 ISBN: 978-623-92207-1-6

Criminal Law Enforcement of Phising Attacks on Online Banking Services

Aryono
Duta Bangsa University of Surakarta
Indonesia
aryono@udb.ac.id

Jaco Barkhuizen
University of Limpopo
South Africa
Jaco.barkhuizen@ul.ac.za

Abstract—The high rate of fraud crimes has a negative impact on bank customers. Where the higher the crime rate, the customers need a high level of system security, because many attackers or phisers are interested in exploiting customer data if the security level is low. In addition, legal or statutory powers are also needed in dealing with these crimes. In this study, the research method used is juridical or normative research methods. This research method uses research on existing library materials to solve problems. The approach method used in this research is to use the statutory regulatory approach. In this study using primary legal materials and secondary legal materials: 1. Primary legal materials are materials that have juridical binding power, such as statutory regulations, court decisions, and agreements. The legal materials used include the Criminal Code. 2. Secondary legal materials are materials that do not have juridical binding power, namely draft laws and regulations, literature, and journals related to the focus of research. E. Legal Material Analysis Techniques Analysis of the legal materials used in this research is qualitative data analysis including data classification activities in accordance with legal issues and provisions, then editing, presenting the results of the analysis in narrative form, and drawing conclusions. Law enforcement of phishing attacks on this online banking service is in the form of: Criminal threats for the perpetrator (phishers) are regulated in accordance with the following provisions: 1) According to Article 378 of the Criminal Code, it explains that "Whoever with the intention of benefiting himself or another person unlawfully, by using a false name or fake dignity, by deception, or a series of lies, moves another person to hand over something to him, or in order to give a debt or write off a debt, he will be punished for fraud with a maximum imprisonment of four years ". 2) In Article 28 of the Law on Electronic Information and Transactions Number 11 of 2008 which states, "every person knowingly and without rights spreads false and misleading news that results in consumer losses in electronic transactions." shall be sentenced to imprisonment for a maximum of 6 (six) years and / or a maximum fine of Rp. 1,000,000,000.00 (one billion rupiah). 3) Based on Article 35 of the Law on Electronic Information and Transactions Number 11 of 2008, which contains: Every person intentionally and without right or against the law manipulates, creates, changes, removes, destroys Electronic Information and / or Electronic Documents with the aim that Electronic information and / or Electronic Documents are considered as if the data is authentic. shall be sentenced to imprisonment of up to 12 (twelve) years and / or a fine of not more than Rp. 12,000,000,000.00 (twelve billion rupiah). " 2. The factor causing phishing attacks on online banking services is the lack of user knowledge about the data security system.

Keywords—Phising, Bank Services, Cybercrime

I. INTRODUCTION

Indonesia is one of the developing countries. One of the characteristics of development is the number of development programs in various fields of life, one of which is developments in the field of information and communication technology. The rapid development of information and communication technology is related to people's daily lives. Information and communication technology is widely used in various services in companies, one of which is banking. In this modern era, banks are increasingly developing online banking due to a relatively more efficient use in which customers facilitate unlimited transactions. However, this development raises new challenges, namely the emergence of various cyber-based crimes (cybercrime) so that many parties try to exploit system weaknesses and user awareness in information systems.

N. P. Singh in Ikhsan Radiansyah, et al (2016), explained that various kinds of cyber threats that attack users of cyberspace or internet systems, one of which is phishing. Phishing is a criminal activity using social engineering techniques. Usually phishers try to cheat to get information such as usernames, passwords and credit card details by posing as a trusted entity in an electronic communication. Various industry-based sectors that are attacked by phishing are usually e-commerce, social media, banking and so on. The occurrence of fraud cases in online banking services is often considered to be the fault of the bank. Maulen (in Firda Atsalis Maulidya Hasanah) stated that the use was also responsible for the case. Users are often considered negligent and ignore the rules set by the bank. The following is data related to phishing attacks that attack internet sites such as online banking services:

