JCA JOURNAL OF CONTEMPORARY ACCOUNTING

Journal of Contemporary Accounting, Volume 6, Issue 2, 2024, 97-112

Journal of Contemporary Accounting

Volume 6 | Issue 2

Analysis of social engineering prevention socialization patterns through websites and Twitter

Rahmadani Ningtyas Sekar Putri
Department of Accounting, Universitas Islam Indonesia, Yogyakarta, Indonesia
rahmadaninsp@gmail.com

Hendi Yogi Prabowo Hendi
Department of Accounting, Universitas Islam Indonesia, Yogyakarta, Indonesia
hendi.prabowo@uii.ac.id

Rahmadani Ningtyas Sekar Putri and Hendi Yogi Prabowo. (2024). Analysis of social engineering prevention socialization patterns through websites and Twitter. *Journal of Contemporary Accounting*, 6(2), 97-112. doi: 10.20885/jca.vol6.iss2.art3

Analysis of social engineering prevention socialization patterns through websites and Twitter

Rahmadani Ningtyas Sekar Putri*, Hendi Yogi Prabowo

Department of Accounting, Universitas Islam Indonesia, Yogyakarta, Indonesia

Article History:
Received : 2022-10-24
Revised : 2024-07-24
Accepted : 2024-08-03
Published : 2024-08-31

JEL Classification:
K42, K24

Keywords:
Prevention socialization, social engineering, website, twitter

***Corresponding Author:**
rahmadaninsp@gmail.com

DOI:
10.20885/jca.vol6.iss2.art3

Abstract

This study aimed to identify social engineering prevention socialization patterns through website and twitter by six major banks in Indonesia. This qualitative research utilized archival research method and documentary secondary data, namely using the bank's website and twitter media. This qualitative research uses content analysis and data was processed using NVivo 12 software. The results showed that the socialization of social engineering prevention provided by six banks in Indonesia through the website and twitter media contained information about the characteristics of social engineering, bank contact service facilities, and steps to prevent social engineering. Optimization of socialization through the website and twitter could be done by creating content that contains complete and up-to-date information about the characteristics of social engineering, contact service facilities, and preventive measures that could be visualized in the form of videos or attractively designed poster images.

Introduction

Nowadays, the existence of internet-based technology has various benefits for the banking sector, namely providing digital banking services such as internet banking, short message service banking, mobile banking and others. Currently the internet is a double-edged sword, because apart from contributing to the advancement of civilization, the internet is also an effective means of committing cyber-crimes.

Gibbs (2020) claimed that the increase in cybercrime was due to the rapid development of technology. This was also agreed by Wall (2017) who claimed that with the development of technology, it could actually create cyber-crime. According to Kävrestad (2018) cyber-crime is formed due to the means and opportunities which will then involve computerized tools and knowledge. Perpetrators can commit various crimes with different techniques and methods in cyberspace, especially in the banking world such as phishing, vishing, identifying theft, denial of service, social engineering, and others that aim to steal customer financial data (Ali, 2019).

Badan Siber dan Sandi Negara (BSSN) (2020) stated that from January 1st to April 12th, 2020, there were 88,414,296 cyber-attacks that occurred. There were 25,224,811 attacks in January, 29,188,645 attacks in February, 26,423,989 attacks in March, and 7,576,851 attacks on April 12th. Based on data from the National Cyber Security Operations Center (Pusopskamsinas) of the National Cyber and Crypto Agency (BSSN), the attack that occurred was of the type of Malicious

Email Phishing with the issue of the Covid-19 pandemic as the background of the attack. This attack affected psychology and exploited the victim's weakness of a security, this fraud technique is called social engineering. Social engineering is the art of influencing individuals in order to gain confidential information such as passwords, addresses, bank details etc. by exploiting human vulnerabilities (Chetioui et al., 2022).

Furthermore, Badan Siber dan Sandi Negara (2020) stated cybercrime in April 2020 was dominated by information gathering cases, which included social engineering attacks. Information gathering is the desire to know more about the information of potential victims. Information gathering cases in April had a percentage of 54%, which shows that there was an increase from the previous month, which was 42%. The banking world is very vulnerable to fraud because the banking sector carries out many financial transactions. Based on information from the BSSN (2022) OJK said that in 2021 there were cyber-attacks in the top 10 industries, as many as 22.4% that occurred in the financial sector. With details of 70% of attacks aimed at the banking sector, 16% insurance companies, and 14% other financial sectors. BSSN noted that there were more than 1.65 billion cyber security traffic anomalies in January – December 2021. This was conveyed by Deputy Head of BSSN Inspector General Luki Hermawan at the launching of the annual cyber security monitoring report.

> *"We are monitoring from the results of monitoring throughout 2021 that there is a very large traffic anomaly threat, namely more than 1.65 billion cyber-attacks," (Irjen Luki Hermawan, 2022)*

Inspector General Luki Hermawan revealed that most of the total anomaly traffic came from malware infections at 62%, trojan activity at 10% and information gathering at 9%, the rest are trends in cyber incidents in Indonesia in the form of web defacements, data breaches, human operated ransomware, advanced persistent threats, phishing (CNN Indonesia, 2022).

Furthermore, the case of a social engineering attack that occurred in 2022 whose video was circulated on May 31st, 2022 and went viral on social media. According to the conference submitted by the Head of the Public Relations Division of the West Sumatra Kombes Pol Stefanus Satake Bayu, this case happened to bank customers in Padang who suffered losses of more than Rp 1.1 billion. This case includes a social engineering attack with a phishing technique, which begins with the victim receiving a WhatsApp message about a notification of a change in transfer fees by the perpetrator claiming to be a bank employee. Then the victim was sent a form and a link by the perpetrator to fill in the username, password, and pin. The victim received an SMS from the bank in the form of an OTP code which is forwarded to the perpetrator. Until finally, the victim received a notification from the bank that there was a transaction out of his missing account that was stolen by the perpetrator (KOMPAS, 2022) .

Hasan and Febriany (2021) stated that the proliferation of digital developments and increasingly sophisticated technology had both positive and negative impacts on the banking world, and more crimes from a financial perspective, so prevention and handling steps were needed. Therefore, a series of solutions are needed as a step to prevent social engineering attacks.

