Journal of Theoretical and Applied Information Technology
30th November 2022. Vol.100. No 22

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AN ANALYSIS OF PHISHING CASES USING TEXT MINING

CHAEYEON JANG[1], OOK LEE[1], CHANGBAE MUN[2], HYODONG HA[1]

[1]Hanyang University, Department of Information System, Korea

[2]Hanyang Cyber University, Department of Information Systems Communication Engineering, Korea

E-mail: wkdcodus123@hanyang.ac.kr(C.J.); ooklee@hanyang.ac.kr(O.L.); changbae@hycu.ac.kr(C.M.)
Corresponding author: special007@hanyang.ac.kr(H.H.)

ABSTRACT

In the modern knowledge and information society, hacking is causing great problems in each area of the industry. Recently, techniques such as distributed denial of service attacks and attacks on management vulnerabilities of cloud servers are gradually evolving. In this study, phishing types were analyzed based on the results of word frequency analysis, clusters were identified, and network analysis was conducted. Through the graph derived from the analysis results, it was possible to identify main keywords, relationships, and trends, and present practical review items for countermeasures against phishing attacks. It also provides a foundation for designing phishing attack prevention measures. By applying this research methodology to the analysis of open source vulnerabilities in the future, it will be possible to have an adaptive defense system for changes in hacking techniques.

Keywords: *Text Mining, Phishing Attack, Cases Study, Semantic Network Analysis*

1. INTRODUCTION

Various types of disasters, including power outages, floods, and hacking, are afflicting businesses and their information systems [1]. In particular, hacking is increasing every year, and the average amount of damage caused by personal information leakage for 10 years from 2007 to 2016 is estimated to be 80 billion to 2.3 trillion dollars [2]. In addition, new security vulnerabilities in the system have been developed by hackers, making the method more sophisticated [3]. For example, shell command injection was the most common in 2020 hacking attacks with 8 million, ThinkPHP remote code insertion attack with 3.5 million, SQL injection with 2.44 million, Webshell access attack with 2.4 million, and File upload vulnerability with 2 million [4].

To effectively respond to these threats, hacking damage can be prevented by analyzing and sharing cyber threat information. There have also been studies on standardization methods using protocols such as structured threat information representation and accident object description exchange formats for sharing cyber threat information [5]. After the accident, there is a study that proposes to actively monitor information on the cyber-based beyond acquisition or sharing in the analysis processs [6].

In addition, it is necessary to strengthen control within the organization to respond to threats. Since crimes by insiders are also increasing, zero-trust measures, which mean "not trusting all access to data," and measures to record and manage surveillance information about who did what are required [7]. issues related to information protection should be continuously identified and analyzed in the optimization stage of the information protection maturity model based on control areas such as human security education and accident management [8].

In order to successfully operate the information system, understanding the external environment surrounding the organization is essentiall [9]. In other words, it is necessary for the organization itself to prevent infringement accidents through analysis of hacking cases from the external environment related to various cyber threats.

Therefore, this study examines major issues using text mining tools for 115 phishing cases of 'Threatpost' from 2017 to 2022. First, phishing cases are collected and reviewed using Python, and then the preprocessing process is performed. And after performing word frequency analysis, keywords for each cluster are extracted through cluster analysis, and implications related to major issues are proposed through related word analysis. Through this, it is possible to establish a

security strategy to protect an organization's information system, and furthermore, it is possible to increase the prevention effect of hacking infringement by sharing information with various organizations.

This study consists of the following. Chapter 2 describes the theoretical background of phishing attacks. Chapter 3 deals with attack cases and analysis techniques and procedures used to conduct the study. Chapter 4 describes the analysis results. And Chapter 5 deals with conclusions and future research.

2. THEORETICAL BACKGROUND AND PRIOR RESEARCH

2.1 Definition and classification of phishing crimes

The term "phishing" was first coined in 1996 [10], and is a compound word meaning "fishing personal information." By deceiving and blackmailing victims using various means such as phone calls, messengers, and SMS, it means a method of extorting money and valuables by exploiting the victim's personal and financial information [11].

Types of phishing include Spear Phishing, Mobile Phishing, Email Phishing, and SNS Phishing [12],[13].

Email phishing is a fraudulent method that steals the names of other institutions, such as financial institutions, and sends mail to victims, and uses it to extract personal financial information and personal information and illegally abuse it [12].

Mobile Phishing is a fraudulent method of deceiving victims using mobile devices and then allowing them to share personal information [13].

Spear Phishing is a fraudulent technique in which an attacker sends personalized attack mail based on the information collected about the victim in the preparation stage of the attack. The cost of Spear Phishing attacks is about 10 times higher than that of regular phishing attacks, but the probability of the victim clicking on the email is also 10 times higher [14].

SNS Phishing is a new phishing technique, such as acquiring financial and personal information of a specific person or requesting money after contacting a specific program on a mobile that is widely used recently, that is, social network service (SNS). From January to April 2018, SNS Phishing damage occurred about 2.5 million dollars, which is an average of about 20 thousand dollars per day [15].

In this study, we analyze the main issues of phishing attacks that are increasing day by day and skillfully developing using text mining techniques. Through this, we intend to improve the effectiveness of preventing hacking infringement by proposing practical implications that can be used for phishing security strategies that can be developed in the future.

2.2 Review of previous studies

Research that deals with the overall part of phishing crimes or focuses on SNS phishing or voice phishing has been actively studied in various aspects such as detection techniques [16], laws [17], policy recommendations [18], and prevention measures [19]. But There was no study that explained the overall trend of phishing accidents compared to cases and conducted a trend analysis of practical accidents using text mining technology.