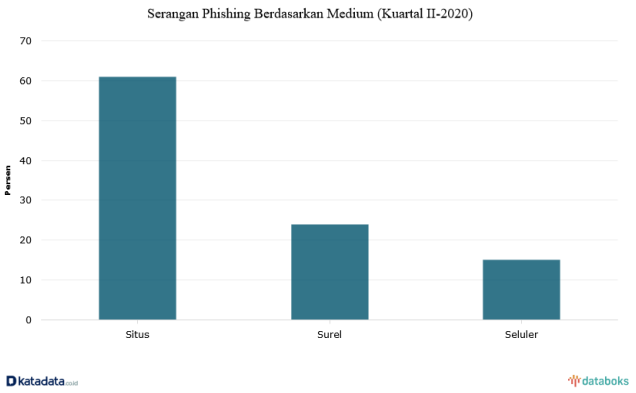

Figure 1. Data on phishing attacks via the internet Source: Databoks.co.id

From the data above, it is known that more cases of phishing attacks occurred via internet sites, it was noted that 61% of the number of phishing attacks occurred via internet sites, as much as 24% occurred via email and as much as 15% via cellular. However, it does not rule out that the case will increase if you look at the data.

ISBN: 978-623-92207-1-6

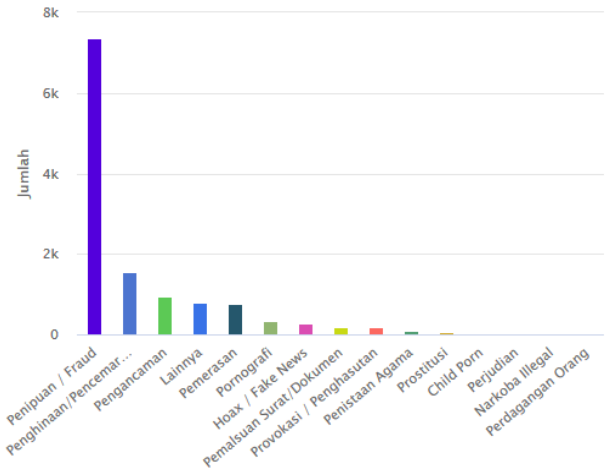

Figure 2. Data on reports of fraud / fraud in January 2020 - January 2021 Source: patrolisiber.id

The high rate of fraud crimes has a negative impact on bank customers. Where the higher the crime rate, the customers need a high level of system security, because many attackers or phisers are interested in exploiting customer data if the security level is low. In addition, legal or statutory powers are also needed in dealing with these crimes. Indonesia is a state based on law, this is stated in article 1 paragraph 3 of the 1945 Constitution. It cannot be separated from Indonesia which is a law enforcing law state which in capturing and enforcing the law must have a strong legal basis, this is based on Indonesia which adheres to the principle of legality as outlined in Article 1 paragraph 1 of the Criminal Code, namely: "an act cannot be criminalized unless it is based on the strength of the existing criminal legislation". The regulation regarding theft conducted via electron has been regulated in law number 11 of 2008 concerning Electronic Information and Transactions which also regulates cybercrime, although it is regulated in this ITE law but in its implementation this law has encountered many obstacles.

One of the obstacles in the ITE law is in the proof of the perpetrator, which requires valid evidence as stated in article 44 of the ITE law which states: "Evidence for investigation, prosecution and examination at court proceedings according to the provisions of this law are as follows: a. Evidence as referred to in statutory provisions; and b. Other evidence in the form of Electronic Information and / or Electronic Documents as referred to in Article 1 number 1 and number 4 as well as Article 5 paragraph (1), paragraph (2) and paragraph (3). In criminal procedural law, information and / or electronic documents and / or printouts thereof constitute an extension of other evidence other than those stipulated in article 184 of the Criminal Procedure Code. This is confirmed in article 44 letter b of the ITE law with another intention that efforts to present electronic information evidence in fulfilling the categorization as evidence known in article 184 of the Criminal Procedure Code. Therefore, the information and / or electronic documents of the perpetrator of theft at a bank via the internet are usually located or stored on the hard disk, so that the perpetrator can erase or replace the hard disk of his computer to remove traces that can complicate the investigation process. Even though the case is difficult to prove, the perpetrator must still be legally responsible (Agus Setiawahyudi, 2015).

The aim of this research is : 1. To determine the law enforcement of phishing attacks on online banking services 2. To determine the factors causing phishing attacks on online banking services

II. METHOD

Based on the problems in this study, the research method used is juridical or normative research methods. This research method uses research on existing library materials to solve problems. The approach method used in this research is to use the statutory regulatory approach.

