Berkala Ilmu Perpustakaan dan Informasi, Vol. 18, No. 2, Desember 2022, Hal. 326-337
https://doi.org/10.22146/bip.v18i2.5866
ISSN 1693-7740 (Print), ISSN 2477-0361 (Online)
Tersedia online di https://journal.ugm.ac.id/v3/BIP

Information items used by online fraudsters and their relationship to Indonesian digital literacy

Ardoni
Library and Information Science Study Program, Faculty of Languages and Arts, Universitas Negeri Padang
Jalan Prof. Dr. Hamka, Kampus Air Tawar Padang, 25131
e-mail:ardoniyonas@gmail.com

Submitted: October 17, 2022, Revised: October 31, 2022, Accepted: November 15, 2022

ABSTRAK

Pendahuluan. Penelitian ini dilakukan untuk mengetahui item informasi yang digunakan oleh penipu online terkait dengan tingkat literasi digital masyarakat. Penelitian ini dilakukan pada pilar keamanan data dalam literasi digital.
Metode penelitian. Pengumpulan data dilakukan dengan menonton video di Youtube, mewawancarai masyarakat secara online yang mengadukan penipuan yang dialaminya di Facebook dan Whatsapp periode 2019-2022.
Data analisis. Data dianalisis secara deskriptif dan diklasifikasikan untuk menggambarkan butir-butir informasi yang digunakan oleh penipu online.
Hasil dan Pembahasan. Butir-butir informasi yang sering digunakan oleh penipu online adalah istilah layanan perbankan, URL asli tetapi palsu, prosedur operasi standar polisi, dan istilah bahasa Inggris yang digunakan oleh pasar. Oleh karena itu, diperlukan sosialisasi yang berkesinambungan dari institusi terkait butir-butir informasi tersebut untuk meningkatkan literasi digital masyarakat yang berpotensi menimbulkan kerugian finansial. Dalam hal sosialisasi, perpustakaan dapat berperan secara proaktif.
Kesimpulan dan Saran. Butir informasi yang sering digunakan oleh penipu online adalah informasi terkait layanan perbankan, polisi, *marketplace*, dan akun media sosial palsu. Penelitian ini dapat dilanjutkan untuk mengetahui seberapa rendah ketidaktahuan korban terhadap item informasi tersebut.
Kata kunci: literasi digital; penipu online; item informasi; kerugian finansial

ABSTRACT

Introduction. *This research was conducted to examine the information items used by online fraudsters related to the level of digital literacy of the society. This research was done on the pillars of data security in digital literacy.*
Data Collection Methods. *Data was collected by watching videos on Youtube, online interviewing people who complained about the fraud they experienced on Facebook and Whatsapp in the period of 2019-2022.*
Data Analysis*. The data was descriptively analyzed and classified to describe information items used by the fraudsters.*
Results and Discussion. *The items used by the fraudsters are banking service terms, real but fake URLs, police standard operating procedures, and English terms used by market place. Therefore, continuous socialization from institutions related to these items of information is needed to improve digital literacy of society which has the potential to cause financial losses. In terms of socialization, libraries can play a proactive role.*
Conclusion*. Information items that often used by online fraudsters are information related to banking services, police, marketplace, and fake social media accounts. This research may be continued to understand how low the victims' ignorance about the information items.*

Keywords: *digital literacy; online fraudster; items of information; financial losses*

A. INTRODUCTION

The digital literacy level of the Indonesian people is in the 56th position out of 63 countries (Indonesia Baik, 2021). Indonesia is under Turkey, Jordan, Romania, Brazil and Bulgaria and above Ukraine, Croatia, Mexico and Peru (Statista, 2022). This position reflects that the Indonesian people are people who have a low digital literacy index. Digital literacy itself consists of four pillars, namely digital culture, digital ethics, digital skills, and digital safety. *First*, digital culture is a workplace where digital tools and technologies are widely used (Slack Team, 2022). In such places, workers use digital technology for various work activities. A library that has implemented a fully automated system can be called a place of high digital culture. *Second*, maintaining comfort is important in using digital technology. For that, it is necessary to set a series of rules and procedures. These rules and procedures are called digital ethics (Kusuma, 2020). *Third*, digital skills include skills using a computer or smartphone (RT Katalisnet, 2022). Today, in the workplace, especially one shaped by digital culture, digital skills are becoming very important. Almost every job vacancy lists these skills as one of the requirements for applicants (Indeed Editorial Team, 2022). *Fourth*, personal data protection and digital security are two things that need to be recognized, implemented and realized by everyone involved in the digital world (Agustini, 2021). In today's digital era, personal data is used as metadata for various accounts, including bank accounts. Included in digital safety, a person's knowledge of items of information that need to be kept confidential when requested online by others. Likewise, of the four pillars of digital literacy, digital safety has the lowest score compared to the other three pillars (Indonesia. Kementerian Komunikasi dan Informasi, 2022).