Junaedi (2017) said that prevention of social engineering in the banking sector can be carried out in various ways, such as improving the banking system to make it more secure, optimizing employee knowledge by training and educating, and providing socialization to customers. Prevention by providing socialization to customers has a higher level of urgency, because many of whom become victims of social engineering attacks are bank customers, so customers are important things that must be protected.

Now, providing social engineering prevention socialization to customers is easier with the presence of the internet. The provision of online socialization can be shared extensively, so that customers from any area can know the socialization. Currently, almost all community activities use the internet, so customers do not find it difficult to access the socialization materials.

Based on data from We are social (2022) there were 204.7 million users using the internet and 191.4 million active social media users out of a total population of 277.7 million people. Then the average daily people use the internet for 8 hours, 36 minutes. The social media platform that is often used by the public is twitter, with 58.3% of the population using twitter. This shows that the interaction of Indonesian people with internet usage is quite frequent, and the data shows that the reason internet users in Indonesia use the internet network is to help find information (We are social, 2022).

Thus, social engineering prevention socialization through website media and twitter social media is the right step, because looking at previous data, people who use the internet have more and more of the total population and plus people are also active on Twitter social media, so that in this way socialization can be delivered by the customer.

Therefore, researchers were interested in investigating more deeply about the socialization of social engineering prevention by banks through the media website and twitter. Thus, this research will analyze social engineering prevention by describing social engineering prevention socialization patterns by six major banks in Indonesia through website and twitter media. The big banks include Bank Central Asia (BCA), Bank Mandiri, Bank Negara Indonesia (BNI), Bank Rakyat Indonesia (BRI), Bank Permata, and Bank Syariah Indonesia (BSI). The results of this analysis process used the help of Computer Assisted Qualitative Data Analysis Software (CAQDAS) called Nvivo 12 Software.

Literature Review

Consumer Fraud

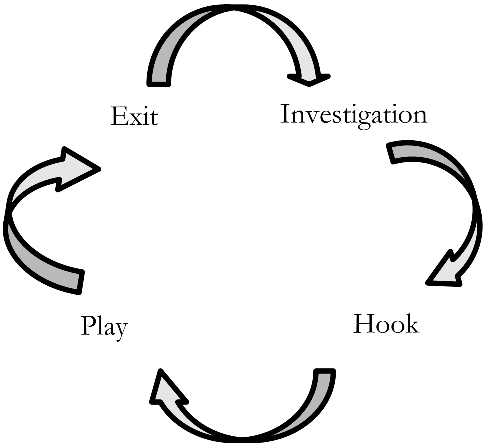
Titus et al. (2001) said that consumer fraud is realized by consumers to be a "facility" in this fraud, which indirectly assists the perpetrator in committing fraudulent acts. The types of consumer fraud that often occurred include product fraud, fake gift promotions, being billed to buy even in a position of disagreement, being billed for buying internet services that are not approved for purchase, and work-at-home program fraud (Anderson, 2011).

In addition, in the research of Rebovich et al. (2000) developed a "risk" index of behavior that was considered to expose consumers to fraud. This study stated that there were several factors that make victims vulnerable to white-collar crime, including: (1) Never responded to an unsolicited message, by purchasing items to win free gifts; (2) Have you ever given a PIN or ATM code to someone else; (3) Neglected to do background check on contractor; (4) Neglected to destroy credit card requests; (5) Provide the victim's credit card number via cordless phone; (6) Has difficulty resisting sales promotions.

Social Engineering Attack

Social engineering according to Chetioui et al. (2022) namely the art of influencing an individual to obtain confidential information such as passwords, addresses, detailed information related to banks. Social engineering is a psychological attack that attacks humans by cheating for something they shouldn't do. According to Safitri et al. (2020) social engineering was often used by attackers to obtain important information because attackers understood that humans or users were the weakest link even though programmers had built a good security system. Humans were very easy to manipulate to provide information or other details that were useful to attackers. In addition, humans were also easier to hack than computer systems and networks (Abass, 2018).

Abass (2018) said that social engineering is divided into two types, namely computer based and human based. Stated that computer-based social engineering was an approach that deceived the victim into believing that the victim was interacting with an actual computer system, thus making the victim provide confidential information. Whereas social engineering based on human was a fraud that took advantage of the victim's ignorance, and exploited the natural human tendency to help and be liked. The success of a social engineering attack certainly had the right steps for the attacker to carry out the action. There are four steps in the social engineering cycle:



Picture 1. Social Engineering Life Cycle
Source: Chetioui et al. (2022)

The social engineering life cycle in the picture above is the steps of social engineering attacks carried out by frauder. The first step is investigation, Chetioui et al. (2022) stated that in this step the attacker selected the target victim, then extracted information on the background of the victim's life, and then determined the attack method to be used.

The second step is the hook, Chetioui et al. (2022) stated that in this step the attacker approached the victim, and tried to establish a closer relationship to gain trust. The social engineering technique used in this stage to ensure the victim trusts the attacker was to collect data such as names, employee and company details (Airehrour et al., 2018).

The third step is play. Abass (2018) stated that in this step the attacker used manipulation techniques to get the target in an emotional state, so the attacker must study the emotional state of his victim to use this advantage. At this stage the attacker manipulated and exploited trust and steals information secretly such as email spoofs, scam phone calls, or malware installations (Airehrour et al., 2018).

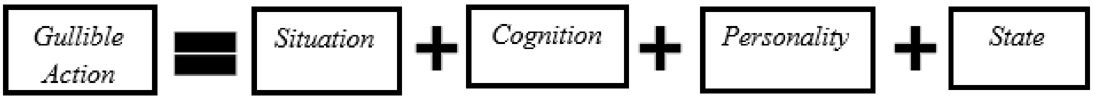
The fourth step is exit. Safitri et al. (2020) stated this exit stage was the stage of completing interactions with victims. At this exit stage, the attacker had received the required information or the victim had carried out the desired command, then the attacker would end communication with the victim and switch to a new target (Chetioui et al., 2022).

The types of social engineering attacked that commonly occur were phishing and skimming. The definition of phishing according to Chetioui et al. (2022) was an attack that tried to get someone's personal information in a misleading way. Furthermore, Shah and Ravi (2012) stated this attack could be via email, short message service, internet protocol, and websites. In addition, according to Hasan and Febriany (2021), skimming was an act of theft of customer data by using a data recording device. The way it worked from skimming was to steal customer data that had been stored on a magnetic strip contained on an ATM card and then sent wirelessly (Enrick, 2019).