In this study using primary legal materials and secondary legal materials: 1. Primary legal materials are materials that have juridical binding power, such as statutory regulations, court decisions, and agreements. The legal materials used include the Criminal Code. 2. Secondary legal materials are materials that do not have juridical binding power, namely draft laws and regulations, literature, and journals related to the focus of research. E. Legal Material Analysis Techniques Analysis of the legal materials used in this research is qualitative data analysis including data classification activities in accordance with legal issues and provisions, then editing, presenting the results of the analysis in narrative form, and drawing conclusions (Wahida Azahrah, 2018).

III. RESULT AND DISCUSSION

Criminal Law Enforcement of Phishing Attacks on Online Banking Services

Phishing (password harvesting fishing) is a fraudulent act using a fake email or fake website which aims to trick the user so that the perpetrator can get the user's data. This fraudulent act is usually in the form of an email that seems to come from an official company, for example a bank with the aim of getting someone's personal data, such as a PIN, account number, credit card number, and so on. Phishing on online banking services is a threat using social engineering techniques by tricking users (customers). Users are attracted to offers via e-mail, short messages, calls from criminals who are posing as official bank entities and inviting customers to provide sensitive data related to bank user data.

Indonesia has its first cyber law law drafted by the Ministry of Communication and Information Technology. Law number 11 of 2008 is known as the ITE Law or the Information and Electronic Transactions Law. With the enactment of this law, various types of criminal acts in cyberspace can be subject to civil and criminal sanctions. In Law Number 11 of 2008 concerning Electronic Information and Transactions, there are 10 Articles that keep the threat of criminal sanctions for violators, namely from Article 27 to Article 37.

According to Sidharta (2012), things that explain criminal sanctions include: 1. Actions of distributing, transmitting, and / or making accessible electronic information and / or electronic documents that contain: violates decency, gambling, extortion and / or threats (intended for the public). 2. Actions spread: - Fake and

 ISBN: 978-623-92207-1-6

misleading news that harms consumers in electronic transactions; - A sense of hatred or hostility towards certain individuals and / or community groups based on SARA. 3. Actions send messages of threat of violence and / or frighten certain individuals; 4. Intentional and unauthorized act of accessing another party's computer and / or electronic system; 5. Intentional and unauthorized acts of interception or interception of electronic information and / or electronic documents belonging to other people; 6. Intentional and unauthorized acts of altering, adding, reducing, damaging, eliminating, transferring, or hiding electronic information and / or electronic documents belonging to others; 7. Intentional and unauthorized actions interfere with the electronic system, so that the system cannot work properly; 8. Acts of deliberately and without rights producing, selling, procuring for use, importing, distributing, providing, or owning computer hardware or software specifically designed to facilitate the above-mentioned criminal acts; and 9. Intentional and unauthorized act of manipulating electronic information and / or electronic documents so that they are judged as authentic.

Crimes against computers and computer programs (including cybercrime in the form of phishing) are crimes that are difficult to prove, because Article 184 of the Criminal Procedure Code has been given restrictions regarding various legal evidence that can be used as a basis for judges' considerations in making decisions. Important things that need to be considered in the regulation of UU-ITE are the stipulation of electronic information, electronic documents, and printouts as valid legal evidence. Thus, there is no more controversy over whether voice recordings, videos, e-mails, or transaction receipts at ATMs are to be used as evidence in court.

With high cases of phishing attacks via internet sites, legal protection is needed for bank customers who are victims of data theft through phishing as described in Article 378 of the Criminal Code, which explains that: "Anyone with the intention of unlawfully benefiting himself or another person, using a false name or false dignity or dignity, by deception, or a series of lies, moves others to surrender something to him, or to give a debt or write off a debt. , was threatened with fraud with a maximum imprisonment of four years. " The elements contained in article 378 of the Criminal Code: 1. Whoever, 2. With the intention of / surrendering oneself against the law, 3. Move other people to / so 1) Hand over the goods according to him (to the perpetrator); 2) Giving a debt to him (to the perpetrator); or 3) Write off the receivables to him (to the perpetrator). 4. By using: 1) Using a false name or false dignity; 2) ruse, or 3) A series of lies. So based on the explanation of the elements above, in the case of phishing attacks in online banking, the perpetrator (phishers) fulfills the elements in Article 378 of the Criminal Code.