A study that combines technology by analyzing cases in one area of phishing is as follows. One study was After writing a crime script using 93 Dutch court records, a study was conducted to investigate phishing methods related to bank accounts in the Netherlands and presented two crime scripts [20]. Another study is Analysis of recent studies on the use of predictive models with phishing detection rules, and the applicability of phishing incidents was evaluated [21]. Despite the contents of previous studies as above, phishing accidents are increasing day by day.

3. RESEARCH METHODS

3.1 Research Procedure

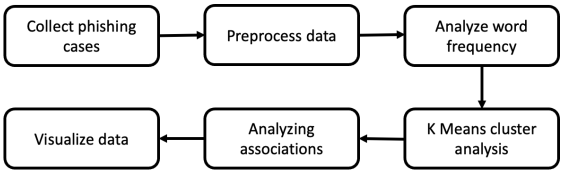

Figure 1: The Procedure of Study

A schematic diagram of the research procedure conducted in this paper is shown in <Figure 1>.

First, we collect 115 phishing cases (keyword: phishing) from 2017 to 2022 on the 'Threatpost' (cyber security news platform). After the collected cases are text-filed, they are labeled as Email Phishing, Spear Phishing, Mobile Phishing, SNS Phishing, and Whaling, etc. according to the phishing type. The victim of the attack means the person who was damaged by the phishing attack, and the victim of the indiscriminate attack that the

victim was not specified was classified as everyone. The contents of the entire case are attached to <Appendix 1>.

In the data preprocessing process, words that appear repeatedly in the case are added to the list of terms to be excluded from data analysis.

When analyzing word networks through word frequency analysis, keywords to be used are extracted, and graphs by attack type and graphs by company and year are visualized. After selecting the top four types among the analyzed phishing types, K means clustering is performed using cases belonging to the phishing type, and the results of K means clustering analysis confirm the distinct clustering of the four types. In addition, after analyzing the frequency of keywords appearing in one sentence at the same time, Semantic network analysis is conducted based on the above.

Finally, based on the results of Semantic network analysis, Semantic network analysis data visualization is performed using Gephi.

4. EXPERIMENTAL RESULTS

4.1 Graph Visualization Using Word Frequency Analysis Results

4.1.1 Graphs by attack type

Graphs by attack type were visualized based on the results of word frequency analysis. It is shown in <Figure 2>. Phishing attacks using e-mail were the most common with 822 cases, and scam, a fraudulent method using the trust of others, was the second most mentioned with 152 cases. Phishing attacks using mobile were the third most common with 77 cases, and spoofing, a fraudulent method such as deceiving opponents and extorting money and valuables, was the fourth most common with 69 cases. Spear, which means spear phishing, a phishing attack to obtain specific information, was the fifth most common with 56 cases, and spam mail, which is a mail sent to an unspecified number of people, was the least mentioned with 32 cases.

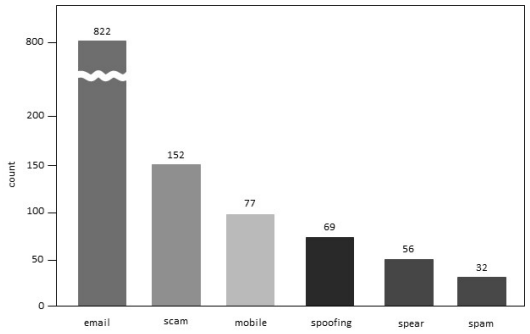

Figure 2: Graphs by attack type

4.1.2 Top 5 Most-Mentioned Companies Graphs

The top five companies mentioned the most among the companies mentioned in the case are shown in <Figure 3>. Microsoft, Google, Facebook, Apple, and Amazon were in the top five, with 226 Microsoft cases, 191 Google cases, 76 Facebook cases, 61 Apple cases, and 40 Amazon cases, respectively.

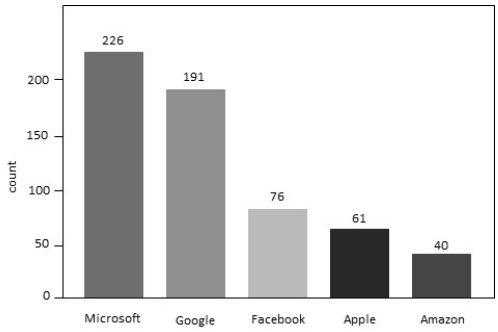

Figure 3: Company TOP 5

4.1.3 Graphs by SNS

The SNS mentioned in the phishing case is as shown in <Figure 4>, and Facebook, Tiktok, Linkedin, and Instagram are mentioned. Facebook was mentioned in 76 cases, Tiktok in 35 cases, and Linkedin and Instagram in 21 cases.

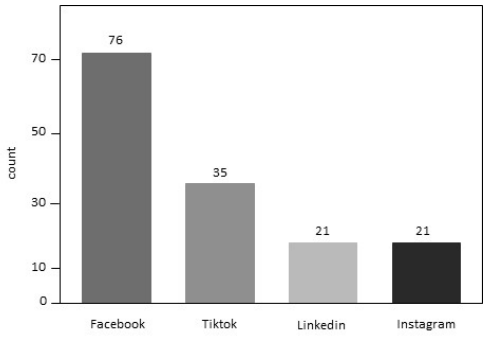

Figure 4: Graphs by SNS

4.2 WordCloud by Year

The cases collected from 2017 to 2022 were classified by each year and word frequency analysis was conducted. WordCloud visualization was conducted based on the results of word frequency analysis. WordCloud is a visualization technique that uses the size of letters to determine the frequency of words [22]. Using the above results, you can know the keywords that had the most issues related to phishing cases in the year, understand the trend of phishing attacks immediately, and are shown in <Figure 5-10>.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

In 2017, financial terms such as DocuSign, which provide electronic signatures, and banking were mentioned a lot, and in 2018, apps, scam, and company were mentioned a lot.