Gullibility

This theory was first created by Stephen Greenspan in his book, Annals of Gullibility: Why We Get Duped and How to Avoid It, which provided a comprehensive view of how easy it was to be deceived. According to Greenspan (2008) gullibility could be defined as an unusual tendency to be deceived or taken advantage of. Fraud could happen to everyone. The term fraud referred to a pattern of fraud that repeated itself in different settings, even in warning signs. A person who was gullible involves some degree of coercion, particularly from psychological coercion (Greenspan, 2008).

Currently the use of the internet and social media has increased, so it is not a new thing to find wrong information from these sources. Pan et al. (2021) stated that the popularity of the internet and social media had facilitated people to share misinformation. According to Greenspan (2008), there were four factors that contribute to how easily people were deceived. It was the mixture of these four factors that caused people to be gullible, which has the following formula:

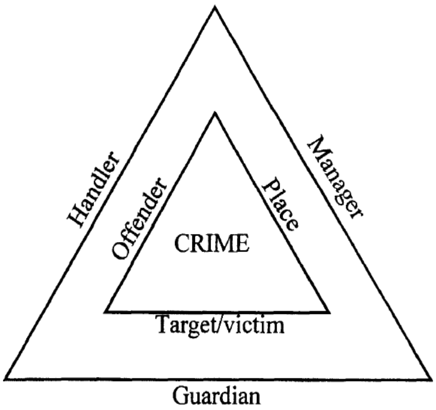


Picture 2. Gullibility formula
Source: Greenspan (2008)

1. The situation, maybe the fraudster was very persuasive, or maybe there was someone else who guarantees his honesty,
2. Cognition, maybe the victim could not read the attitude of the fraudster or did not know the type of investment covered by the scam,
3. Personality, maybe the victim was a very trusted person or difficult to say "no",
4. Circumstances, maybe the victim was tired or drunk or very dependent on the fraudster.

Crime Triangle of Routine Activity Theory

The crime triangle is a theory of environmental criminology which is often called Routine Activity Theory (RAT). This theory was first created by Marcus Felson and Lawrence Cohen in 1979. According to Cohen and Felson (1979) there were three elements in which the crime occurred, as these three elements must be united in the context of the same place or time including the offender, target, place.



Picture 3. Crime Triangel of Routine Activity Theory
Source: (Eck, 2003)

Meanwhile Eck (2003) said that for the latest version of the crime triangle, there were triangles in the outer layer, namely guardian, handler, and manager which function as controllers for each element of the crime triangle in the inner layer. According to Eck (2003) the position of controllers had an important role in preventing crime and had responsibility for the elements that were in the inner layer of the crime triangle. Thus, in this research, the existence of controllers was likened to a bank that had an important role in overcoming a problem experienced by bank customers who were victims of fraud.

Socialization Media

Now, online socialization is easier and more effective because of the presence of an internet network that is easy to find. The internet network facilitates communication between individuals without time and distance limits so that many types of online media appear as a medium for communicating. According to Aditama (2021) social media was a media that was free to use to express and explore one's opinions continuously. Social media could be interpreted as a medium based on internet technology that allowed a person to interact socially, communicate and collaborate, and share with other people (Ratnamulyani and Ike Atikah Maksudi, 2018).

The presence of the internet could be used as an intermediary to convey social engineering prevention and socialization. The use of the internet network made all activities effective and efficient. This could also help the Indonesian banks to socialize social engineering prevention. This research uses social engineering for prevention and socialization using websites and Twitter media.

Website

Currently, many banking companies have websites as a means of supporting information. Setiawan et al. (2021) said that website media has advantages for the company itself, which can be used to introduce the company profile. This can serve to increase public confidence in the performance of the banking company. According to Hasugian (2018), the website media makes it easier for banks to carry out broader and more efficient outreach and public education programs that aim to provide an understanding of the benefits of banking products and services that can be utilized by the public. The web aims to explore relationships across large and complex data sets easily, quickly and interactively (Balzer et al., 2020).

Twitter

Twitter is a social media platform that combines social networking media and microblogs. Setiawan et al. (2021) said that Twitter can be used as a promotional medium for company profile websites. According to Setyadi (2020), Twitter can be a means of interacting with consumers to maintain good relations and provide education for consumers regarding the products or services owned by the company. In addition, Bank Mandiri (2023) states that Twitter can be used as a medium for customer complaints to banks. On social media, Twitter is known as a trending topic," which is indicated by the number of retweets, replies, or mentions. Information can be spread widely and quickly via Twitter because of its retweet feature (Iryanti and Rahman, 2019).

Research Methods

This study utilized a qualitative approach. Saunders et al. (2012) stated that this qualitative research was the process of summarizing parts of the data, categorizing the data, and connecting the categories by creating a structure in order to answer the problem formulation. The method used was archival research. Saunders et al. (2012) defined archival research as a research strategy that used records and documents as the main source resulting from daily activities. The researcher collected complete and in-depth information, starting with observing the social engineering prevention socialization carried out by major banks in Indonesia. The patterns of socialization carried out by these banks have been collected by researchers from the bank's official website and twitter.

This study aimed to analyze social engineering prevention socialization patterns through website and twitter through the media website and twitter. Furthermore, in data collection, this research used secondary data which was documentary in nature. According to Saunders et al. (2012) documentary secondary data whose type of text could be in the form of books, journal articles, magazines, or newspapers. Meanwhile, documentary secondary data which was non-text in the form of sound recordings, videos, pictures, films, television programs, DVDs and CD ROMs, as well as web pages. Thus, in this study, researchers used journal articles, Indonesian Banks' website and twitter social media as media to collect data. The data was taken from January to February 2022 by using the N-Capture feature to capture content on the website and twitter social media. The output of N-Capture was complete data related to the captured account. N-Capture was a default application from Nvivo that was automatically installed on Google Chrome. The use of N-Capture made it easier to obtain research data related to content analysis on website media and Twitter social media, so there was no need to read and analyze posts one by one. The websites and Twitter social media used as data in this study were major banks in Indonesia that had large assets recorded by the OJK and Bank Indonesia including Bank Central Asia (BCA), Bank Mandiri, Bank Negara Indonesia (BNI), Bank Rakyat Indonesia (BRI), Bank Permata, and Bank Syariah Indonesia (BSI).