This situation leads to various kinds of negative impacts. One of the negative impacts is that some Indonesian easily believed hoax information. Another negative impact is the rise of online fraud using digital information (Indonesia. CNN, 2022). According to Analytics Insight(Prambors, 2022), in terms of the number of frauds (online and offline), Indonesia is in sixth place behind Nigeria, India, China, Brazil, and Pakistan. A large amount of fraud cases in Indonesia implies that the people (potential victims of fraud) live in the digital era, but still, they have manual way of thinking. The low digital literacy of the community potential to be used by online fraudsters to gain financial advantage. The fraudsters use information that their victims do not understand and gain financially from their actions. The fraudsters use various communication devices, especially telephones in carrying out their actions. The fraudsters then lead the potential victim to ATM (Automated Teller Machine) to send some funds, knowingly or not.

Through cursory observation, the victims of these frauds are spread across various levels of education, place of residence, ages, gender, etc. Victims come from any economic group, from low to high. Anyone is the potential to become a victim of these crimes. By the end of 2021, the number of reported online fraud cases in Indonesia was 115.756 (Digidata, 2022). That number could be much higher because many cases go unreported. Victims who do not report this may be due to shame or lack of evidence that can legally prosecute fraudsters. From time to time, the number did not decrease, but increased (including an increasing variety of modes) and resulted in financial losses suffered by the victims (Ponce et al, 2022). One of the cases of online fraud via cell phones even made a loss of hundreds of millions of rupiah (Erik, 2022). More precisely, the number of funds the fraudsters managed to control was Rp.222.9 million. The victim lost that much money in just 52 minutes. In October 2022, there was also an online fraud that caused hundreds of millions of rupiah losses (Supriadi, 2022). The loss suffered by the victim was Rp105 million. That much money disappeared from the victim's account.

The rise of online fraud cases is in line with the large number of articles discussing the case. A Google search result for "online fraud in Indonesia" is 12,100,000 recalls. However, the number of online fraud perpetrators who are punished is very small, even the number of fraudsters who are caught is not much

(Rahmanto, 2019). Nowadays, eradicating the crime of online fraud may be difficult to do. However, online frauds are unlikely to go unpunished. Online fraud should at least be prevented. One of the possible prevention efforts is to study the mode of operation of online fraud. Regarding digital literacy, the effort is to find out what items of information are often used by online fraudsters. This research was conducted to find out the items of information that are often used by fraudsters. The results of this study can be expected to be a starting point for increasing digital literacy as well as reducing the number of online frauds. The results of this study are also expected to be the basis for further research.

B. LITERATURE REVIEW

Research on digital literacy is quite a lot both in Indonesia and abroad. Some of them are research on digital literacy competencies for teachers and students (Asari et al., 2019). Fauzi and Marhamah (2021) research the effect of digital literacy on the prevention of hoax information. Another research is about the legal analysis of policies to accelerate digital literacy conducted by Indradi and Hendryanto (2022). Research related to digital literacy was also carried out by Lee et al. (2022), namely about the influence of digital literacy programs on the digital social behavior of the elderly. Another research is about the relationship between librarian performance and digital literacy (George et al., 2022). Digital literacy was also investigated concerning the increased use of e-learning applications (Ilham et al, 2022). Then, there was research conducted by Hayden (2020) on the development of digital literacy through digital universities. Finally, Johan et al. (2020) carried out research on society's literacy, namely the use of social media to improve public literacy.

However, research on the relationship between digital literacy and online fraud was not found. Digital literacy research is more directed at the influence of digital literacy in education or measuring the level of digital literacy. Research on digital literacy is also research to find ways to improve digital literacy itself. Similar to that, research on online fraud is not associated with digital literacy, but with the application of law (Rahmanto, 2019). Other research is about legal studies of online fraud cases (Rahmad, 2019). Online fraud cases are seen as mere legal events, even though the cause of the case could be due to other triggering factors. The Indonesian people's digital literacy index is relatively low, which makes fraudsters take advantage of this opportunity; the occurrence of crime is not only because of the intention of the perpetrator but also because there is an opportunity (Zainal, 2017).

According to the American Library Association (ALA), digital literacy is "the ability to use information and communication technologies to find, evaluate, create, and communicate information, requiring both cognitive and technical skills" (ALA, 2022). The ability to examine and understand the meaning of information and assess the credibility of information sources is the scope of digital literacy skills (Martens & Hobbs, 2015). It is implied that digital literacy includes the ability to evaluate the information received and determine whether a piece of information can be conveyed/disseminated or not. These two items are related to one of the four pillars of information, namely digital safety (Agustini, 2021).