In 2019, Google was mentioned the most, and the term social emerged. In addition, there were many references to targeting, which means spear fishing.

In 2020, companies, targeting, Microsoft, and Google were mentioned most prominently due to cases of phishing attacks against companies, and COVID due to the coronavirus emerged.

In 2021, many companies such as Google, Microsoft, and FedEx were mentioned a lot, and terms such as Covid, anti virous, and online related to the coronavirus were mentioned a lot.

In 2022, Linkedin, a business-oriented social network service, was newly introduced, and Ukraine was also mentioned due to the Russian and Ukrainian wars.

Figure 5: 2017 WordCloud

Figure 6: 2018 WordCloud

Figure 7: 2019 WordCloud

Figure 8: 2020 WordCloud

Figure 9: 2021 WordCloud

Journal of Theoretical and Applied Information Technology
30th November 2022. Vol.100. No 22

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Figure 10: 2022 WordCloud

4.3 K Means Cluster Analysis

K means cluster analysis is a data mining technique that is expressed by dividing each data into K clusters representing each data using the number of cluster centers. While there is an advantage of having a relatively simple algorithm that does not require separate prior information other than the initial value of K, there is a disadvantage in the difficulty of setting an appropriate size of K [23].

In this study, phishing types were labeled for each case in the process of collecting phishing cases, and K means cluster analysis was conducted on the top four phishing types. As for the phishing types of classified cases, Email Phishing was the most common with 61 cases, followed by Spear Phishing with 20 cases and Mobile Phishing and SNS Phishing with 7 cases. In the case of phishing attacks in which phishing attack names are specifically mentioned, such as Phishing–as-a-Service (PhaaS) and AiTM phishing, the attack type itself was set as the attack name and was excluded from Semantic network analysis excluded. Therefore, 95 cases, the total of the above cases, were used as data, and the analysis was conducted by setting the K initial value to 4, the number of case types.

As shown in <Figure 11>, the results of clustering of cases with similar characteristics were obtained through K means cluster analysis, and the characteristics of each cluster could be identified.

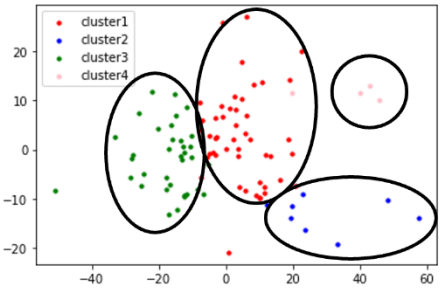

Figure 11: K Means Cluster Analysis

4.4 Visualization by Phishing Type

4.4.1 Email Phishing

The results of the Semantic network analysis of the Email Phishing cases are shown in <Figure 12>. Companies such as Microsoft, Google, Cisco, Webex, and Netflix are mentioned a lot, and the above results can be confirmed because there are many cases where victims are deceived by impersonating other companies through e-mail and then extracting victims' personal and financial information. In the case of targeting and deceiving fraudulent techniques, there were cases of sending e-mails to victims under the guise of certain countries such as Israel and Ukraine.

In one case of Ukraine, employees of certain organizations that manage refugee fundraising, were attacked and there were cases where malicious code was planted in Microsoft Excel under the guise of breaking news about Ukraine, and then e-mails were distributed.

Therefore, in order to prevent email phishing incidents, it is necessary not to open or download websites and attachments linked to email content, but to call email recipients banks and credit card companies directly to check whether the information is true [24].

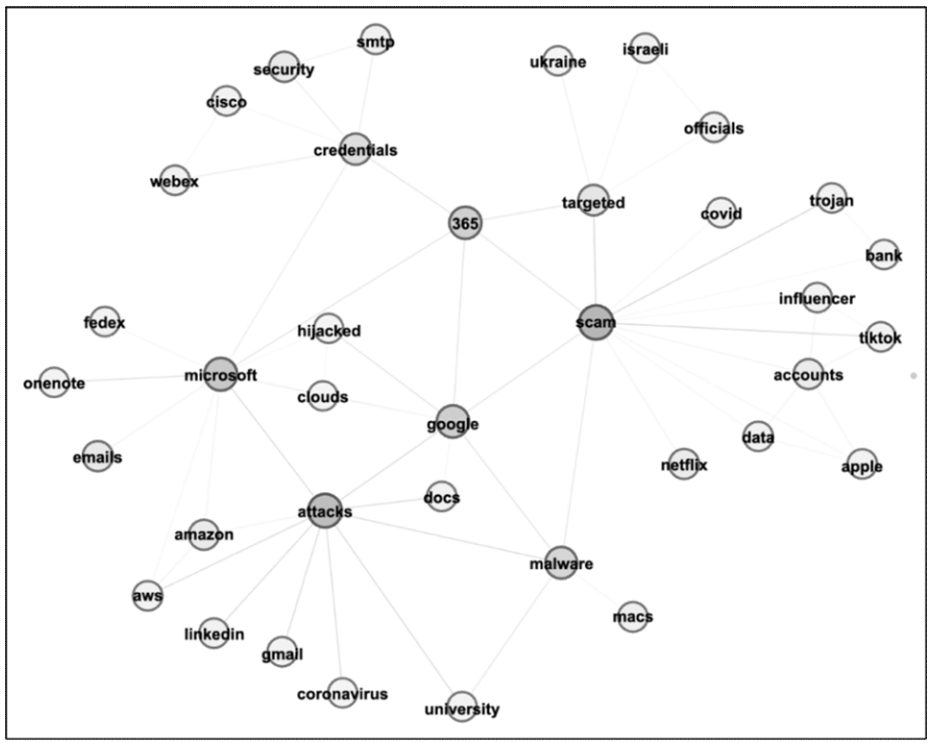

Figure 12: Visualizing Email Phishing Gephi

4.4.2 Spear Phishing

The results of the Semantic network analysis of Spear Phishing cases are shown in <Figure 13>. Spear Phishing is a combination of words such as hook and targeted because it does not indiscriminately search for victims and targets specific groups or companies. Also, because there are national phishing scams targeting high-ranking officials and governments, words such as Trump, Iran, and Global, the former presidents of the United States, have been mentioned together.

