contains keywords that are closely related to people's everyday lives (e.g., impersonation of public institutions) (Yeboah-Boateng & Amanor, 2014). This allows them to obtain personal information or financial gain from their victims (Yeboah-Boateng & Amanor, 2014). From this perspective, it can be said that smishing is a type of social engineering method where the sender pretends to be a trustworthy person or institution such as a bank (CEQUENS Team, 2019). Social engineering is normally used to explain duplicity such as information gathering or fraud with its main purpose being swindling or accessing the targeted system (Yeboah-Boateng &

Citation Information: Choi, Y.J., & Lee, J. (2021). The change in the methods of smishing in South-Korea after the onset of covid-19. *Journal of Legal, Ethical and Regulatory Issues, 24*(S5), 1-12

Amanor, 2014). With the proliferation of smartphones and tables, the cases of social engineering is also on the rise which can be a serious threat to all computer users since strictly confidential information such as sensitive, personal information is open to high risk (Yeboah-Boateng & Amanor, 2014). This is especially true since most people nowadays use their phones or PCs to satisfy their bank or stock work and if remote access were to be possible through a smishing attack, it would allow for serious damage since the digital certificate or the memo app that contains personal information or financial information would be exposed (Anti-Fraud Research Society, 2020). As it can be seen from above, smishing is evolving as the day goes on so it is imperative to prepare preventive and counter-active measures diligently through a detailed analysis of smishing since it contains a high level of threat.

Previous Smishing Methods

There are various ways to undergo cyberattacks, but the core principle of most of them is the fact for the need to deceive the other person (Jakobsson, 2018). The same applies to smishing and since criminals can launch phishing attacks against millions of internet users with ease (Luo et al., 2013), different methods are used. As one of the main objectives of this research is to compare and contrast the smishing methods before and after the onset of COVID-19, this section will be looking at the smishing methods before the start of COVID-19.

The following are the common types of smishing methods: delivery-related smishing, family-occasion-related smishing, gift card/coupon-and-present-related smishing, impersonation-of institution smishing, impersonation-of-person smishing (Financial Services Commission, 2020; Hana Bank, 2013). Delivery-related smishing is one of the most common types of smishing with delivery status check, delivery returns, delivery delay being the main content (Financial Services Commission, 2020; Hana Bank, 2013). Family occasion-related smishing usually occurs in the form of mobile invitation such as a wedding invitation (Hana Bank, 2013). With the advancement in the internet and telecommunications technology, mobile invitations have taken off which brought a lot of convenience to the users; this type of smishing came to a rapid rise due to criminals having decided that the mobile invitations were a good medium for smishing attacks. Gift card/coupon-and-present-related smishing sends SMSs with keywords such as “sale”, “free”, “no cost” that’ll entice its readers usually during ChuSeok and the Lunar New Year- Korea’s two most important holiday periods (Financial Services Commission, 2020; Hana Bank, 2013). Impersonation-of-institution smishing usually includes content that allures the victims’ fear where the criminals pretend to be from a public institution, such as the police department, public prosecutor’s office, court or from a financial institution such as a bank (Financial Services Commission, 2020; Hana Bank, 2013). Impersonation-of-person smishing usually occurs in combination with present related smishing where the criminal pretends to be an acquaintance of the victim and wishes to send a present as a gratitude (Financial Services Commission, 2020).

Even though they do not form the common types of smishing, minor-payment-notice smishing, excess-cellular-bill smishing, lude-message smishing, zombie-smartphone smishing also exist (Hana Bank, 2013). Minor-payment-notice smishing and excess-cellular-bill smishing

Citation Information: Choi, Y.J., & Lee, J. (2021). The change in the methods of smishing in South-Korea after the onset of covid-19. *Journal of Legal, Ethical and Regulatory Issues, 24*(S5), 1-12

is a type of smishing to persuade the victims to click on the link in the SMS from the alleged notification service. Lude-message smishing deceives its victims with its sensational message that captivates the human nature of its interest in sexual matters. Zombie-smartphone smishing sends a link without any content with the purpose of drawing the person's curiosity to click on it (Hana Bank, 2013).