The Digital Safety pillar has the lowest score compared to the other three pillars. The Digital Safety pillar score was 3.1. The other three pillars, namely Digital Culture got the highest score (3.9), followed by the Digital Ethics pillar with a score of 3.53 and Digital with a score of 3.44 (Indonesia. Kementerian Komunikasi dan Informasi, 2022). Digital literacy is the ability to evaluate both received and disseminated information (Jansen et al, 2013). Evaluation of the information received is influenced by knowledge of the content of that information. Likewise, the evaluation of the information disseminated is influenced by whether or not the information is disseminated. The items of information received by the victim from the fraudster should be evaluated by the victim.

This study was conducted to determine the items of information used by online fraudsters who take advantage of the low digital literacy index of the community. This research is expected to be the first step in reducing the impact of low digital literacy. Increasing digital literacy is not an effort that can be done in a short time, but gradually in the long term.

C. RESEARCH METHODS

This type of research is descriptive research (Creswell, 2012). The data collected and analyzed are the terms used by fraudsters. Data is collected by listening to the fraud process from start to finish. The items of information recorded are the ones that fraudsters most frequently cite. The data was presented descriptively. The main data was obtained through observations, in the period from 2019 to 2022, of fraudulent videos on YouTube (Rosenthal, 2018). Observations conducted were using the YouTube algorithm (Skerrett, 2019) that displays videos with related themes. This makes "snowball-like" sampling (Sugiyono, 2014). The data from YouTube obtained were viewed through online fraudulent videos. In the video, there is a conversation between the fraudster and his or her potential victim. The content of the conversation was noted in writing, especially the terms that reflect the items of information used by the fraudster. The same topic video will automatically play when autoplay is activated. Since the topic is online fraud in Indonesia, the videos that are played automatically are videos uploaded by Indonesians. For Facebook and Whatsapp data sources, data collection is not carried out routinely. Data was collected based on cases found in both Whatsapp groups and comments on Facebook. This data is treated as supporting data because the data collected was obtained incidentally.

Data validation was done by triangulation of sources (Hayati, 2022). In validation, data checks from various Youtube channels that have the same fraudulent video are carried out. In addition, validation was also conducted by time triangulation, namely extending the observation period, so that data collection took place within the 2019-2022 period. The data was analyzed using content analysis to get a contextual understanding of the data(Alan, 2011). To get a better understanding, the data are classified and partially reduced before being analyzed (Advernesia, 2020). In classifying, institutions or services, activity, and the terms were used as facets. There were data that had to be reduced because the terms found were not related to digital literacy. Therefore, data that can be analyzed are those that meet the validity technique requirements based on some steps of Huberman (Laugu, 2019). The data collection flowchart is as shown in the following figure.

D. RESULTS AND DISCUSSION

Based on the data obtained, it was found that there were four groups of institutions which related to digital literacy: banking services, police, marketplaces, and fake social media accounts. On banking services, the items of information used are ATM service terms and customer personal data theft. In police agencies, fraudsters use information about distorted standard operating procedures. Items of information related to the marketplace are cash-back, prizes, and communication outside the marketplace application. Fraudsters also take advantage of the victim's ignorance of the emblem of an institution's official social media account. The information items classification is shown in the table below.

1. Banking Services

The fraudsters ask the victims to do something that can withdraw the victim's account. The withdrawal of funds from the victims' accounts can be done by the victims themselves or by the fraudsters. During fraud, the fraudsters guide the victim to select a menu and type in codes.

a. ATM Service Terms

The frauds were carried out by using terms in a foreign language (English). There are four terms those meanings are changed according to the interests of the fraudsters. The terms are e-cash, transfer, OTP, and Briva.

1) e-Cash

The term e-cash is used in one of the menus of a bank's ATM service. This service allows users to make financial transactions without having to have a bank account (Qu et al, 2022). e-Cash makes cell phones a substitute for credit/debit cards. As the "account number," the phone number on the cellphone is used (Naik & Singh, 2021). The e-cash menu at the ATM is a menu for top-up services to the smartphone of the e-cash number owner. By doing a top-up, the smartphone is filled with a number of funds that can be used to pay electronically for a purchase transaction. So to make cashless payments, it is not needed an e-money card, debit card, or credit card.

By fraudsters, the term e-cash was changed and its meaning was conveyed to victims of fraud. To the victim, the fraudster stated that e-cash was an ATM facility to withdraw funds in cash, even though the victim was guided to top-up the fraudster's cellphone number. The cellphone number typed by the victim was referred to as the receipt code by the fraudster. This scam made the victim deposit some money into the fraudster's (smartphone) account. The fraudster's account number was entered by the victim because the fraudster convinces the victim that it was a code number to receive a certain prize. The e-cash menu will then ask to type the number of funds that would be topped up to the smartphone; the victim filled in because the fraudster said that the field for filling in the funds was filling in the reward activation code.