Looking at one phishing case, phishing emails were sent to executives of certain companies, pretending to have been sent by a telecommunications conglomerate, intercepting credentials, and payment information. The attack was a highly targeted email sent to only a few executives, including major financial firms.

As such, Spear Phishing is more dangerous and damaging than regular spam mail because it is strategized for a specific group. Therefore, e-mails containing links or attachments require high attention [14].

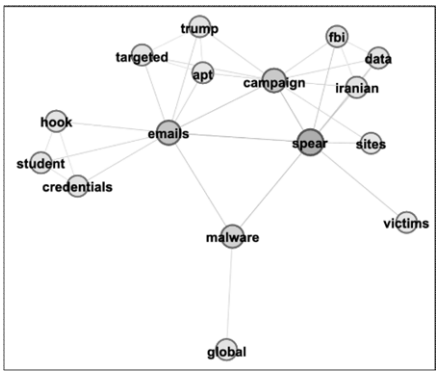

Figure 13: Visualization of Spear Phishing Gephi

4.4.3 Mobile Phishing

The results of the Semantic network analysis of Mobile Phishing cases are shown in <Figure 14>. Since it is a phishing attack through mobile, mobile-related words such as app, sms, and Android have been mentioned a lot. Since the coronavirus epidemic, mobile phishing has increased sharply due to alternative telecommuting, and the incidence of mobile phishing by companies in particular has increased 37% from about 16% to 22% between the fourth quarter of 2019 and the first quarter of 2020.

It is necessary to check the smartphone periodically using a anti virous program available on the smartphone, and applications whose sources

have not been identified should be careful about installation [12].

Moreover, as the most frequently mentioned term in 2018 is app, the risk of mobile phishing should not be overlooked, and practical security measures against mobile phishing attacks are needed.

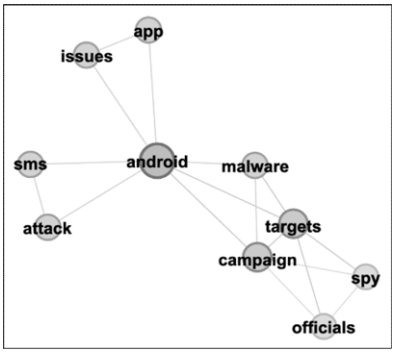

Figure 14: Visualization of Mobile Phishing Gephi

4.4.4 SNS Phishing

The results of the Semantic network analysis of SNS Phishing cases are shown in <Figure 15>. Since SNS Phishing is a fraudulent method of extorting and exploiting victims' personal information or payment information [15] through the messenger function of SNS, SNS-related words such as Instagram, Messenger, and Facebook have been mentioned a lot.

In one case of SNS Phishing, an attacker distributed a fake Facebook login page through Facebook Messenger, and then induced the victim to submit credentials, causing about 10 million users to be damaged. In 2021, about 2.8 million victims were identified, and by June 2022, about 8.5 million victims were reported [25]. As such, SNS phishing is showing an increasing trend day by day, and it seems necessary to have a countermeasure and a stable network.

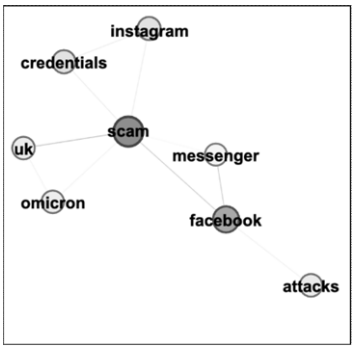

Figure 15: Visualization of SNS Phishing Gephi

5. CONCLUSIONS AND FUTURE RESEARCH

With the development of information and communication, phishing accidents are gradually increasing, and the methods are also becoming more diverse. Various studies are being conducted to prevent phishing accidents, and preparation of countermeasures against the changing phishing fraud method is being emphasized.

In this paper, the most prominent keywords from 2017 to 2022 were derived through the analysis of real-life cases of phishing accidents published in ThreatPost, and the network association analysis of the words used in the case was conducted according to the type of phishing labeled.

the authors conducted a study to analyze various defense techniques against security infringement along with social phenomena. The excellence of this study lies in the attempt to apply a convergent research methodology by linking information security technology with social phenomena. Security threats to information technology are particularly related to political and social phenomena. Using the methodology and result data of this study, new attempts can be made on the application of security technology. For example, diagnostic software, which provides automatic diagnosis of the characteristics and related phenomena of security vulnerabilities, can be used to find solutions and methods with excellent detection results based on various texts on the phenomenon and the number and risk of vulnerable source codes detected.

It is expected that the results of word network analysis according to the type of phishing derived in this paper will help to prepare a solution to prevent phishing fraud.

As a follow-up study of the methodology of this study, it is intended to be applied to measures to improve open source vulnerabilities. The vulnerability of open-source targeting has a wide range of applications, so there is a risk of infection at the same time, so the vulnerability spreads rapidly. Since it has a risk, vulnerabilities spread rapidly. In terms of operation, security updates must be constantly applied during the period of use, and off-source solutions with EOS for the version are at high risk of use, which leads to a review of equipment reapplication. Certain paid solution-based projects have static vulnerabilities only in software targeted and applied directly, even if vulnerabilities occur, so the damage is less in scope than open source vulnerabilities. These shortcomings are closely

related to the trends and social phenomena of security technology, and it is expected that applying the methodology of this study will lead to more adaptable conclusions.