There is a need to be aware of the functions of malicious applications since most smishing types fall under the category of luring their victims to click on the link so that the malicious application is installed. The main functions of the malicious application is as follows: deleting and uploading of files, information theft of the device, theft of contacts list, theft of the call list, theft and deletion of SMSs, blocking of incoming phone calls, forwarding of outgoing calls (Alyac1, 2021). As seen from the list, malicious applications can be said to be of a great threat not only because of sensitive information theft from its victims, but as well as acts such as blocking of incoming calls and forwarding of outgoing calls which controls the victims' smartphone.

As mentioned before, most smishing occurs in the form of luring its victims to click on the domain address or URL address in the SMS. However, a different form where an e-mail address or phone number being in the SMS where it suggests the victims to contact the criminals also exists (Mishra & Soni, 2019). This can be said to be an evolved form of smishing with phishing and voice-phishing have been combined together. This type usually entails the victims providing financial and personal information to the criminals which thereby the victims suffer damage (Mishra & Soni, 2019), but prudence is required since a knock-on effect can occur.

METHODS

Data Collection

The smishing-related materials used in this research were collected in the open space. The reason for this is that it is almost impossible for the district police station to come in contact with a victim's case regarding smishing as it has a high rate of hidden crime (Choi & Kim, 2016). Since the topic of this research is the change in methods of smishing in South-Korea after the onset of COVID-19, the websites that Koreans often visit were used for the collection of data. In a survey to find out The Most Often Used Portal Sites, Naver took first place with 74.8%, while Google took second place with 15.8%, followed on by Daum with 7.6% (Opensurvey, 2021). Youtube took the crown with 49.4% for *"The Most Often Used Social Media Application"* (Opensurvey, 2021) - an indication that almost half of the participants used Youtube as their main social media application. This research was conducted based on these rankings where smishing related materials were gathered from the three largest websites (Naver, Daum, and Google) as well as Youtube. The researchers were able to accumulate 280 smishing related precedents by searching words such as "*smishing*", "*SMS phishing*", "SMS *fraud*", "*financial fraud*" from the before mentioned mediums. Korean portal sites provide a separate webpage where users are able to write their personal experience and story and then get advice or legal counselling (Choi et al., 2017). Communication occurring on the internet exhibits the

Citation Information: Choi, Y.J., & Lee, J. (2021). The change in the methods of smishing in South-Korea after the onset of covid-19. *Journal of Legal, Ethical and Regulatory Issues, 24*(S5), 1-12

attributes of anonymity and openness thereby giving a catharsis effect to those who write on it (Na, 2006). From this perspective, when smishing victims write their experience on the internet, they are able to do so quite freely which was helpful in finding out the modus operandi of smishing.

Analytic Strategies

After the collection process as mentioned above and based on it, the researchers continued with a content analysis in order to categorize the different types of smishing crimes. Classifying the keywords related to smishing methods in order to deduce the variety of smishing criminal types after COVID-19 is essential where in this process the content analysis was used. This is a research method which allows for a repetitive and valid deduction from data within a specific context. One of the most suitable data for this is text that accurately reflects the author's opinion and thoughts (Krippendorff, 2018). The datasets used in the following research are reflections from the smishing victims as well as smishing related content published by the highly regarded institution, KISA, when it comes to cyber threats which is effective for doing the content analysis. The standard methods used in the process of analyzing and interpretation are "*comparing", "ordering", "aggregating", "theorizing", "contrasting"* and *"categorizing*", but depending on the nature of the research, more than one of these are applied (Cho, 2005). In fact, in commencing the content analysis in this research, "*categorization*", "*contrast*" and "*comparison*" were mainly used for classifying the smishing criminal methods that occurred after the start of COVID-19.

Alongside a content analysis, a crime script analysis was used in this research. In order to examine the overall process of smishing crimes, a crime scrip analysis was commenced in accordance with the research's purpose and scope. A crime script analysis is an analysis method which measures chronological stage that criminals go through when they commit a crime (Choi et al., 2017) where a crime script comprises what happens before, during and after the event (Hutchings & Holt, 2015). To go in detail, the three main stages of the process are (1) the pre-crime phase: offense planning; (2) the criminal event phase: offense strategies; and (3) the post-offense phase: the aftermath (Beauregard & Leclerc, 2007). There were noticeable changes in the pre-crime phase and the criminal event phase before and after COVID. However, since the post-offense phase consists of the criminal obtaining a financial advantage from its victims and it also does not align with the research's purpose and scope, this research concentrated on the pre-crime phase and criminal event phase when going on with the crime script analysis. Through this method, a cognitive script is able to be drawn up through which future actions can be foreseen so it can be said that it is useful in analysing human behaviour and making predictions of them (Kim & Suh, 2019). The same thing can be said for this research where the modus operandi of smishing was investigated thoroughly as well as the whole process of smishing being analysed systematically through the crime script analysis.