2) Transfer

In ATM, the term transfer (in the Bahasa Indonesia menu group) is a word taken from English. The menu is a service facility that allows ATM users to send funds to the destination account. In this menu, ATM users are asked to fill in the destination account number and the number of funds to be sent. This fraud began with a call from the victim by the fraudster who informs that the victim gained some funds (gifts or cashback) from an institution. The victim was asked to go to an ATM to withdraw the funds in cash. In ATM, the victim was asked to choose an Indonesian menu on the ATM's main menu.

The fraudster then asks the victim to choose "transfer" on the options listed on the ATM monitor screen. By fraudsters, the term transfer is stated as an acronym for "*transaksi penerimaan* (acceptance transaction)" which means this menu is used so that the victim can receive a certain amount of funds from the fraudster. Victims who do not understand English, of course, will trust the fraudsters. In addition, the victim could be reassured because the "transfer" option was in the Indonesian menu, so the term "transfer" might be an abbreviation. This fraud will not occur if the ATM menu (Indonesian group) does not have a "transfer" option, but instead, it is replaced with "*kirim uang* (send money)", for instance.

3) OTP

OTP stands for One Time Password. In Bahasa Indonesia the term means "*sandi sekali pakai*" (Naik & Singh, 2021). The OTP is sent by the service provider (electronically) as a tool to ensure that the recipient of the OTP is the same person as the account owner of the service provider. Usually OTP is sent via SMS (Short Message Service). By fraudsters, OTP is said to be an abbreviation of *Otorisasi Tanda Penerimaan* (accept authorization). The OTP needs to be reported to the fraudster so that the OTP recipient (the account owner) will receive some money from the fraudster. The OTP was sent by the service provider because someone was trying to log into the victim's account. Thus, when the victim gives the OTP to the fraudster, his or her account will be able to be hacked by the fraudster

In the SMS message containing the OTP, the phrase "don't give this OTP to anyone" had been included. When this phrase was questioned by the victim, the fraudster argued by saying that the phrase was only for people around the victim. The phrase could be given to the fraudster because the fraudster is an official employee of the OTP sending agency. In the message, there was also the phrase "Beware of scams". Similar to the previous phrase, when the victim questions it, the fraudster also explained

it in detail to the victim. With this explanation, the victim usually became increasingly convinced that the fraudster was an official employee of the OTP sending agency. The SMS message should include a phrase that follows the term "OTP", i.e. "code to log in to the account".

4) Briva

Briva is an acronym for BRI Virtual Account. With Briva, a BRI account owner can make payments to certain accounts through a one-time identity number. This identification number is unique for each transaction (BRI, 2018). Usually, the identity number consists of several digits plus the mobile number of the BRI account owner.

The fraudsters take advantage of the weaknesses of victims who do not know what Briva really means. The fraudster stated that Briva was a facility used to send funds to the victim using the victim's mobile number. In fact, if the victim complies with the fraudster's request, the reality is that the victim sends an amount of money that the fraudster can use to pay for the purchase of certain goods.

Apart from that, in three cases involving e-cash, transfer, and Briva, the victim would be asked to enter an account number and nominal money. By fraudsters, the nominal money is mentioned as an activation code. Usually, the victim was asked to type in the number zero followed by a number stating the amount of money disguised as a code. Of course, the zero would be lost because the type of lever in the ATM is numeric. The loss of zeros was called by the fraudster that the code is legit.

b. Identity Data Theft

Fraudsters steal the victim's (private) data in two ways, namely through a form sent from a fake URL that is made similar to the URL of an official institution. The second way is to ask for the serial number (16 digits) of the ATM card listed on each ATM card. The two information items should only be known by the customer and the bank where the account was opened. Unfortunately, most account owners become victims because they do not understand bank rules or they are not aware about bank secrecy.

1) Fake URL

The victims are usually asked by fraudsters to fill out an electronic form which is said to be a form sent by an official institution, such as a bank. The data that must be filled in includes name, account number (account), PIN (Personal Identification Number), or password. By filling in the data, the fraudster will hack the victim's account or account and withdraw all the funds contained in the account.

Victims are often deceived because URL addresses (Uniform Resource Locators) are made similar or contain the name of the institution (bank). The victim complied with the fraudster's request because he or she believed that the form came from an official institution. The victim complied with the fraudster's request because he or she did not know the official URL of the institution (bank).