ACKNOWLEDGEMENTS

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education (2020R1G1A1006677).

REFERENCES:

[1] Baltzan, P., & Phillips, A. (2014). Business Driven Information Systems. McGraw Hill.

[2] Im Kyu-gun, Ryu Mina, & Lee Jung-mi. (2018). A Study on the Cost Calculation Model of Personal Information Leakage Damage Journal of the Society for Information Protection, 28(1).

[3] Shin, H., Lim, H. S., & Lim, C. H. (1997). Understanding and Countermeasures of Internet Hacking Techniques Communications of the Korean Institute of Information Scientists and Engineers, 15(4), 21-29.

[4] Korea Financial information sources, annual strike attack, https://www.fis.kr/ko/major_biz/cyber_safety_oper/attack_info/notice_issue?articleSeq=1755

[5] Mkuzangwe, N. N., & Khan, Z. C. (2020). Cyber-threat information-sharing standards: A review of evaluation literature. The African Journal of Information and Communication, 25, 1-12.

[6] Kim In-hwan, Kang Ji-won, Ahn Hoon-sang, & Jeon Byung-guk. (2022). A Study on the Threat Detection Model Using Cyber Base Convergence Security Paper, 22(1), 19-27.

[7] Hiroyuki, Atsumori, Kyohei, & Manabu. (2022).Microservice Gu to study painting Joe. J. Pub

[8] Kim Ja-hee, Choi Kwang-ryul, & Kim Chang-jae (2015). A Study on the Mature Model of Information Protection in Public Institutions Journal of the Korean Society of Information Technology, 13(11), 51-60.

[9] Piccoli, G. (2007). Information systems for managers: texts and cases. Wiley Publishing.

[10] DikshaGoelAnkit KumarJain . (2018). Mobile phishing attacks and defence mechanisms: State of art and open research challenges, The ELSEVIER Journal of Computers & Security, 73, 519-544.

[10] DikshaGoelAnkit KumarJain . (2018). Mobile phishing attacks and defence mechanisms: State of art and open research challenges, The ELSEVIER Journal of Computers & Security, 73, 519-544.

[11] Korea Internet & Security Agency (KISA Internet Protection Country & KrCERT), Phishing Prevention Guide, https://www.boho.or.kr/cyber/preventPhishing.do

[12] Kang Hyun-joong (2014). A Study on the Analysis and Response to Phishing Convergence Security Paper, 14(5), 65-74.

[13] RFAUDWATCH, https://fraudwatch.com/expert-explanation-what-is-mobile-phishing-why-is-it-on-the-rise/

[14] Son Yu-seung, Nam Ji-hyun, & Ko Seung-cheol. (2013). Access by administrative security measures to respond to spear phishing. Journal of the Korean Society for Information and Communication, 17(12), 2,753-2,762.

[15] Yoo Jae-doo (2018). A Study on the Countermeasures through the Analysis of New SNS Phishing Status and Cases Korea Crime Psychology Research, 14(4), 103-116.

[16] Bae Ji Hyo, Chae Su Yeol, Song Myeong Jun, Bang Kyeong Chan. (2019). Detection method through analysis of messenger phishing conversation. Proceedings of Symposium of the Korean Institute of communications and Information Sciences, (), 537-538.

[17] Lee, Ki Soo. (2018). Recent Trends in Crime Methods and Legal Measures of Voice-Phishing. Criminal Investigation Studies, 4(2), 3-19.

[18] Chung Woong. (2020). Trend of Voice Phishing Crime and Development Direction of Investigation Response System. Journal of the Korean Society for Public Security Administration, 29(4), 461-484.

[19] Yoon Hae-Sung, Kwack Dae-gyung. (2009). Study on Prevention and Countermeasure of Voice Phishing. the Criminal Policy Institute's Research Paper, (), 9-118.

[20] Loggen, J., Leukfeldt, R. (2022). Unraveling the crime scripts of phishing networks: an analysis of 45 court cases in the Netherlands. Trends Organ Crim, 25, 205–225.

[21] Thabtah, F., Kamalov, F. (2017). Phishing Detection: A Case Analysis on Classifiers with Rules Using Machine Learning. Journal of Information & Knowledge Management, 16(4).

[22] Rob Atenstaedt. (2012). Word cloud analysis of the BJGP. British Journal of General Practice, 62(596), 148.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[23] Lee Dong Heon, Chun Woo Je, & Park Soo Hong. (2005). Vector Data Compression Method Using K-means Clustering. Paper, Open Geographic Information Systems Society, 7(3), 104-118.

[24] Yoo Jae-hyung, Lee Dong-hwi, Yang Jae-soo, Park Sang-min, & Kim Gwi-nam (2008). Review of the current status and countermeasures of domestic voice phishing telephone financial fraud - Focusing on measures in the telecommunications sector. Information and Communication Policy Research Paper, 24 (15), 50-69.

[25] Threatpost, Facebook Messenger Scam Duped Millions, https://threatpost.com/acebook-messenger-scam/179977/

Appendix 1.