The following is an explanation of why phishers meet the elements in article 378 of the Criminal Code, 1. First element: Whoever is fulfilled, who is meant by the existence of a phishing actor (phishers). 2. Second element: With the intention of benefiting / surrendering himself against the law, what is meant by benefiting / surrendering himself against the law is the perpetrator obtains an amount of money from the customer's account by stealing data in the form of the customer's personal username and password. 3.The third element: Mobilizing other people to / to deliver goods or something to the perpetrator is fulfilled, which is meant by moving other people to / to hand over the goods or something to the perpetrator, namely the perpetrator deliberately sending an email containing notification to the customer to immediately update it. his personal account through a fake website that is made to resemble the original website of the bank. 4. Fourth element: By using a false name or fake dignity, with trickery, or a series of lies fulfilled, what this means is that the perpetrator creates the original website of the bank in order to convince customers that the notification to immediately update their personal account is true. from the bank.

Based on Article 28 No. 11/2008 concerning the ITE Law, which explains that, "everyone knowingly and without right spreads false and misleading news without the right to spread false and misleading news which results in consumer losses in electronic transactions." Shall be punished with imprisonment of 5 (six) years and / or a maximum fine of Rp. 1,000,000,000.00 (one billion rupiah). Meanwhile, according to Article 35 no. 11/2008 concerning the ITE Law, explains that, "every person intentionally and without rights or against the law manipulates, creates, changes, removes, destroys Electronic Information and / or Electronic documents with the aim that Electronic Information and / or Electronic Documents are considered as if the data were authentic. " Shall be sentenced to imprisonment of up to 12 (twelve) years and / or a maximum fine of Rp. 12,000,000,000.00 (twelve billion rupiah). The rules for compensation for victims of criminal acts can be carried out in 3 ways, namely: 1. Through a combination of compensation cases (regulated in Article 98 paragraph (1) and paragraph (2) of the Criminal Procedure Code), 2. Through a lawsuit against the law and 3. Through a request for restitution.

Factors that cause phishing attacks on online banking services

The following data on the causes of phishing according to the authors in No Author's Name and Year of the Factors Cause of Phishing 1 (Dhamija, et al., 2006) User knowledge is minimal and psychological 2 (Alsharnouby, et al., 2015) Minimal user knowledge 3 (Arachchilage & Love, 2014) Minimal user knowledge 4 (Mohammad, et al., 2015) Minimal user knowledge 5 (Parmar, 2012) Minimal user knowledge, psychological and privacy of social networking services 6 (Meulen, 2013) Psychological 7 (Sein, 2011) Minimal user knowledge 8 (Vishwanath, et al., 2011) Psychological 9 (Button, et al., 2014) Psychological 10 (Zielinska, et al., 2015) Minimal user knowledge 11 (USE Act, 2010) Minimal user knowledge 12 (Hilley, 2006) Minimal user knowledge 13 (Elsevier Advanced Technology, 2015) Minimal psychological and user knowledge 14 (Malik & Malik, 2011) Privacy social networking services Based on the data above, it can be concluded that the factor causing phishing attacks is due to the lack of user knowledge of the importance of maintaining data security.

users are considered not to have good knowledge of computer systems, especially distinguishing legitimate and fake domains. This is supported by the statement of Mohammad, Thabtah, & McCluskey (2015) in (Atsalis et al.,

2014), the factor why users become victims of phishing attacks is that the majority of users have minimal knowledge of the threat of online crime, do not have good knowledge of threats. phishing, does not have a good strategy in recognizing phishing attacks, focuses on content rather than indicators on the website, and does not know the online service procedures used so they get stuck when they get e-mails from online services they use regarding maintenance information and other information phishers are used to get sensitive user data.