Furthermore, in analyzing the data, the researcher refers to the data model of Miles and Humberman (1994). First, data reduction through the coding process. Tracy (2013) said that coding is an active process in identifying, labeling, and systematizing data as belonging to or representing several types of phenomena. The coding process is carried out in three stages, namely; open coding, axial coding, and selective coding. Second, data display. Display data in this study using analytical maps display and matrix coding query. Analytical Maps help researchers create analytical maps to illustrate thought concepts related to the topic. While the matrix coding query how often and how many nodes are related to one another. The use of matrix coding queries involves two features, namely text search and word frequency. Third, drawing conclusions, which is a process of reviewing the results of data analysis and assessing the implications of a meaning that arises from the questions that occur during the research process.

Then, the data that has been collected is analyzed using a content analysis approach and its validity is tested using source triangulation which focuses on data obtained from various sources. If the source triangulation technique is associated with this research on social engineering prevention socialization by banks, then testing the validity of the data obtained can be done by looking for information sourced from the official website and social media twitter belonging to the bank which has been validated.

Results and Discussion

In presenting the research results, the researcher refers to the results of content analysis, which has been processed by researchers from the results of the N-Capture Indonesian Banks' website and twitter social media which is then coded using the NVivo 12 Software. The following are the results of data coding and analysis results which can be seen in Figure 4.

Based on the analysis map on Figure 4, the results of research related to socialization patterns in the context of preventing social engineering can be seen in the descriptions below:

Social Engineering Prevention Socialization by Banks Through Website

Socialization through the website is easily conveyed to customers, because the website media makes it easy for customers to find information through the Google search engine so that it is easy to access, practical, and fast. Information provided in social engineering prevention socialization through the websites of Bank Central Asia (BCA), Bank Mandiri, Bank Negara Indonesia (BNI), Bank Rakyat Indonesia (BRI), Bank Permata, and Bank Syariah Indonesia (BSI) include: characteristics of the social engineering, contact service, and steps to prevent social engineering.

Socialization Recognizing the Characteristics of Social Engineering Through Websites

As an initial action to prevent social engineering, namely by recognizing the characteristics of social engineering. The characteristics of social engineering that were informed through the website pages of the big banks include: recognizing fake accounts, often using the mode of claiming to be a bank officer accompanied by offers of unreasonable profits and asking for personal data. This is evidenced by the information provided through the websites of these banks as shown in Table 1.