Citation Information: Choi, Y.J., & Lee, J. (2021). The change in the methods of smishing in South-Korea after the onset of covid-19. *Journal of Legal, Ethical and Regulatory Issues, 24*(S5), 1-12

FINDINGS

There is a need to comprehend the overall process of how smishing occurs in order to assess the change of methods in smishing in South-Korea from COVID-19. Taking into consideration of the scope of the collected datasets and the purpose of this research, we have drawn the modus operandi from the pre-crime phase and the criminal event phase.

Pre-Crime Phase

The pre-crime phase means the stage criminals prepare themselves before committing a crime. From the analysis based on the collected materials, the pre-crime phase of smishing can be divided into two stages: criminals go through a pre-information gathering phase and a smishing attack preparation phase before they initiate. The pre-information gathering phase encompasses gathering the personal information of the smishing targets illegally. In this process, criminals pay a certain amount of money and obtain a wide variety of personal information from the brokers. Under the current jurisdiction, it is against the law to trade personal information (Kim, 2019). In essence, crime is already committed from the stage of preparing for a smishing attack. Since including content that will attract the attention of the victims in the SMS is the key to smishing attacks, the latest and trending issues in phishing scenarios(delivery-related scenarios, impersonation-of-institution scenarios, impersonation-of-person scenarios) are already set from the moment of sending the SMSs which ends the pre-information gathering phase.

Next, criminals enter the smishing attack preparation phase which is the foundation phase for the actual smishing attack. First, criminals purchase malicious application or develop them through professionals. This is an indispensable step since the role of malicious applications is vital for smishing attacks. Criminals also need to prepare a server in order to disseminate the malicious applications where they request the professionals for the set-up. Lastly, the criminals upload the malicious applications on the servers mainly being Dropbox, commercial servers such as Amazon or private ones run by themselves. Through this whole process, the pre-crime phase of smishing comes to an end. A table form of this process can be seen in Table 1.

Table 1
Criminal Event Phase

Pre-preparation
Gathering of victims' personal information illegally Construction of various phishing scenarios
↓
Preparation of smishing attack
Arrangement of malicious applications Set-up of dissemination servers Upload of malicious applications

The Criminal event phase entails the criminals moving their plans to action. This phase is initiated by the criminals sending the smishing messages to the victims where the link that

Citation Information: Choi, Y.J., & Lee, J. (2021). The change in the methods of smishing in South-Korea after the onset of covid-19. *Journal of Legal, Ethical and Regulatory Issues, 24*(S5), 1-12

connects to the site with the uploaded malicious application and text that would catch the attention of the victims is included. The link within the message plays an essential role in accessing the victims' smartphone -the reason for being included in the SMS- while the text is drawn upon social issues that would attract the attention of the victims. This smishing process was the one that was affected the most from COVID-19- especially, the text to attract the victims' attention.

According to EST security, the smishing keywords that are used include "*delivery", "finance", "investigation agency", "wedding invitation", "cryptocurrency", "health check-up*" etc. However, with COVID-19, text related to the pandemic were used in smishing attacks on top of the ones mentioned before. When MERS (Middle East Respiratory Syndrome) was an on-going issue back in 2015, content related to MERS was used in smishing attacks (Korea Internet & Security Agency, 2015) and the same phenomenon is occurring with the new COVID-19 related smishing attacks.

Issues related to COVID-19- free give-away of masks, issues related to COVID patients that had been discharged- as well as content related to the policies from the government to counter-act COVID-19- notification of the trail of positive tested COVID patients, disaster relief fund, reservation of vaccines, surveys concerning the vaccines- are used in smishing attacks. Also, quite a number of text has been found that had combined the keyword "*delivery*" and COVID-19 such as SMS stating the delay of delivery due to COVID-19 or impersonation of a particular company for delivering masks. With the increase in the use of delivery due to COVID-19, the before-mentioned smishing has come to light. Since this type of content was not used in smishing, it can be said to be a characteristic of smishing crime after the start of COVID-19.

When criminals undergo a smishing attack, they lure their victims to click the URL within the SMS by incorporating text that would grab their attention- such as social issues. Themes that were readily used for smishing attacks before COVID-19 still persists to this day and recently, new themes arising from the pandemic are often used. Smishing is a form that makes good use of the social issues from the period of phishing messages being sent and its guile is developing as times goes on.