IV. CONCLUSION

Based on the description above, it can be concluded that: 1. Law enforcement of phishing attacks on this online banking service is in the form of: Criminal threats for the perpetrator (phishers) are regulated in accordance with the following provisions: 1) According to Article 378 of the Criminal Code, it explains that "Whoever with the intention of benefiting himself or another person unlawfully, by using a false name or fake dignity, by deception, or a series of lies, moves another person to hand over something to him, or in order to give a debt or write off a debt, he will be punished for fraud with a maximum imprisonment of four years ". 2) In Article 28 of the Law on Electronic Information and Transactions Number 11 of 2008 which states, "every person knowingly and without rights spreads false and misleading news that results in consumer losses in electronic transactions." shall be sentenced to imprisonment for a maximum of 6 (six) years and / or a maximum fine of Rp. 1,000,000,000.00 (one billion rupiah). 3) Based on Article 35 of the Law on Electronic Information and Transactions Number 11 of 2008, which contains: Every person intentionally and without right or against the law manipulates, creates, changes, removes, destroys Electronic Information and / or Electronic Documents with the aim that Electronic information and / or Electronic Documents are considered as if the data is authentic. shall be sentenced to imprisonment of up to 12 (twelve) years and / or a fine of not more than Rp. 12,000,000,000.00 (twelve billion rupiah). " 2. The factor causing phishing attacks on online banking services is the lack of user knowledge about the data security system. B. Suggestions 1. Law enforcement or legal protection given to victims, in the form of sanctions or penalties for the perpetrators of data theft (phishing) based on Article 378 of the Criminal Code, Article 28 of the ITE Law, and Article 25 of the ITE Law, must be emphasized more and firmly in the application of the articles. this article, considering the many similar cases experienced by banking institutions. 2. Clearer regulations and tighter legal protection is needed, especially for cybercrime cases in the banking sector.

REFERENCES

[1] Anderson, K. B. (2006). Who are the victims of identity theft? The effect of demographics. Journal of Public Policy & Marketing, 25(2), 160–171.

[2] Anderson, R. (2007). Closing the phishing hole - Fraud, risk and nonbanks. Proceedings of the Payments System Research Conferences, 1–16.

[3] APWG [Anti-Phishing Working Group] (2015). Phishing activity trends report: 4th quarter 2014. Retrieved from http://docs.apwg.org/reports/apwg_trends_report_q4_2014.pdf.

[4] Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. International Journal of Cyber Criminology, 3(1), 400–420.

[5] Brown, J. S., Collins, A. & Duguid, P. (1989). Situated cognition and the culture of learning. Educational Researcher, 18(1), 32–42.

[6] Choi, K.-S. (2008). Computer crime victimization and integrated theory: An empirical assessment. International Journal of Cyber Criminology, 2(1), 308–333.

[7] Cohen, L. E. & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44, 588–608.

[8] Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M. & Baskerville, R. (2013). Future directions for behavioral information security research. Computers & Security, 32, 90–101.

[9] Davinson, N. & Sillence, E. (2014). Using the health belief model to explore users' perceptions of "being safe and secure" in the world of technology mediated financial transactions. International Journal of Human-Computer Studies, 72(2), 154–168.

[10] Einspruch, E. L., Lynch, B., Aufderheide, T. P., Nichol, G. & Becker, L. (2007). Retention of CPR skills learned in a traditional AHA Heartsaver course versus 30-min video self-training: A controlled randomized study. Resuscitation, 74(3), 476–486.

[11] Harrell, E. & Langton, L. (2013). Victims of identity theft, 2012. Washington DC: Bureau of Justice Statistics. Hong, J. (2012). The state of phishing attacks. Communications of the ACM, 55(1), 74–81.

[12] Hutchings, A. & Hayes, H. (2009). Routine activity theory and phishing victimisation: Who gets caught in the net? Current Issues in Criminal Justice, 20, 433–451.

[13] Jansen, J. (2015). Studying safe online banking behaviour: A protection motivation theory approach. Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance, 120–130.

[14] Jansen, J. & Leukfeldt, R. (2015). How people help fraudsters steal their money: An analysis of 600 online banking fraud cases. Proceedings of the 5th Workshop on SocioTechnical Aspects in Security and Trust, 25–31.

[15] Jansson, K. & von Solms, R. (2013). Phishing for phishing awareness. Behaviour & Information Technology, 32(6), 584–593.

[16] Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F. & Hong, J. (2010). Teaching Johnny not to fall for phish. ACM Transactions on Internet Technology, 10(2), 7:1–7:31.

[17] Lastdrager, E. E. (2014). Achieving a consensual definition of phishing based on a systematic review of the literature. Crime Science, 3(1), 1–10. Leukfeldt, E. R. (2014). Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. Cyberpsychology, Behavior, and Social Networking, 17(8), 551–555.