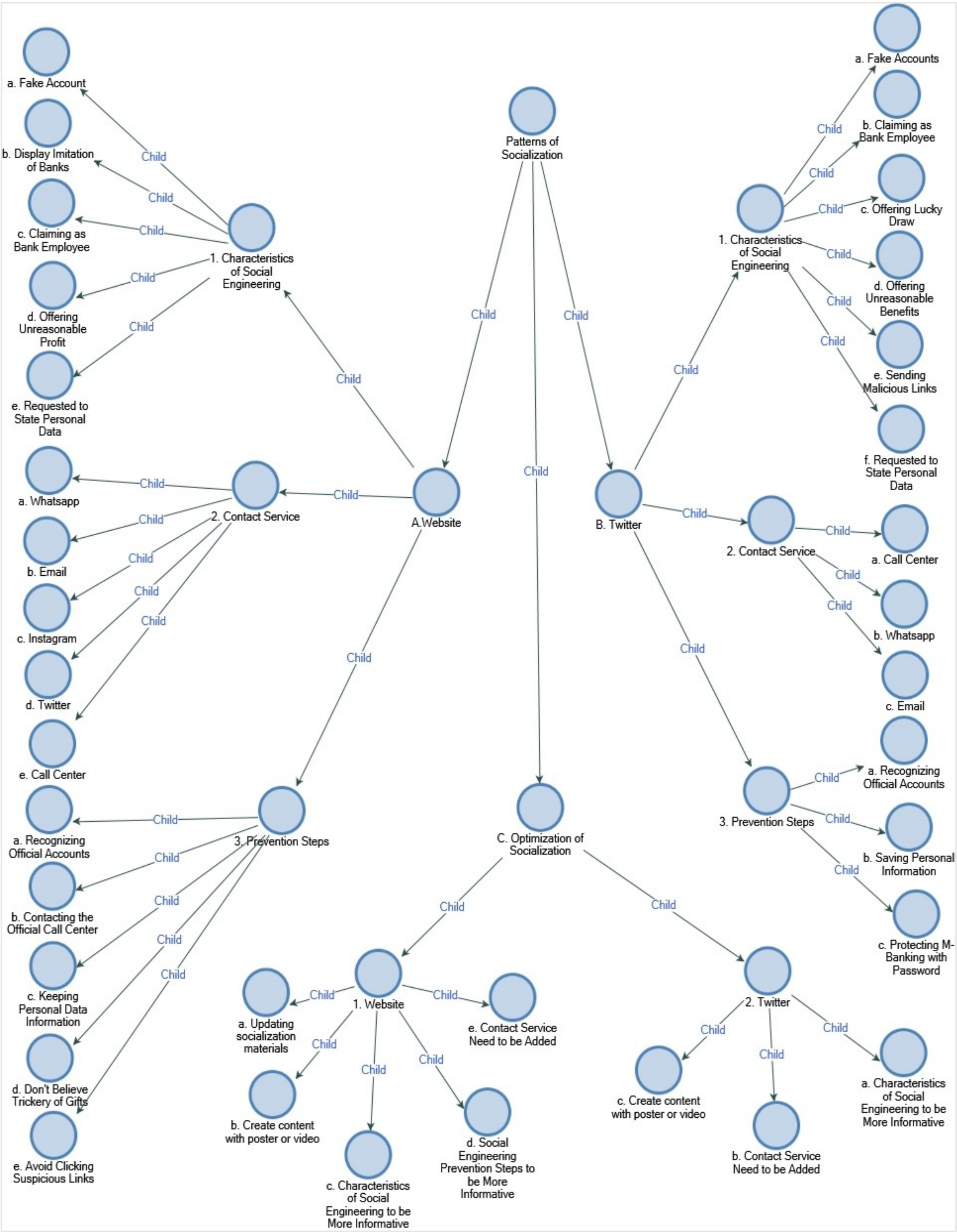

Patterns of Socialization
A.Website
1. Characteristics of Social Engineering
a. Fake Account
b. Display Imitation of Banks
c. Claiming as Bank Employee
d. Offering Unreasonable Profit
e. Requested to State Personal Data
2. Contact Service
a. Whatsapp
b. Email
c. Instagram
d. Twitter
e. Call Center
3. Prevention Steps
a. Recognizing Official Accounts
b. Contacting the Official Call Center
c. Keeping Personal Data Information
d. Don't Believe Trickery of Gifts
e. Avoid Clicking Suspicious Links
B. Twitter
1. Characteristics of Social Engineering
a. Fake Accounts
b. Claiming as Bank Employee
c. Offering Lucky Draw
d. Offering Unreasonable Benefits
e. Sending Malicious Links
f. Requested to State Personal Data
2. Contact Service
a. Call Center
b. Whatsapp
c. Email
3. Prevention Steps
a. Recognizing Official Accounts
b. Saving Personal Information
c. Protecting M-Banking with Password
C. Optimization of Socialization
1. Website
a. Updating socialization materials
b. Create content with poster or video
c. Characteristics of Social Engineering to be More Informative
d. Social Engineering Prevention Steps to be More Informative
e. Contact Service Need to be Added
2. Twitter
a. Characteristics of Social Engineering to be More Informative
b. Contact Service Need to be Added
c. Create content with poster or video
Child

Figure 4. Map Analysis of Social Engineering Prevention Socialization Patterns Through Websites and Twitter
Source: Processed by Researchers Using Nvivo

Table 1. Matrix Coding Socialization of the Characteristics of Social Engineering Through Website Media

Characteristics of Social Engineering	BCA	BNI	BRI	BSI	MANDIRI	PERMATA
1. Fake Account	205	0	82	0	0	0
2. Display Imitation of Banks	143	14	0	0	0	0
3. Claiming as Bank Employee	143	0	**244**	45	35	90
4. Offering Unreasonable Profit	52	0	0	0	35	33
5. Requested to State Personal Data	171	22	100	94	0	0

Source: Processed by Researchers Using NVivo

Table 1 is the socialization of the characteristics of social engineering through website media generated when processing the N-Capture data results on the website pages of banks in Indonesia. Furthermore, in coding, it provides information in "numbers," which means the number of words that often appear from the point of view of the characteristics of social engineering. The prevention socialization provided by the six banks is an appeal to customers to safeguard personal data. Based on Table 1, of all the characteristics of social engineering provided by these banks, BCA contains the most complete information regarding the characteristics of social engineering, namely using fake accounts, displaying social media impersonating parties, claiming to be bank officials or employees, offering unfair advantages, and being asked to provide personal data. Even on the BCA website, it also provides preventive measures for each characteristic of social engineering. One of them is to directly block the fake account.

Socialization of Contact Services Through Website

Social engineering prevention socialization provided by the bank through the website generally includes a bank contact facility that functions as information media needed by customers. Therefore, it is important for customers to recognize the official contact facilities provided by the bank. Major banks in Indonesia have several contact facilities ready to serve customers, including:

Table 2. Matrix Coding Socialization of Contact Services Through Website Media

Contact Service	BCA	BNI	BRI	BSI	MANDIRI	PERMATA
1. Whatsapp	8	0	**305**	0	0	0
2. Email	7	0	171	16	15	3
3. Instagram	22	0	69	52	0	1
4. Twitter	8	0	0	52	11	1
5. Call Center	84	61	69	16	5	3

Source: Processed by Researchers Using NVivo

Table 2 is the socialization of contact services through the media website that was generated when processing the N-Capture data results on the website pages of banks in Indonesia. Furthermore, coding in providing information in the form of "numbers" means the number of words that often appear from the service points of bank contact facilities. Based on Table 2, the six banks above provide information related to contact facilities that can be contacted by customers, including WhatsApp, email, Instagram, Twitter, and call centers, which are posted on the web pages of these banks. Table 2 shows that the WhatsApp contact service provided by BRI is the most mentioned on its web page compared to other banks' contact facilities. This is evidenced by the number of words that appear in the WhatsApp contact point in Table 2, namely 305 words.

Socialization of Social Engineering Prevention Steps Through Website

Customers need to know how to prevent social engineering fraud so they don't become victims of it. These steps include recognizing official accounts, contacting official call centers, keeping personal data information, don’t believe trickery of gifts, and avoiding clicking on suspicious links. In the following, the researcher will describe several steps to prevent social engineering fraud that are published on the websites of official banks:

Table 3. Matrix Coding Socialization of Social Engineering Prevention Steps Through Website

Social Engineering Prevention Steps	**BCA**	**BNI**	**BRI**	**BSI**	**MANDIRI**	**PERMATA**
1. Recognizing Official Accounts	**505**	67	66	45	25	0
2. Contacting the Official Call Center	120	55	209	0	31	0
3. Keeping Personal Data Information	185	44	137	49	85	78
4. Don't Believe Trickery of Gifts	21	58	0	45	0	0
5. Avoid Clicking Suspicious Links	0	17	0	0	31	0

Source: Processed by Researchers Using NVivo

Table 3 is the socialization of social engineering prevention steps through the website generated when processing the results of N-Capture data on the website pages of banks in Indonesia. Furthermore, the coding provides a "numbers" description which means that the number of words that often appear from the points of steps to prevent social engineering. Based on Table 3, the socialization of social engineering prevention steps is mostly mentioned by BCA on its web page, namely prevention step by recognizing the bank's official account, which is marked by the number of words mentioned on its web page, which is 505 words.