If the victims were to click the link within the SMS after the smishing message had been sent, the malicious application would be downloaded to their smartphones. Most of them have malicious code based on the Android operating system where the criminals are free to take control of the victims' smartphone through the application. The criminals then save the personal information, verification number and sensitive information that is stored on the smartphone at a separate place which ends this phase.

Afterwards, criminals earnestly attempt to steal the financial assets of their victims. In this step, the criminals utilize the personal and financial information they had obtained from their victims in the previous step to purchase items and cyber money. Another way is to remotely control the victims' smartphone through the malicious application so that they take over the verification code in an attempt to go through a transaction in gaming sites. They also purchase online gift cards in mass because it is difficult to track them and it doesn't take much effort to take an unfair advantage by selling the gift cards to the brokers. In recent days, a method of applying for a loan under the victim's name by remotely controlling the financial account

Citation Information: Choi, Y.J., & Lee, J. (2021). The change in the methods of smishing in South-Korea after the onset of covid-19. *Journal of Legal, Ethical and Regulatory Issues, 24*(S5), 1-12

through the malicious application has been developed which is an indication of the progress that had been made in gaining the financial assets of the victims through smishing attacks. Criminals exploit the before mentioned methods in order to attain the financial assets of their victims which they then charge the amount to their victims- ending the criminal event phase. A table form of this process can be seen in Table 2.

Table 2
SENDING OF SMISHING MESSAGE

Sending of smishing message
Insertion of link that will connect to the website where the malicious application is uploaded within the message Inclusion of text that will attract the attention of victims within the message
↓
Download of malicious application onto victim's smartphone & theft and storing of their information
Personal Information (e.g., identification number, phone number) Financial Information (e.g., digital accredited certificate, credit card number, security card number, bank account password) Verification Number Sensitive Information (e.g., location, call records)
↓
Attempt of financial gain through utilization of the stolen victim's information
Purchase of items and cyber money Transaction at gaming sites Purchase of mobile gift cards Application of loans under victim's name
↓
Charging of payments to the victims

DISCUSSION AND CONCLUSION

The main objective of smishing is to lure the target to click the link within the SMS. In other words, criminals need to catch the attention of the victims for their targets to click on the link within the SMS and in order to increase the likelihood, the incorporation of suitable text is essential. Taking a look at the recent smishing occurrences, themes such as COVID-19, cryptocurrency (Bitcoin) were used for this purpose and it can inferred that smishing has the characteristic of utilizing the trending themes of that time.

The South-Korean government has implemented a diverse range of strategies in order to prevent and counter-act the spread of COVID-19 since its start and spread throughout the world. One of these is the "*contact trace data disclosure on people with COVID-19 in South Korea*" where the locations that the patient has been to before and after showing symptoms are notified to the citizens in a way that infringes the patients' privacy the least (Central Disaster and Safety Countermeasure Headquarters Patient Management Team, 2020). So far, this policy was effective in preventing the spread of the pandemic which can be proven by the relatively lower contraction numbers of COVID cases in South-Korea compared to other countries. However, this

Citation Information: Choi, Y.J., & Lee, J. (2021). The change in the methods of smishing in South-Korea after the onset of covid-19. *Journal of Legal, Ethical and Regulatory Issues, 24*(S5), 1-12

has also contributed to the development of smishing methods. Looking at the results from this research, the reason for the development for such new smishing methods is the fact that the ones handing out COVID-19 related information are public institutions which have a high trust rate and issues related to the pandemic are one of the hottest social issues today and this makes it suitable to focus the people's attention.