NO	DATE	VICTIM	ATTACK	CONTENTS
1	2022-06-16	top Israeli government officials	Email Phishing	An intelligent persistent threat (APT) group linked to Iran carried out phishing attacks against the Israeli government and soldiers, and the goal of the attack is to obtain personal information from targets.
2	2022-07-13	everyone	AiTM phishing	An attacker uses a middleman attack to steal a password, intercept a login session, skip authentication, and use the victim's mailbox to perform a BEC attack on another target.
3	2022-07-12	everyone	Email Phishing	A 'callback' attack was found, a phone that impersonates a famous security company to trick the victim and then instructs him to download malicious code.
4	2022-05-11	User of Using mail	Email Phishing	It takes advantage of the main difference between the email inbox and the way the browser reads the URL, through which an attacker sneaks a malicious link into the victim's inbox.
5	2022-03-29	User of Using mail	Email Phishing	Phishing email sent using a corrupted Microsoft Exchange server.
6	2022-03-03	EU government employees about managing Ukraine	Email Phishing	Phishing EU officials involved in logistics management of refugees fleeing Ukraine using hacked Ukrainian military email addresses
7	2022-02-21	OpenSea NFT's Users	Email Phishing	Phishing email sent to OpenSea NFT members.
8	2022-02-16	Great Resignation' job hunters	Email Phishing	Phishing emails to job seekers impersonating LinkedIn.
9	2021-12-03	everyone	SNS Phishing	Sent a new test kit proposal link specifically designed to detect Omicron variants using SMS such as text and email.
10	2021-11-18	User of Using mail	Email Phishing	MIRCOP ransomware, known as Crypt888 ransomware, was sent over an email link.
11	2021-11-17	TikTok influencer	Email Phishing	Send an email impersonating TikTok and ask the user to check their login information to steal the account.
12	2021-11-11	User of Using mail	Email Phishing	An attacker uses an emergency message to attach a message to the content, such as a password expiration notification that encourages a potential victim to click on a malicious link.
13	2021-10-27	Google Ads	phishing	A British teenager collects people's payment information using a fake Love2shop gift card site and steals money from cryptocurrency.
14	2021-09-28	User of Using mail	Email Phishing	About 75,000 inboxes have been emailed through spam and security controls such as Office 365, Google Workspace, Exchange, and Cisco ESA.
15	2021-09-23	everyone	PhaaS (Phishing-as-a-Service)	Found BulletProofLink, which provides more than 100 available phishing templates that mimic known brands and services, including Microsoft itself.
16	2021-09-15	Industrial Enterprise	Email Phishing	A site masquerading as the U.S. Department of Transportation sends phishing e-mails that induce bids for projects benefiting from the $1 trillion

				infrastructure package recently passed by Congress for two days.
17	2021-08-13	everyone	phishing	When phishing content is hidden using the so-called 'Not Robot' feature (CAPTCHA), the security crawler does not detect malicious content and provides a legitimate appearance.
18	2021-08-13	Asian manufacturers	Spear phishing	Attack on Asian manufacturers through phishing that provides Warzone RAT using a compromised WordPress website.
19	2021-08-04	Company of Using Microsoft office 365	Email Phishing	Send phishing emails impersonating someone from a trusted organization.
20	2021-08-02	Chipotle Mexican Grill	Email Phishing	Chipotle's email vendor hacking, providing customers with malicious links to phishing sites.
21	2021-07-29	University of California San Diego Health	Email Phishing	E-mail phishing exposes personal information including the name, address, date of birth, email, social security number, etc. of the registered patient.
22	2021-07-07	everyone	phishing	Nine years of cyberattacks against thousands of victims through phishing, website tampering, malware development, fraud and carding. 'Dr HeX'
23	2021-06-17	Google Docs	Email Phishing	After sending an e-mail that has something to do with Google Docs used by the company, we have taken away the account.
24	2021-06-08	User of Using mail	Email Phishing	The content of the email contains a link, which links you to a photo site and then to a fraudulent data site.
25	2021-06-02	candidates for political office and related associates	Spear phishing	Steals the identity of a trusted colleague to induce him to comply with the message's credential request.
26	2021-05-28	Industrial Enterprise	Email Phishing	A group of hackers impersonated a U.S.-based development organization to distribute emails containing malicious URLs using Constant Contact, a legitimate bulk email service.
27	2021-05-19	User of Using mail	Email Phishing	95% of organizations are subject to cloud account breaches, more than half of which are reported to be successful.
28	2021-05-05	immigrant community	Spear phishing	A site targeting the immigrant community and pretending to be for a company developing the COVID-19 anti virous has been found and closed.
29	2021-05-04	Electronics Manufacturer	Spear phishing	The attackers impersonated the account manager of a small electronics manufacturer in California, investigating the target and adjusting the phishing email title to suit the victim.
30	2021-04-23	User of Using mail	Email Phishing	Users visited the site where they watched the first few minutes of the movie to watch the Oscar nomination, and they must enter payment information to continue watching.
31	2021-04-02	User of Using mail	Email Phishing	Hackers impersonate securities trading brokers using fake websites to include tax files containing malicious code in attachments.