Based on the data above, the social engineering prevention socialization through the media website carried out by the six banks contained information about the characteristics of social engineering, contact service facilities, and steps to prevent social engineering. However, the socialization provided by the six banks was still not optimal in conveying socialization to the prevention of social engineering through media website, including: (1) The bank does not upgrade information regarding social engineering prevention socialization, so that the information provided is still with the old issues and the prevention is still the old way. As for the banks that have not upgraded their socialization materials with the latest issues, including Bank Mandiri, BNI, BSI; (2) In distributing socialization content through the website, it is necessary to display interesting readings so that customers are enthusiastic about reading. Not only black text writing with a plain website background, but social engineering prevention socialization can be distributed in the form of posters that have unique and interesting visualizations like those done by Bank Permata and BRI; (3) The first precaution that can be taken is to identify the characteristics of social engineering. However, there are several banks that do not provide complete socialization of the characteristics of social engineering, namely frauder use fake accounts as intermediary media. The banks are BNI, BSI, Bank Mandiri, and Bank Permata. (4) Based on the results of data processing, the information provided by BCA, BRI, BSI, and Bank Permata does not completely provide preventive measures, namely avoiding clicking on links that are deemed suspicious, because basically social engineering can occur starting from sending links that are dangerous for customers. These links generally direct victims to fill in customer privacy data. So, it is necessary to socialize related to this; (5) The socialization of the contact facilities provided by BNI through the website is not yet complete. In addition to the call center, banks need to provide other means of contact so that customers can easily communicate with the bank. Such as contact services using social media, namely Instagram, Twitter, and email.

Social Engineering Prevention Socialization Through Twitter

Tweets made by banks regarding social engineering generally provide information on the characteristics of social engineering, contact service, and steps to prevent social engineering. However, there are differences in socialization through the website and twitter, namely socialization on the website is more informative, because the website can contain information without any word limits, while twitter when making a tweet has a limit of 280 characters. Therefore, socialization through twitter is dominated by information that has short sentences. In the following, the researcher will describe the patterns of bank socialization in preventing social engineering provided through twitter.

Socialization Recognizing the Characteristics of Social Engineering Through Twitter

Various social engineering techniques often make people become victims and suffer financial losses that are not small. Therefore, efforts are needed to be able to recognize some common characteristics when there are parties who will commit fraud. Based on Table 4, there are six characteristics of social engineering posted on the bank's official twitter account, including:

Table 4. Matrix Coding Socializing the Characteristics of Social Engineering Through Twitter

Characteristics of Social Engineering	BCA	BNI	BRI	BSI	MANDIRI	PERMATA
1. Display of Twitter Accounts Impersonating Banks (Fake Accounts)	55	133	240	302	**3298**	17
2. Claiming as Bank Employee	85	446	195	329	217	43
3. Offering Lucky Draw	0	0	0	107	0	90
4. Offering Unreasonable Benefits	10	0	38	0	0	49
5. Sending Malicious Links	0	0	74	119	123	0
6. Requested to State Personal Data	12	69	79	238	3148	323

Source: Processed by Researchers Using NVivo

Table 4 is the socialization of the six characteristics of social engineering through the twitter media generated when processing the results of N-Capture data on twitter accounts of Indonesia banks. Furthermore, in coding, it provides information "numbers" which means the number of words that often arise from points of characteristics of social engineering. Based on Table 4, of all the characteristics of social engineering provided by the six banks, Bank Mandiri contains the most information about the characteristics of social engineering, namely the appearance of a twitter account imitating the bank or a fake account. In order to socialize about fake twitter accounts, Bank Mandiri tweets mentions many fake accounts to inform their followers to be careful and not easy to believe if they are contacted by the fake account. The prevention steps taken by Bank Mandiri are interesting and of course this method is different from socialization from other banks, because Bank Mandiri itself looks for fake accounts that can be dangerous for its customers, so that followers can find out the fake accounts. As this is proven by the number of words mentioned in this tweet, which is 3298 words.

Socialization of Contact Services Via Twitter

Currently, bank contact services are not only call centers but most bank contact services have utilized social media. In the following, the researcher will describe some of the contact service services that are published through twit posts on the bank's official twitter account.

Table 5 is the socialization of contact facilities through twitter media which is generated when processing the results of N-Capture data on twitter accounts of banks in Indonesia. Furthermore, the coding provides a "numbers" description which means that the number of words that often appear from the service points of the bank contact facility. Call center contact facility services are carried out via calls with bank customer service, so that bank communication with customers can be direct. Meanwhile, the WhatsApp contact facility can exchange messages, make calls, and send various forms of documents. The Whatsapp service does not require credit, however, you must prepare an internet network. As with WhatsApp, email can also send messages in various forms of documents, such as audio, video, image files. However, email services cannot make direct calls between customers and bank customer service.

Table 5. Matrix Coding Socialization of Contact Services Through Twitter Media

Contact Services	BCA	BNI	BRI	BSI	MANDIRI	PERMATA
a. Call Center	15	114	116	72	109	0
b. Whatsapp	19	**1192**	43	0	0	0
c. Email	0	0	0	0	27	0

Source: Processed by Researchers Using Nvivo

Based on Table 5, the contact services provided by the six banks are through tweet posts, BNI is the one who mentions the whatsapp contact service the most in their tweet posts. This is shown in Table 5, which is evidenced by the number of words the whatsapp contact service mentioned in the tweet, which is 1192 words. In order to socialize the whatsapp contact service, the socialization pattern carried out by BNI begins with responding to problems or complaints experienced by customers by replying to the customer's account in a tweet. Then, BNI directs its customers to contact BNI's whatsapp business contact with a green check with number 08115881946.

Socialization of Social Engineering Prevention Steps Through Twitter

At the time of the incident, the victim may not realize that his personal data has been stolen by the frauder and result in the victim losing personal data, because the victim does not have knowledge of the preventive steps that must be taken to avoid social engineering attacks. Thus, customers need to understand and learn about steps to prevent social engineering. Therefore, the researcher will describe several steps to prevent social engineering which are published through tweets on the bank's twitter account which are listed in Table 6:

Table 6. Matrix Coding Socialization of Social Engineering Prevention Steps Through Twitter

Social Engineering Prevention Steps	BCA	BNI	BRI	BSI	MANDIRI	PERMATA
a. Recognizing Official Accounts	67	2320	235	39	**3299**	17
b. Saving Personal Information	105	35	286	235	**3315**	127
c. Protecting M-Banking with Password	29	0	128	45	0	43

Source: Processed by Researchers Using Nvivo

Table 6 is the socialization of the steps to prevent social engineering through twitter generated when processing the results of N-Capture data on twitter accounts of banks in Indonesia. Steps to prevent social engineering include recognizing official accounts, saving personal information, and protecting m-banking with passwords in coding provides a "numbers" description which means that the number of words that often appear from the points of steps to prevent social engineering. Based on Table 6, the steps to prevent social engineering provided by the six banks through tweet, Bank Mandiri mostly mentions the steps to prevent social engineering in their tweet, namely providing preventive measures by recognizing official accounts with 3299 words, and the second step is to keep personal information which has 3315 words. In order to socialize the steps to prevent social engineering through twitter media, Bank Mandiri continues to urge its followers on twitter to be careful of irresponsible accounts that are in the name of Bank Mandiri accounts and do not provide confidential data to anyone. In addition, Bank Mandiri's tweet reminded to followers for recognize the official Bank Mandiri verified twitter account.