The previous researches related to the diverse range of phishing modus operandi such as voice-phishing (Choi et al., 2017; Choi & Kim, 2015), romance-scam (Kim & Suh, 2019), smishing (Choi & Kim, 2016) etc. do not reflect the changes from COVID-19 since they were conducted before the pandemic. This is especially true for previous researches handling the overall process of smishing (Choi & Kim, 2016; Joo et al., 2017; Kang et al., 2014; Lee et al., 2014; Mishra & Soni, 2019; Mishra & Soni, 2020; Park et al., 2017) since they were conducted based on the events before the change in smishing methods from COVID-19 which is why this research sets itself apart from the rest as it is based on smishing methods after COVID-19. To be more specific, there were considerable differences in the research results related to the content of the messages. The previous researches state that the modus operandi of smishing consists of the following phases: preparation of the scenario for smishing messages (Choi & Kim, 2016; Kang et al., 2014), sending of smishing messages (Choi & Kim, 2016; Joo et al., 2017; Kang et al., 2014; Lee et al., 2014; Mishra & Soni, 2019; Mishra & Soni, 2020; Park et al., 2017), downloading of malicious application by the victims clicking on the URL (Choi & Kim, 2016; Joo et al., 2017; Kang et al., 2014; Lee et al., 2014; Mishra & Soni, 2019; Mishra & Soni, 2020; Park et al., 2017), taking ill-willed intention to action (Choi & Kim, 2016; Joo et al., 2017; Kang et al., 2014). It could be said that the phase of sending smishing messages and the phase of the malicious application being downloaded by the victims is core to the modus operandi of smishing since they were included in all of the previous researches. This research shares similarity to previous ones as it has included those two critical phases in the modus operandi of smishing.

It was found in this research that the following comprises the modus operandi of smishing in South-Korea after COVID-19: pre-preparation, preparation of smishing attack, sending of smishing message, downloading of malicious application onto victims' smartphone & theft of victims' information and storing it, attempt at financial gain through utilization of attained victims' information, charging of transaction/payments to the victims. Looking at this, the overall process shows a similar flow to previous findings, but there is a key difference in the methods in sending of smishing messages phase: the mechanism of smishing follows suit, but there has been a change in the diversity in the methods after the onset of COVID-19. To explain in more detail, previous researches focus on the delivery-related smishing (Choi & Kim, 2016), impersonation of public institutions smishing(such as a bank, police department, courts of law etc.) (Choi & Kim, 2016; Mishra & Soni, 2019), and impersonation-of-person smishing (Choi & Kim, 2016) while this research was able to find out the rise of new types of smishing such as delivery of free masks, issues regarding discharged COVID patients, notification of number of COVID cases, notification of trail of positively tested COVID patient, emergency disaster fund, reservation of COVID vaccine, surveys related to the vaccines, notification of left-over vaccines.

Citation Information: Choi, Y.J., & Lee, J. (2021). The change in the methods of smishing in South-Korea after the onset of covid-19. *Journal of Legal, Ethical and Regulatory Issues, 24*(S5), 1-12

Through this research it was also found that new types of smishing, where it is a combination of the previously common type and the new types after COVID, have appeared.

In the case of researches done overseas, they had classified the smishing types according to whether a URL, phone number or email ID was included in the smishing message (Mishra & Soni, 2019; Mishra & Soni, 2020). However, only a few accounted that included a phone number of email ID in the smishing message where including the URL was the majority by far in the analyzed results from the smishing datasets in South-Korea in this research. In the event of sending a smishing message with a phone number or email ID, it requires extra work of needing to trick the victims by asking for sensitive information which lowers the chance of success, but sending a smishing message with a URL exempts this additional step which makes it more effective compared to other methods. Taking these points into account, the modus operandi of smishing in this research was discovered based on the smishing messages including a URL and it is also why a more detailed and professional analysis of the modus operandi of smishing in South-Korea was able to be conducted in comparison to earlier researches.

Not only that, but the South-Korean government provides the Emergency Alert Message Service where they are able to deliver COVID-19 related news its citizens without delay, but this service had an influence on smishing since it is provided through the medium of smishing attacks- the SMS. This is especially meaningful in light of the fact that the percentage of people owning a smartphone in Korea being 95%, while owning a phone that is not a smartphone being 5%, in essence the total percentage of owning a phone being close to 100%, makes it the top ranking country in owning smartphones (Silver, 2019) and the percentage of checking the messages is up to 98% among South-Korean citizens after the onset of COVID-19 (Kim, 2020). Therefore, it is safe to say that the probability of smishing occurrences related to the pandemic is much higher than before. Also, the amount of risk can be calculated by the magnitude of influence and the chance of the risk materializing (Yoon, 2011) which is why in can be inferred that that the amount of risk regarding the new types of smishing related to COVID-19 is higher.