2) ATM Serial Number

On each ATM card, a 16-digit number is stamped. These numbers can be used by fraudsters to hack victims' accounts. To the victim, the fraudster asks for this number to be notified to the fraudster. Victims are often unaware or unaware of the use of these 16 numbers and give them to fraudsters who usually claim to be employees of the bank where the ATM was issued. Indeed, the 16 digits listed on the ATM card are identification for each customer who holds the card (Subroto, 2022). The first two digits are the switching code of the network used, Visa or MasterCard. The next five digits are the identity of the bank that issued the card. The remaining nine digits are the identity of the ATM cardholder or account owner (Firdhayanti, 2022).

One of the uses of the 16-digit number is when the cardholder applies for account blocking remotely (online). The bank officer will ask for the 16-digit number on the ATM card to ensure that the blocking is submitted by a legitimate person as the account owner. It should be noted that this event only occurs when the customer contacts the bank officer. The four banking terms and the two instruments that are used as "tools" for online fraudsters can be

changed into terms that are more understandable to the general public. For example, the term transfer is changed to "*kirim uang* (send money)". Likewise, the OTP is changed to *Password Sekali Pakai* in Bahasa Indonesia (One Time Password in English) or *Kode untuk Login* (login code).

For the terms, Briva and e-cash, the service provider bank needs to carry out more intensive socialization so that the public understands the two terms. Socialization also includes the risks that may occur if the community uses the service incorrectly. The socialization is not only for certain bank customers but for the whole community. Therefore, a common awareness is needed which can only occur if the bank conducts comprehensive socialization to all account holders and the potential public. If the same mistakes are repeated over and over again by the account holders, then in the end the community will reduce their relationship with banking and this kind of situation will be detrimental to the banking sector itself. In this kind of situation, prevention programs need to be continuously carried out by banks with various methods and approaches to protect the public, particularly bank account owners from fraudsters.

2. Police

In cases related to the police, fraudsters use the victim's lack of knowledge about the SOP (Standard Operating Procedure) of the police in handling cases, especially cases of motor vehicle raids, traffic accidents, and narcotics. The fraudster, who claimed to be a police officer, did not mention his or her unit or the location of the crime scene. The fraudster then persuades the victim to choose the "peaceful" route or bribery as a way to resolve cases related to the victim.

In this case of fraud, the fraudster usually poses as a police officer or a relative or friend of the victim. Victims are usually asked for help in the form of money sent through an online account. At the same time, fraudsters also claim that the police have never been willing to mention the place of the crime or the institution where the "policeman" works.

Such fraud cases occur because the public does not know for sure about handling cases of accidents, raids, and narcotics. In the minds of the people, these cases can be solved by bribing police officers. The standard operating procedures (SOP) can be socialized by the police (the library can assist), including socializing that bribery is an act that violates the law and can be subject to criminal sanctions.

3. Market Place

a. Cash-back

Cash-back is a return of an amount of money taken from the total money for the purchase of an item(Idris, 2021). Cash-back is used as a means of promotion from an agency selling goods or services, including a marketplace. Fraudsters use cash-back as a lure for the victim so that the victim sends a certain amount of funds or discloses data related to the victim's account on the marketplace. The data provided by the victim can be used by the fraudster to hack the victim's account and withdraws funds or makes purchases on behalf of the victim

b. Prizes

Almost similar to cashback, fraudsters lure victims with gifts given by the marketplace for celebrating something. To get the prize, the fraudster asks the victim to provide data related to the victim's account on the marketplace. In fact, the marketplace always displays announcements about prizes on the marketplace website and on the official social media accounts belonging to the marketplace.

c. Off-App Communication

In this case, the fraudster usually has an online shop in the marketplace. When the victim purchases goods sold by the fraudster, the fraudster invites the victim to communicate through other media, generally Whatsapp. When the victim complies with the fraudster's will, that is the time for the fraudster to ask the victim to send the payment to the fraudster's account. The victim was tricked into saying and sending false evidence that the victim's order had been delivered and was on its way.

4. Fake Social Media Account

In this case, the fraudster gives an announcement that the victim gets a reward on a fake account, for example, a fake Twitter account. The account was created as if it were an account of an official institution. Not infrequently, fake accounts are used as evidence by fraudsters that the victim is communicating with an official institution. The victim does not know the difference between an official account and an unofficial account. Official social media accounts belonging to an institution have a check mark behind the account name. However, this sign is not known by many people. Perhaps it should be considered to add a narrative that accompanies the check mark. In order not to be falsified, the narrative is made in image format, not text.