Based on the data above, social engineering prevention socialization through twitter media carried out by banks contains information about the characteristics of social engineering, contact service facilities, and steps to prevent social engineering. Twitter as media of socialization can be said to be successful if it provides the right information and is needed by its followers. Of course, the socialization provided must be clear and informative, so that the socialization provided can be well received by the reader. However, social engineering prevention socialization carried out by Bank Mandiri, Bank Central Asia (BCA), Bank Rakyat Indonesia (BRI), Bank Negara Indonesia (BNI), Bank Permata, Bank Syariah Indonesia (BSI) was still not optimal in conveying socialization to the prevention of social engineering through twitter, including: (1) Does not provide complete information about the characteristics of social engineering such as BCA, BNI, BRI, Bank Mandiri and Bank Permata does not include the mode of offering lottery prizes; (2) The socialization provided by BCA, BNI, BRI, Bank Permata provided a call center contact facility, but did not include an email contact service. E-mail contact service is also important, because e-mail can help customers to send a lot of documents to the bank and have flexibility in communicating with other people; (3) The socialization carried out by BNI through twitter is still monotonous, because the tweets are dominated by text without any pictures or videos.

Optimization of Bank Websites in Social Engineering Prevention

Banks must provide informative and useful socialization for their customers so that socialization through the website is conveyed properly and optimally, so that some improvements are needed in conveying social engineering prevention socialization through website media. These improvements include: (1) Social engineering prevention socialization distributed through Bank Mandiri, BNI, BSI needs to update the socialization material, because social engineering attacks each year have different types of attacks and added technology is growing which makes the birth of more diverse types of social engineering, so there are also ways to prevent social engineering attacks with new types; (2) Website is a medium that can share images, videos, and text, so that this can be used by banks as a means to optimize social engineering prevention socialization. Therefore, BCA, BNI, Bank Mandiri, BSI can create useful content using poster images or videos that attract customers to view; (3) Socialization regarding the characteristics of social engineering must contain complete information and use language sentences that are easy for customers to understand. The characteristics of social engineering that often occur are using fake accounts, displaying websites or other social media that imitate the bank, claiming to be bank officials or employees, offering unreasonable benefits, being asked to mention personal data. Therefore, BNI, BSI, Bank Mandiri, and Bank Permata can complete the characteristics of social engineering to be more informative; (4) Socialization of social engineering prevention steps must provide complete information. This needs to be done by BCA, BRI, BSI, Bank Permata to complete information on preventive step, namely avoiding clicking suspicious links; (5) Socialization of contact service facilities by BNI is not only for the call center. BNI needs to have other alternative ways so that customers have no difficulty in contacting BNI, which can include BNI's social media and email. This is considering that people nowadays access social media and email more in their daily lives.

Optimization of Bank Twitter in Social Engineering Prevention

Social engineering prevention socialization must contain clear and informative information, so banks need to pay attention to the quality of the information provided so that the socialization provided is successful. As for the improvements that need to be made by banks related to social engineering prevention socialization through twitter media, including: (1) Socialization of the characteristics of social engineering must contain clear and complete information, because recognizing the characteristics of social engineering can be the first step to prevent attacks. Therefore, BCA, BNI, BRI, Bank Mandiri and Bank Permata need to add a social engineering mode by offering lottery prizes, because this mode often occurs so that victims want to hand over personal information to perpetrators; (2) It is important to include contact service services in tweets regarding social engineering prevention socialization. BCA, BNI, BRI, Bank Permata need to have a variety of contact facilities, not only call centers, but can include bank email addresses. E-mail contact service is also important, because e-mail can help customers to send documents in large quantities or even simply submit a complaint report to the bank; (3) BNI can provide socialization not only through posting text on twitter, but can also provide poster images or videos that contain complete information about preventing social engineering modes, so that socialization is more optimal and can attract customers' interest in reading.

Conclusion

Social engineering is a psychological attack that attacks humans by exploiting weaknesses or by tricking their victims. Therefore, awareness is needed from humans themselves to understand how the characteristics of social engineering and prevention steps are needed to avoid the mode of social engineering. Thus, the position of banks in Indonesia as controller elements has an important role to overcome the social engineering experienced by bank customers, namely by providing socialization regarding the prevention of social engineering modes to bank customers through the website and social media twitter. The provision of this socialization can reduce the gullibility element in customers, because it can strengthen the customer's way of thinking (cognition) by increasing knowledge about social engineering modes and customers are not easily trapped in the elements of the situation that have been designed by the perpetrators.

The six banks in this study including Bank Central Asia (BCA), Bank Mandiri, Bank Negara Indonesia (BNI), Bank Rakyat Indonesia (BRI), Bank Permata, and Bank Syariah Indonesia (BSI) have different socialization patterns regarding the prevention of social engineering. The socialization that was distributed by BRI through the media website provided more information about the characteristics of social engineering and contact services. Meanwhile, BCA provides more information about social engineering prevention steps by recognizing the bank's official accounts. Furthermore, the bank that is active in providing socialization related to the prevention of social engineering through twitter is Bank Mandiri. Bank Mandiri provides more socialization about steps to prevent social engineering, responding to customer reports regarding social engineering and mentioning fake accounts to be socialized to their followers as an effort to prevent social engineering. In addition, the socialization of contact services through twitter media was mostly provided by BNI, which mentioned a lot of whatsapp contact service in their tweets. Optimization of socialization through the website and twitter can be done by creating content that contains complete and up to date information about the characteristics of social engineering, contact service facilities, and steps to prevent social engineering that can be visualized in the form of videos or poster images that are designed to attract customers interest in reading.