Just as smishing methods evolved after COVID-19, it will continue to do so which is why the prevention and counter-measurements need to be developed alongside with it. It can be said the findings of this research is of value since additional alternatives to the prevention and counter-measurements of a more evolved smishing could be suggested based on the modus operandi of smishing from this research. Also, this paper was able to come to light because of the thorough research on the more advanced methods of smishing after COVID-19- the first in its field. As the pandemic has caused mayhem in countries through the globe and the reliance on online mediums has been elevated, the smishing situation will be exacerbated which is why this research will be able to contribute to a certain degree in preventing the harm from it.

REFERENCES

Anti-Fraud Research Society (2020). *The world of fraud*. Pybook.

Banu, M. N., & Banu, S. M. (2013). A comprehensive study of phishing attacks. *International Journal of Computer Science and Information Technologies, 4*(6), 783-786.

Citation Information: Choi, Y.J., & Lee, J. (2021). The change in the methods of smishing in South-Korea after the onset of covid-19. *Journal of Legal, Ethical and Regulatory Issues, 24*(S5), 1-12

Beauregard, E., & Leclerc, B. (2007). An application of the rational choice approach to the offending process of sex offenders: A closer look at the decision-making. *Sexual Abuse: A Journal of Research and Treatment, 19*(2), 115-133.

Central Disaster and Safety Countermeasure Headquarters Patient Management Team. (2020). *Contact trace data disclosure on people with COVID-19 in South Korea*. https://www.tongyeong.go.kr/_res/portal/popup/20201028/cov19.pdf

CEQUENS Team. (2019). *7 Deadly types of SMS fraud*. Retrieved from https://www.cequens.com/story-hub/7-deadly-types-of-sms-fraud

Cho, Y. D. (2005). *A study on the qualitative research methodology of institutional settings*. Kyoyookbook.

Choi, D. H. (2020). New Coronavirus: Smishing and spam mail aimed at anxiety are rampant. *Ajunews*.

Choi, K., & Kim, M. C. (2015). A study on the voice phishing fraud crime for national security and public safety in South Korea: Focus on the its process. *Policejournal, 15*(3), 233-261.

Choi, K., & Kim, M. C. (2016). A study on the modus operandi of smishing crime for public safety. *Convergence Security Journal, 16*(3), 3-12.

Choi, K., Lee, J. L., & Chun, Y. T. (2017). Voice phishing fraud and its modus operandi. *Security Journal, 30*(2), 454-466.

Financial Services Commission. (2020). Watch out for Smishing during the Chuseok holiday. Delete these texts right away. *South Korea Policy Briefing*.

Hana Bank. (2013, November 25). Don't be fooled!... A collection of vulnerable smishing tricks. *Hana 1Q Blog*. Retrieved from https://blog.hanabank.com/345

Hong, J. I. (2021). Smishing jumped 2.6 times last year. Due to the aftermath of the coronavirus, cell phone hacking attempts have been intense. *Yonhapnews*.

Hutchings, A., & Holt, T. J. (2015). A crime script analysis of the online stolen data market. *The British Journal of Criminology, 55*(3), 596-614.

Infinigru. (2021) *Voice phishing analysis report*. Retrieved from https://www.bigdata-policing.kr/policy/contents/policy-etcData.do?schM=view&id=248

Institute of Information & Communications Technology Planning & Evaluation. (2021, August). *Weekly ICT Trends.* https://www.itfind.or.kr/WZIN/jugidong/2008/file6534007100323952012-2008(2021.08.04)-30.pdf

Jakobsson, M. (2018). Two-factor inauthentication–the rise in SMS phishing attacks. *Computer Fraud & Security, 18*(6), 6-8.

Jeon, H. J. (2020). Hacking through messages that exploited the coronavirus situation increased by 96 percent. *ChosunBiz*.

Jeon, H. W. (2021). The number of smishing texts related to corona 19 has increased by 60 times in a year *"It is urgent to come up with measures to prevent it." Enewstoday*.

Joo, C. K., & Yoon, J. W. (2014). Discrimination of SPAM and prevention of smishing by sending personally identified SMS (For financial sector). *Journal of the Korea Institute of Information Security & Cryptology, 24*(4), 645-653.

Joo, J. W., Moon, S. Y., Singh, S., & Park, J. H. (2017). S-Detector: An enhanced security model for detecting smishing attack for mobile computing. *Telecommunication Systems, 66*(1), 29-38.

Jung, M., & Chang, H. (2020). The case study of technology leakage in cyber-physical space. *Korean Journal of Industry Security, 10*(2), 151-173.