Apart from all of the cases above, libraries (especially public libraries) also have the opportunity to help increase public understanding of banking terms, for example, by providing "fast food" information services or an information desk. Public libraries, through mobile library services, can also make leaflets that contain the definition and ins and outs of online banking transactions. The leaflets are distributed to the public so that they can improve the digital literacy of the community. Besides, private libraries can also participate, because they are not only making efforts to increase interest in reading but also providing sources of information that can increase the digital literacy of their visitors (Nuraini, 2022). Likewise, school libraries can also expand the scope of their duties, not only increasing the role of school libraries in terms of supporting the teaching and learning process but also seeking to increase students' digital literacy '(Nurhayati, Riyanto, & Rifan, 2022).

E. CONCLUSION

Information items that often used by online fraudsters are information related to banking services, police, marketplace, and fake social media accounts. Online fraud is carried out by taking advantage of the victim's lack of knowledge about certain information. However, the victim's lack of knowledge is not only caused by the victim alone, but also by the service provider institutions. In this kind of position, the victims as account owners who have suffered losses need to get serious attention from the bank service owners. Such an incident should not be the sole fault of the account holders because they may not understand when getting banking services because of several reasons, such as an unfavorable situation when they first had a bank account. Thus, the results of this study indicate that continuous socialization from institutions related to these information items is needed to increase the literacy of the digital community which causes financial losses. In a short time, the use of terms that are easier to comprehend by the public needs to be a concern for financial service providers. With such terms, the public will be difficult to be deceived. For a long time, efforts to increase people's digital literacy are still needed. Libraries, especially public libraries, can act as one of the institutions that carry out socialization. Libraries may make socialization their role in improving people's digital literacy. Socialization may be integrated into existing library service programs, such as the mobile library program. Lastly, it is recommended to continue this research as a way to find out further how low the victims' ignorance about the information items is as well. Through further research, it can be revealed which community groups are most vulnerable to being deceived. By understanding this, it is easier to design socialization programs.

REFERENCES

Advernesia. (2020, October 1). *Pengertian data kuantitatif dan kualitatif serta contohnya*. https://www.advernesia.com/blog/data-science/pengertian-data-kuantitatif-dan-kualitatif-serta-contohnya/

Agustini, P. (2021, January 17). *Empat pilar literasi untuk dukung transformasi digital*. https://aptika.kominfo.go.id/2021/01/empat-pilar-literasi-untuk-dukung-transformasi-digital/

ALA. (2022, March 1). *Digital literacy*. https://americanlibrariesmagazine.org/tag/digital-literacy/

Alan, B. (2011). *Business research methods*. Oxford University Press.

Asari, A., Kurniawan, T., Ansor, S. & Putra, A. B. (2019). Kompetensi literasi digital bagi guru dan pelajar di lingkungan sekolah Kabupaten Malang. *Bibliotika: Jurnal Kajian Perpustakaan dan Informasi*, 3(2), 98-104.

BRI. (2018, January 1). *Briva*. https://developers.bri.co.id/id/product/briva

Creswell, J. W. (2012). *Planning, conducting, and evaluating quantitative and qualitative research*.-- (4th ed.). Pearson.

Digidata. (2022, March 21). *Kejahatan online mencapai 115.756 kasus, jangan sampai menjadi korbannya!* https://www.digidata.ai/2022/03/21/kejahatan-online-mencapai-115-756-kasus-jangan-sampai-menjadi-korbannya/

Erik. (2022, September 27). Warga Madiun jadi korban penipuan: uang tabungannya ratusan juta hilang. *Tribunnews*, p. 1.

Fauzi & Marhamah. (2021). Pengaruh literasi digital terhadap pencegahan informasi hoaks pada remaja di SMA Negeri 7 Kota Lhokseumawe. *Pekomnas, 6*(2), 77-84 https://doi.org/10.30818/jpkm.2021.%25x

Firdhayanti. (2022, June 14). *Ternyata ini makna 16 nomor di kartu ATM, perlu dijaga kerahasiaannya*. https://www.parapuan.co/read/533327003/ternyata-ini-makna-16-nomor-di-kartu-atm-perlu-dijaga-kerahasiaannya

George, T. M., Okwu, E. & Ogunbodede, K. F. (2022). Digital literacy and job performance of librarians in Rivers State University Libraries, Nigeria. *Library Philosophy and Practice; Lincoln ,* Summer 4-7-2022, 1-19.

Hayati, R. (2022, June 2). *3 jenis teknik validasi data dan contohnya*. https://penelitianilmiah.com/jenis-validasi-data/

Hayden, L. (2020). Building digital literacy through digital university. *U.S. Department of Defense Information / FIND,* 31-46.

Idris, M. (2021, May 20). *Mengenal apa itu cashback dan bedanya dengan diskon*. https://money.kompas.com/read/2021/05/20/102137326/mengenal-apa-itu-cashback-dan-bedanya-dengan-diskon?page=all

Ilham, Apriliyanti, M., Setiawan, H. C. & Yazid, M. (2022). Digital literacy and increased utilization of higher education e-learning in Indonesia : A literature review. *Library Philosophy and Practice; Lincoln*. Summer 4-15-2022, 1-14.