32	2021-03-19	executives in the insurance and financial services industries	Whaling	Attackers send Office365 impersonation emails to senior executives and attach malicious links for security updates.
33	2021-04-10	everyone	Spear phishing	It was written that a colleague was late for the office and included a link to the pdf preview asking you to check the presentation material.
34	2021-04-08	User of Using Microsoft	Email Phishing	Create phishing sites using fake Google reCAPTCHA systems and top-level domain visit pages with victim company logos.
35	2021-02-24	User of Using Microsoft	Email Phishing	Utilizes Outlook, Teams, and other Microsoft-themed phishing bait
36	2021-02-23	User of Using Microsoft	Email Phishing	impersonating Fedex to steal credentials from Microsoft email users.
37	2021-02-19	User of Using mail	Email Phishing	Use http://\ in the URL prefix of the phishing email to bypass the scanner, then send the phishing email.
38	2021-01-26	User of Using TikTok	phishing	Attackers use TikTok's loopholes to automate the contact upload and synchronization process on a large scale to build a DB for sparse phishing.
39	2020-12-15	Subway loyalty program members in U.K	Email Phishing	Phishing attacks have been discovered targeting members of Subway Premium Card in the UK and Ireland to download malware.
40	2020-11-25	User of Using mail	Email Phishing	After developing phishing links and domains, it carries out mass email campaigns impersonating employees of various organizations.
41	2020-10-29	University Students	Email Phishing	More than a dozen universities have stolen legitimate email accounts and tricked victims into handing over email credentials or installing malware
42	2020-10-22	User of Using Microsoft Teams	Email Phishing	Attackers attempted to hack Office 365 recipients' login credentials using Microsoft Teams' 'out of office chat' weaknesses.
43	2020-10-20	User of Using Facebook	SNS Phishing	Send malicious YouTube video links to Facebook users using Facebook messages.
44	2020-10-08	User of Using Amazon	Email Phishing	Create phishing pages using Amazon brands and logos, and lure victims to fraudulent sites that leverage both Amazon's capabilities and consumer behavior.
45	2020-10-01	User of Using Microsoft Office 365	phishing	The phishing page is a Microsoft Office 365 page, which uses the page above to hack the victim's credentials.
46	2020-09-30	User of Using Microsoft Office 365	Email Phishing	Victims are prompted to click a link to the third-party app consent page upon legitimate Microsoft login.
47	2020-09-11	User of Using Microsoft Office 365	Email Phishing	Real-time verification is possible when entering the victim's Office 365 credentials on the visit page using the authentication API.
48	2020-09-02	High-ranking official	Whaling	Sent mail containing weaponized RTF attachments disguised as WHO's 'Important Preparation and Response Measures for COVID-19, Temporary Guidelines'.
49	2020-08-28	User of Using Instagram	SNS Phishing	Attackers use Instagram's Direct Message to provide phishing links to victims.

50	2020-06-08	High-ranking official	Whaling	The attacker sent a mail to the victims containing a URL to go to the fake Microsoft login page.
51	2020-06-04	campaign staffers for both Donald Trump and Joe Biden	Spear phishing	The Chinese group targeted Biden's campaign staff, while the Iran-linked group conducted phishing attacks targeting Trump's staff.
52	2020-06-03	User of Using Mobile	Mobile phishing	You can use SMS, social media, messaging platforms, and dating apps to pass malicious payloads through phishing attacks on mobile devices.
53	2020-05-19	User of Using Microsoft Office 365	Email Phishing	Clicking on a link disguised as a typical invitation for a SharePoint hosting file takes you to the fake Microsoft Office 365 login page.
54	2020-05-21	Corporation	Email Phishing	Encourage recipients to click on the Google Firebase link by email, and when they click on the link, they are directed to go to the virtual login page and enter their credentials.
55	2020-05-05	High-ranking official	Whaling	An attack was found impersonating a telecommunications company EE to steal credentials and payment details from a corporate executive.
56	2020-04-30	High-ranking official	Whaling	An attack has been found that leverages Microsoft File Sharing Service to force a victim to hand over credentials.
57	2020-04-27	University Students of America	Spear phishing	Using adult dating bait for emails of victims of American college students.
58	2020-04-23	User of Using Skype	Email Phishing	Encourage the victim to click the 'Review' button by impersonating a Skype warning notification email.
59	2020-04-09	User of Using mail	Email Phishing	Sent phishing emails under the guise of Cisco that are written as 'Critical Security Advice'.
60	2020-04-02	User of Using mail	Email Phishing	Attackers send phishing emails pretending to be a trusted brand.
61	2020-04-01	American	Email Phishing	Targeted at U.S. healthcare and higher education institutions and sent phishing emails under the guise of mails sent by payroll departments.
62	2020-04-01	User of Using mail	Email Phishing	Attackers impersonate children's online learning game domains using spoofed IP addresses located in the United States to avoid ATP detection.
63	2020-03-16	everyone	phishing	An attacker impersonates a domain name using isomorphic characters in a website URL and disseminates malicious websites that appear legitimate.
64	2020-03-11	User of Using YouTube	Email Phishing	An attacker used a phishing email using a YouTube redirect link.
65	2020-03-10	User of Using mail	Spear phishing	The attacker used a phishing email telling the victim that he could check the results of the HIV test.
66	2020-03-04	User of Using mail	Email Phishing	Attackers use OneNote to bypass detection tools and induce malicious code to be downloaded to the victim's system.
67	2020-02-14	Customers of North America bank	SNS Phishing	Mobile phishing has been discovered targeting approximately 12 or more North American bank customers.