Kang, A., Lee, J. D., Kang, W. M., Barolli, L., & Park, J. H. (2014). Security considerations for smart phone smishing attacks. In H. Y. Jeong, M. S. Obaidat, N. Y. Yen, & J. J. Park (Eds.). *Advances in Computer Science and its Applications* (pp. 467-473). Springer.

Kim, H. S., & Suh, J. B. (2019). A Study on Romance Scam: The Current Situation and Effective Countermeasures. *The Police Science Journal (PSJ), 14*(3), 117-146.

Kim, K. H. (2019). Tracking illegal transactions of personal information. *Shindonga*.

Kim, K. S. (2021). Shadows of untact economic expansion. Smishing fraud has greatly increased. *Hankyoreh*.

Citation Information: Choi, Y.J., & Lee, J. (2021). The change in the methods of smishing in South-Korea after the onset of covid-19. *Journal of Legal, Ethical and Regulatory Issues, 24*(S5), 1-12

Kim, S. H. (2020). A sudden smishing text bomb... Anxiety caused by unprotected access lists [Personal information punctured by Coronavirus Prevention]. *Financial News*.

Korea Communications Commission. (2021). Voice phishing, smishing out! Save me, Korea Communications Commission. *South Korea Policy Briefing*.

Korea Internet & Security Agency. (2015, June 12). *Watch out for smishing and malicious codes related to MERS*. Retrieved from https://www.kisa.or.kr/notice/press_View.jsp?cPage=1&mode=view&p_No=8&b_No=8&d_No=1380&ST=T&SV=%EC%8A%A4%EB%AF%B8%EC%8B%B1

Krippendorff, K. (2018). *Content analysis: An introduction to its methodology (Fourth Edition)*. Sage publications.

Lee, S. Y., Kang, H. S., & Moon, J. S. (2014). A study on smishing block of android platform environment. Journal of The Korea Institute of Information *Security & Cryptology*, *24*(5), 975-985.

Luo, X. R., Zhang, W., Burd, S., & Seazzu, A. (2013). Investigating phishing victimization with the Heuristic–Systematic Model: A theoretical framework and an exploration. *Computers & Security*, *38*, 28-38.

Mishra, S., & Soni, D. (2019). SMS phishing and mitigation approaches. *2019 Twelfth International Conference on Contemporary Computing (IC3)*, 342-346.

Mishra, S., & Soni, D. (2020). Smishing Detector: A security model to detect smishing through SMS content analysis and URL behavior analysis. *Future Generation Computer Systems*, *108*, 803-815.

Na, E. (2006). Internet Communication: Anonymity, Interactivity and Group Polarization. *Communication Theories*, *2*(1), 93-127.

National Police Agency. (2016). *Cyber financial crime prevention rules (memory hacking, smishing, pharming)*. https://policy.nl.go.kr/search/searchDetail.do?rec_key=SH2_PLC20160155982&kwd=%EC%8A%A4%EB%AF%B8%EC%8B%B1&paramPreKwds=%EC%8A%A4%EB%AF%B8%EC%8B%B1

Opensurvey. (2021). *Social Media/Search Portal Trend Report 2021*. Retrieved from https://contents.opensurvey.co.kr/form_socialmedia_2021

Park, H., Kim, W., Kang, S., & Shin, S. U. (2017). Cloud messaging service for preventing smishing attack. *Journal of Digital Convergence*, *15*(4), 285-293.

Park, J., & Ryu, J. K. (2018). Social engineering evaluation of electronic financial fraud: Analysis of actual victims through FGI. *Journal of Digital Convergence*, *16*(7), 9-17.

Shin, H. K. (2021). New Year's holiday security rules, Watch out for corona 19 smishing and hacking. *Newdaily*.

Silver, L. (2019). Smartphone ownership is growing rapidly around the world, but not always equally. *Pew Research Centre*.

Yeboah-Boateng, E. O., & Amanor, P. M. (2014). Phishing, SMiShing & Vishing: An assessment of threats against mobile devices. *Journal of Emerging Trends in Computing and Information Sciences*, *5*(4), 297-307.

Yoon, Y. K. (2011). A study on the risk assessment occurred possibly in a civil project. *Explosives and Blasting*, *29*(2), 59-66.

Citation Information: Choi, Y.J., & Lee, J. (2021). The change in the methods of smishing in South-Korea after the onset of covid-19. *Journal of Legal, Ethical and Regulatory Issues, 24*(S5), 1-12