References

Abass, I. A. M. (2018). Social engineering threat and defense: A literature survey. *Journal of Information Security*, *09*(04), 257–264. https://doi.org/10.4236/jis.2018.94018

Aditama, R. (2021). Penegakan hukum cyber crime terhadap tindak pidana pencurian uang nasabah dengan cara pembajakan akun internet banking lewat media sosial. *Wajah Hukum*, *5*(1), 118. https://doi.org/10.33087/wjh.v5i1.360

Airehrour, D., Nair, N. V., & Madanian, S. (2018). Social engineering attacks and countermeasures in the New Zealand banking system: Advancing a user-reflective mitigation model. *Information (Switzerland)*, *9*(5). https://doi.org/10.3390/info9050110

Badan Siber dan Sandi Negara. (2020). *Rekap serangan siber (Januari – April 2020).* https://bssn.go.id/rekap-serangan-siber-januari-april-2020/

Balzer, C., Oktavian, R., Zandi, M., Fairen-Jimenez, D., & Moghadam, P. Z. (2020). Wiz: A web-based tool for interactive visualization of big data. *Patterns*, *1*(8), 100107. https://doi.org/10.1016/j.patter.2020.100107

BSSN. (2022). *Berkomitmen kawal tingkat kematangan keamanan siber sektor keuangan, BSSN gandeng OJK selenggarakan workshop penilaian kematangan keamanan siber.* https://bssn.go.id/berkomitmen-kawal-tingkat-kematangan-keamanan-siber-sektor-keuangan-bssn-gandeng-ojk-selenggarakan-workshop-penilaian-kematangan-keamanan-siber/

Chetioui, K., Bah, B., Alami, A. O., & Bahnasse, A. (2022). Overview of social engineering attacks on social networks. *Procedia Computer Science*, *198*(2021), 656–661. https://doi.org/10.1016/j.procs.2021.12.302

CNN Indonesia. (2022). *BSSN catat 1,6 miliar insiden keamanan siber sepanjang 2021.* https://www.cnnindonesia.com/teknologi/20220330181041-192-778082/bssn-catat-16-miliar-insiden-keamanan-siber-sepanjang-2021

Eck, J. (2003). Police problems: The complexity of problem theory, research and evaluation. *Crime Prevention Studies*, *15*, 79–113.

Enrick, M. (2019). *Pembobolan ATM menggunakan teknik skimming kaitanya dengan pengajuan restitusi.* *2*(2), 555–580.

Gibbs, T. (2020). Seeking economic cyber security: a Middle Eastern example. *Journal of Money Laundering Control*, *23*(2), 493–507. https://doi.org/10.1108/JMLC-09-2019-0076

Greenspan, S. (2008). *Annal of gullibility: Why we get duped and how to avoid it.* Santa Barbara, CA: ABC-CLIO.

Hasan, A., & Febriany, L. (2021). Identifikasi tindakan pengawasan dan pencegahan terhadap kejahatan finansial perbankan syariah selama masa pandemi COVID 19. *Jurnal Ilmiah Akuntansi dan Keuangan*, *4*(4), 1089–1090. https://doi.org/26222191

Hasugian, P. S. (2018). Perancangan website sebagai media promosi dan informasi. *Journal of Informatic Pelita Nusantara*, *3*.

Iryanti, Y. S., & Rahman, M. A. (2019). Promosi perpustakaan melalui media sosial twitter di perpustakaan hukum Daniel S. Lev. *Edulib*, *9*(2), 128–143. https://doi.org/10.17509/edulib.v9i2.17763

Junaedi, D. I. (2017). Antisipasi dampak social engineering pada bisnis perbankan. *Jurnal Ilmu-Ilmu Informatika dan Manajemen STMIK*, *11*(No.1). https://doi.org/1978-3310

Kävrestad, J. (2018). Fundamentals of digital forensics. In *Fundamentals of Digital Forensics* (Second). Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-319-96319-8

KOMPAS. (2022). *Pasutri di Padang jadi korban phising Rp 1,1 miliar, OJK Sumbar minta warga hati-hati.* https://regional.kompas.com/read/2022/06/10/181226578/pasutri-di-padang-jadi-korban-phising-rp-11-miliar-ojk-sumbar-minta-warga?page=all&lgn_method=google

Pan, W., Liu, D., & Fang, J. (2021). An examination of factors contributing to the acceptance of online health misinformation. *Frontiers in Psychology*, *12*(March), 1–11.

https://doi.org/10.3389/fpsyg.2021.630268

Ratnamulyani, Ike Atikah Maksudi, B. I. (2018). Peran media sosial dalam peningkatan partisipasi pemilih pemula dikalangan pelajar di Kabupaten Bogor. *Jurnal Ilmu - Ilmu Sosial Dan Humaniora*, *20*(2), 154–161. https://doi.org/1411 - 0903

Rebovich, D.J., Layne, J., Jiandani, J., & Hage, S., (2000). *The national public survey on white-collar crime.* Morgantown, WV: National White Collar Crime Center.

Safitri, E. M., Ameilindra, Z., & Yulianti, R. (2020). Analisis teknik social engineering sebagai ancaman dalam keamanan sistem informasi: Studi literatur. *Jurnal Ilmiah Teknologi Informasi Dan Robotika*, *2*, 21–26. http://jifti.upnjatim.ac.id/index.php/jifti/article/view/26

Saunders, Lewis, & Thornhill. (2012). Research methods for business students. *International Journal of the History of Sport*, *30*(1).

Setiawan, D., Baraja, A., & Sukoco. (2021). Pembuatan company profile berbasis website pada PT Aether Digital Indonesia. *Surakarta Informatic Journal*, *3*. https://doi.org/2621-5330

Shah, A., & Ravi, S. (2012). *A to Z of cyber crime*. Lexcode Education & Assessment Platform (LEAP).

Titus, R. M., Gover, A. R. (2001). Personal fraud: The victims and the scams. *Crime Prevention Studies*, *12*, 133–151.

Tracy, S. J. . (2013). *Qualitative research methods: Collecting evidence, crafting analysis, communicating impact* (1st ed.). John Wiley & Sons, Ltd.,. https://doi.org/10.5613/rzs.43.1.6

Wall, D. S. (2017). Towards a conceptualisation of cloud (cyber) crime. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *10292 LNCS*(July), 529–538. https://doi.org/10.1007/978-3-319-58460-7_37

We are social. (2022). Indonesian digital report 2022. In *We Are Social* (p. 113). https://datareportal.com/reports/digital-2021-indonesia