Indeed Editorial Team. (2022, October 28). *Top 11 skills employers look for in job candidates*. https://www.indeed.com/career-advice/resumes-cover-letters/skills-employers-look-for

Indonesia. CNN. (2022, October 8). *Kenapa warga +62 gampang kena tipu dan hoaks?* https://www.cnnindonesia.com/teknologi/20221004150217-197-856229/kenapa-warga-62-gampang-kena-tipu-dan-hoaks

Indonesia Baik. (2021, January 3). *Indonesia makin melek literasi digital.* https://indonesiabaik.id/videografis/indonesia-makin-melek-literasi-digital

Indonesia. Kementerian Komunikasi dan Informasi. (2022, January 20). *Budaya digital membaik, indeks literasi digital Indonesia meningkat*. https://www.kominfo.go.id/content/detail/39488/siaran-pers-no-15hmkominfo012022-tentang-budaya-digital-membaik-indeks-literasi-digital-indonesia-meningkat/0/siaran_pers

Indradi, A. H. & Hendryanto, Y. D. (2022, February 9). *Analisis hukum terhadap instrumen kebijakan pemerintah dalam mewujudkan akselerasi literasi digital*. http://repository.unigal.ac.id/handle/123456789/1177

Jansen, J., Stoyanov, S., Ferrari, A., Punie, Y., Pannekeet, K. & Sloep, P. (2013). Experts' views on digital competence: commonalities and differences. *Computers & Education*, 68(October 2013), 473-481. https://doi.org/10.1016/j.compedu.2013.06.008

Johan, R. C., Emilia, E., Syahid, A. A., Hadiapurwa, A. & Rullyana, G. (2020). Gerakan literasi masyarakat berbasis media sosial. *Berkala Ilmu Perpustakaan dan Informasi, 16*(1), 97-110. https://doi.org/10.22146/bip.v16i1.35

Kusuma, I. P. (2020). *Mengajar bahasa Inggris dengan teknologi: Teori dasar dan ide pengajaran*. Deepublish.

Laugu, N. (2019). Ideology contestation in management of university library development. *JSW (Jurnal Sosiologi Walisongo), 3*(2), 179-194. https://doi.org/10.21580/jsw.2019.3.2.4266

Lee, H., Lim, J.-A. & Hae-Kweun, N. (2022). Eiffect of a digital literacy program on older adults' digital social behavior: A quasi-experimental study. *International Journal of Environmental Research and Public Health; Basel, 19*(19), 1-10. https://doi.org/10.3390/ijerph191912404.

Martens, H. & Hobbs, R. (2015). How media literacy supports civic engagement in a digital age. *Atlantic Journal of Communication, 23*(2), 10–11. https://doi.org/10.1080/15456870.2014.961636

Naik, R. & Singh, U. (2021). Secured 6-digit OTP generation using B-exponential chaotic map. *International Journal of Advanced Computer Science and Applications; West Yorkshire, 12*(12), 786-794. https://doi.org/10.14569/IJACSA.2021.0121296

Nuraini. (2022). Peran Perpustakaan Kafe Literacy Coffee dalam meningkatkan minat baca pengunjung di kota Medan. *Berkala Ilmu Perpustakaan dan Informasi, 18*(1), 45-58 https://doi.org/10.22146/bip.v18i1.2100.

Nurhayati, A., Riyanto, R. & Rif'an, M. (2022). Memaksimalkan peran perpustakaan sebagai sumber belajar di Sekolah Menengah Atas Muhammadiyah 1 Ponorogo. *Berkala Ilmu Perpustakaan dan Informasi, 18*(1), 113-127 https://doi.org/10.22146/bip.v18i1.3650.

Ponce, E. K., Sanchez, K. E. & Andrade-Arenas, L. (2022). Implementation of a web system: Prevent fraud cases in electronic transactions. *International Journal of Advanced Computer Science and Applications West Yorkshire, 13*(6), 865-876. https://doi:10.14569/ijacsa.2022.01306102

Prambors. (2022, August 30). *Negara-negara rawan penipuan online dan offline, Indonesia nomor berapa?* https://www.pramborsfm.com/news/negara-negara-rawan-penipuan-online-dan-offline-indonesia-nomor-berapa/all

Qu, B., Li, W. & Zhang, Y. (2022). Factors affecting consumer acceptance of electronic cash in china: An empirical study. *Financial Innovation; Heidelberg, 8*(1), 1-19. https://doi.org/10.1186/s40854-021-00312-7

Rahmad, N. (2019). Kajian hukum terhadap tindak pidana penipuan secara online. *J-HES Jurnal Hukum Ekonomi Syariah 3*(2) , 103-117.