68	2020-02-13	Industrial Development Company of Puertorico	Spear phishing	The organization receives a phishing email claiming to change its bank account related to remittance payments.
69	2020-02-10	User of Using PayPal	Spear phishing	Phishing email has been sent to PayPal users.
70	2020-02-07	User of Using Mobile	Mobile phishing	It hijacks your Android mobile device to steal your credentials, installs a keylogger, and sends malicious code via phishing email to extort your data.
71	2020-01-21	User of Using PayPal	Spear phishing	A phishing attack was found targeting PayPal users.
72	2019-11-26	User of Using PayPal	Spear phishing	When a victim attempts to purchase something by mistaking a phishing page using a MiTM attack, it moves to a fake payment page and collects payment information.
73	2019-11-18	User of Using Microsoft Office 365	Email Phishing	An attack was found attempting to send phishing emails to victims by compromising their Office 365 administrator account.
74	2019-11-06	everyone	phishing	Attackers leverage key technical indicators used in web analytics, especially Google Analytics, to create more sophisticated, targeted phishing attacks.
75	2019-11-06	User of Using mail	Email Phishing	An attacker impersonates the UK Department of Justice and induces an e-mail to click on a phishing page link.
76	2019-10-16	University Students	Spear phishing	Silent Liberian devised phishing emails aimed at stealing student login credentials for college students.
77	2019-09-13	Company of America	Email Phishing	Phishing emails included Trojan Horse documents, which use social engineering techniques.
78	2019-09-12	University Students	Spear phishing	Silent Liberian uses a fake library-themed landing page to steal student credentials and then use it to perform internal phishing.
79	2019-09-11	User of Using mail	Email Phishing	Phishing email attacks using private, human emotions such as pharmaceutical companies, diet pills, divorce lawsuits, etc. have occurred.
80	2019-09-11	User of Using MacOS	phishing	The Trojan horse downloader Shlayer, which downloads and installs various adware, threatens macOS users.
81	2019-09-04	User of Using Mobile	Mobile phishing	An attack occurs that sends malicious wireless provisioning messages to vulnerable mobile phones and routes all Internet traffic through a proxy controlled by a hacker.
82	2019-08-08	User of Using mail	Email Phishing	Targeted phishing attacks using the branding and email formats of DocuSign.
83	2019-06-05	everyone	phishing	Vulnerable phishing kits provide entry points that can compromise legitimate website servers.
84	2019-03-20	Saudi Government	Bad Tidings	The hacking attack, codenamed "Bad Tidings," found a phishing site pretending to be an electronic service portal for Saudi Arabia's Interior Ministry.
85	2019-03-05	everyone	Jmail Breaker	Attacker Alarg53 uses Jmail to create a phishing site that mimics the Zomla! site.

86	2019-02-22	Polish bank and its users	Email Phishing	Targeting bank users with malicious code and using fake Google reCAPTCHA.
87	2019-02-15	User of Using Facebook	phishing	When the victim visits the website, the message to access the fake Facebook login site appears.
88	2019-02-06	User of Using Facebook and Gmail	Email Phishing	This is a two-stage phishing attack that targets Facebook and Google credentials using a visit page hidden behind Google's translation capabilities.
89	2019-01-25	User of Using mail	Email Phishing	An attack using a phishing email containing a Word attachment containing a macro was found.
90	2019-01-04	Customers of U.S. bank	Email Phishing	Clicking on a phishing email loads a phishing site that looks like a login page for a major U.S. bank.
91	2018-12-27	User of Using Netflix	Email Phishing	The scams impersonated Netflix and guided the victim's link to unprotect their account due to billing issues.
92	2018-11-20	User of Using Gmail	phishing	Phishing attacks using bugs that manipulate Gmail's headers to ultimately leave the sender mark blank and anonymize emails.
93	2018-11-16	User of Using Gmail	Email Phishing	Phishing attacks are carried out using a fatal bug that can induce a victim to click a malicious link or open a file with malicious code.
94	2018-10-10	User of Using mail	Email Phishing	When a user clicks a button included in phishing mail, it is taken to the page of the fake Office 365 login form.
95	2018-09-28	User of Using Android	Mobile phishing	A new design-based security API was discovered after a design flaw was discovered in the way the password manager checked the Android app.
96	2018-08-23	everyone	phishing	Democratic National Committee finds attempt to corrupt voter databases
97	2018-08-15	User of Using Microsoft Office 365	Email Phishing	The attack, named 'PhishiPoint', is propagated to the victim via an email containing a SharePoint document and an invitation to collaborate.
98	2018-08-13	User of Using Mobile	Mobile phishing	Contains text messages that prompt victims to download the Trojan horse app and dangerous links within fake Facebook accounts.
99	2018-08-09	User of Using mail	Email Phishing	Suspicious mail has arrived in the inbox of the target under the title 'Project Proposal'.
100	2018-08-02	Industrial Development Company	Email Phishing	An email impersonating a commercial proposal was found.
101	2018-07-16	bank Customers	Email Phishing	Phishing email was found for bank customers.
102	2018-06-20	User of Using Netflix	Email Phishing	Phishing emails impersonated Netflix, with links included.
103	2018-06-06	User of Using Facebook	SNS Phishing	The attack uses a Facebook post to extort information using a bait that provides two free tickets in return for completing the survey.
104	2018-05-21	User of Using Android	Mobile phishing	Victims are redirected to malicious web pages distributing Trojan horse applications pretending to be Facebook or Chrome.
105	2018-05-15	Top officials, primarily in the Middle East	Mobile phishing	Customized surveillance wear has been found, used primarily to extract data from senior Middle Eastern officials.
106	2018-05-14	User of Using Apple	Email Phishing	Trick the victim to disclose his Apple account credentials to collect personal details, including

				credit card and Apple account information.
107	2018-03-26	U.S.universities, private companies, government departments	Spear phishing	Hackers allegedly worked for more than four years to steal expensive scientific and engineering research, company trade secrets, and sensitive U.S. government information.
108	2022-06-16	User of Using Facebook	SNS Phishing	The same phishing scam has been found that forces millions of Facebook users to hand over their account credentials.
109	2018-02-23	User of Using mail	Email Phishing	One of several new variants of IRS and tax-related phishing campaigns targeting W-2 information has been discovered.
111	2017-09-07	User of Xero	Email Phishing	Sophisticated phishing attacks have been found targeting users of cloud-based accounting firm Xero.
112	2017-08-14	User of Using Apple	phishing	Illegal phishing sites found targeting Apple users.
113	2017-06-06	User of Using Facebook	SNS Phishing	An attack using Facebook messages was detected.
114	2017-05-26	everyone	phishing	Distributed TLS certificates to ensure that the victim thinks they are visiting a secure site.
115	2017-05-16	User of Using DocuSign	Email Phishing	Attackers impersonate DocuSign and send phishing emails to members with links to malicious Word documents.