Rahmanto, T. Y. (2019). Penegakan hukum terhadap tindak pidana penipuan berbasis transaksi elektronik (legal enforcement against fraudulent acts in electronic-based transactions). *Jurnal Penelitian Hukum De Jure, 19*(1), 31-52 http://dx.doi.org/10.30641/dejure.2019.V19.31-52.

Rosenthal, G. (2018). *Social interpretive research: An introduction*. Universitätsverlag Göttingen.

RT Katalisnet. (2022, January 3). *Pengertian skill digital dan keterampilan yang dibutuhkan saat ini*. https://katalisnet.com/pengertian-skill-digital-dan-keterampilan-yang-dibutuhkan-saat-ini/

Skerrett, D. (2019). How technology, 5G, familiarity, and community shape content in our mobile world . *EContent; Wilton, 42(*4) , 35-37.

Slack Team. (2022, July 29). *What is digital culture?* https://slack.com/blog/collaboration/what-is-digital-culture

Statista. (2022, Oktober 18). *Country-level digital competitiveness rankings worldwide as of 2021*. https://www.statista.com/statistics/1042743/worldwide-digital-competitiveness-rankings-by-country/

Subroto, V. K. (2022, Mei 19). *Mengenal nomor kartu ATM dan fungsinya*. http://komputerisasi-akuntansi-d4.stekom.ac.id/informasi/baca/Mengenal-Nomor-Kartu-ATM-dan-Fungsinya/c65b79a71ffdd196d7fe6f821126e9c77d881dd7

Sugiyono. (2014). *Metode penelitian pendidikan pendekatan kuantitatif, kualitatif, dan R&D*. Alfabeta.

Supriadi, B. (2022, Oktober 13). *Curhat Angga, uang Rp105 juta di rekening raib, diduga jadi korban penipuan online*. https://surabaya.kompas.com/read/2022/10/13/060000478/curhat-angga-uang-rp-105-juta-di-rekening-raib-diduga-jadi-korban-penipuan?page=all

Zainal, A. (2017, October 3). Ingat kata-kata 'waspadalah! waspadalah!'? Bang Napi 'Sergap' RCTI meninggal dunia. *Batam.Tribunnews.Com*. https://batam.tribunnews.com/2017/10/03/ingat-kata-kata-waspadalah-waspadalah-bang-napi-sergap-rcti-meninggal-dunia.

FIGURE LIST

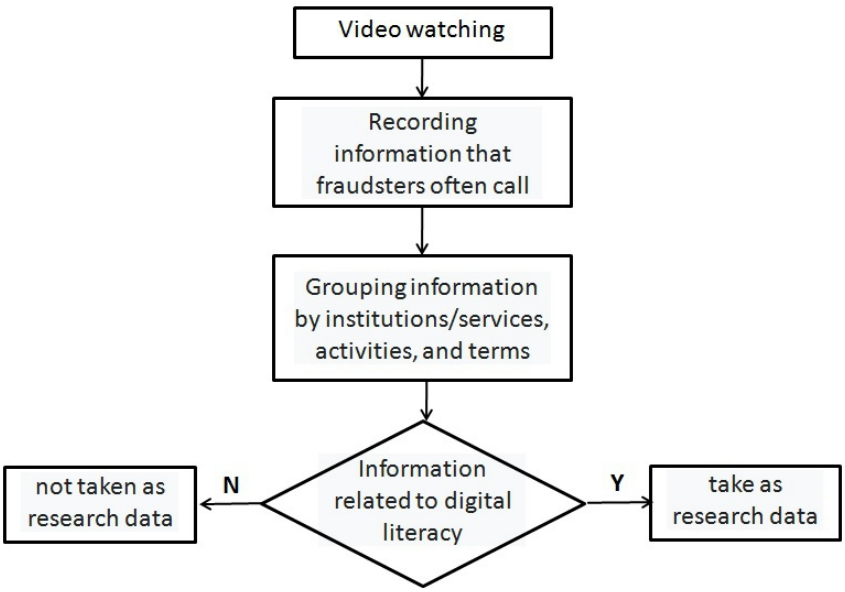

Figure 1. Data Collection Flowchart

TABLE LIST

Table 1. Information Items Classification

Institution	Item	
Banking Services	ATM Service Terms	e-Cash Transfer OTP Briva
	Identity Data Theft	Fake URL ATM Serial Number
Police	SOP	
Market Place	Cash-back Prizes Off-App Communication	
Fake Social Media Account	The symbol of official account	

Source: Result of Research Data Processing, 2019-2022