Received: 01 February 2024; Revised: 05 February 2024; Accepted: 07 February 2024

Internet Banking Anti-Cybercrime

Nanang Setiawan
Institut Agama Islam Al-Fatimah Bojonegoro
*Corresponding email: nanang.setiawan@iai-alfatimah.ac.id

ABSTRACT - This paper aims to explain the reality of cybercrime cases in Internet banking and provide alternative prevention to minimize the occurrence of cyber crimes in Internet banking in Indonesia. This article uses a descriptive qualitative method with a literature study approach. Cybercrime is a white-collar crime, the perpetrators are educated people who have a great curiosity about computer technology and who see the opportunity for negligence from computer users (especially access to banking) and also a weak network security system and rationalization get a large benefit with low risk. Preventive actions to avoid cyber-crime are to constantly increase knowledge of the modus of cyber-crime and how to deal with it, to be extra careful in every transaction and access to banking either through cellular or computers, be extra careful with every data, passwords, PINs and other banking codes and make changes regularly, and not easily tempted from irresponsible people.

Keywords: Internet banking, anti-cybercrime, white-collar crime, fraud, bank

ABSTRAK – Pencegahan Kejahatan Siber Perbankan. *Makalah ini ditujukan untuk menjelaskan perkembangan kasus cyber-crime dalam perbankan dan memberikan alternatif pencegahannya (fraud prevention) di Indonesia. Artikel ini menggunakan metode kualitatif deskriptif dengan pendekatan studi literatur. Cyber-crime merupakan kejahatan kerah putih (white collar crime), pelakunya adalah kaum terpelajar yang mempunyai rasa ingin tahu yang besar terhadap teknologi komputer yang melihat adanya opportunity kelalaian dari pengguna computer (terutama akses perbankan) dan juga sistem keamanan jaringan yang lemah dan dengan rasionalisasi mendapatkan benefit yang cukup besar atas tindakannya dengan resiko yang rendah. Fraud prevention yang perlu dilakukan agar terhindar dari kejahatan cyber-crime adalah senantiasa meningkatkan pengetahuan terhadap modus operandi cyber-crime dan cara menanggulanginya, ekstra berhati-hati pada setiap transaksi dan akses perbankan baik melalui media ponsel maupun komputer (laptop), terhadap setiap data, password, PIN dan kode perbankan lainnya dan melakukan perubahan secara berkala, serta tidak mudah tergiur dengan godaan dari oknum yang tidak bertanggungjawab.*

Kata Kunci: *Internet banking, pencegahan kejahatan siber, kejahatan kerah putih, penipuan, perbankan*

INTRODUCTION

The rapid development of technology today has led to many innovations related to technology, one of which is Internet technology. The Internet is a network of millions of interconnected computers (Fuady, 2005; Setiawan & Wahyudi, 2023). Because of the internet, people worldwide are now capable of communicating with one another by merely using the keyboard and mouse in front of them. Any information needed is available, and because of the convenience it offers, many individuals use it. Technology based on the Internet has been implemented in many facets of modern life, including the financial sector, in the form of online banking technology .

The use of the Internet by financial institutions to promote and carry out online transactions, both conventional and new is referred to as Internet banking. (Aini & Taman, 2020). The trend of using banking transactions is increasing; payment transactions made by the public are no longer done conventionally but have switched to online banking through mobile banking, internet banking, and online stores. Banks' adoption of online banking results in both an increase in their competitive edge and overall productivity. Customers of banks appreciate the convenience of online banking, allowing them to transact from any location and anytime.

Internet banking facilities that provide many benefits and conveniences for customers, such as reduced costs, market expansion, and increased service speed, have given rise to new types of crime, both traditional organized crime and cybersecurity violations using computer and internet media, including Internet banking technology, where the crime is known as cyber-crime. For most people who are used to using communication technology (telecommunication), cybercrime is not a term that is foreign to their ears. Cybercrime is a computer-generated crime that includes unauthorized access to data and damage to electronic devices' security, privacy, PINs, passwords, etc. with the use of technology (Singh et al., 2021).

Cybercrimes that have occurred in the banking world include illegal access to customer banking accounts, falsification of customer data stored via the Internet (cloud), and crimes using the Internet for spying. In addition, there are also crimes directed against customers' data stored on computers. The customer's data, such as PIN, account number, and others, as well as making transactions with someone else's credit card or debit card. In banking crimes, a hacker can enter a banking network system to steal customer information contained on the server regarding the bank account database, because with e-

banking, the network becomes open and can be accessed by anyone (Golose, 2006). Even if data theft is carried out often, it cannot be proven in plain sight because no data is lost, but it can be known to have been accessed illegally from the system being run. This cybercrime will have a major impact on the banking sector concerned, and the impact will affect, among others, reduced customer trust, more commonly known as reputation risk, and efforts are needed to make asset repairs and physical repairs very large.

Many studies have been conducted related to the reality of cybercrime in the banking industry. Wang et al. (2020), in his research, stated that four types of cybercrime are most significant in the banking industry, namely: 1) virus, worm, and trojan infections; 2) electronic spam e-mail; 3) hacking; and 4) cyberstalking or online harassment. Wang et al., (2020) stated that the impact of cybercrime on banking is: 1) loss of revenue; 2) damage to reputation; 3) loss of customers; and 4) regulatory sanctions.

According to Akinbowale et al. (2020), most evaluations focus on the financial perspective of the banking sector and consumer perceptions of banking services, precisely the consequences of cybercrime on customer perceptions and financial services. A rising tide of cybercrime is detrimental to the economic growth of financial institutions, either indirectly through a lack of trust in digital and internet infrastructure or directly via fraud and extortion. This can occur indirectly through a lack of trust in digital and internet infrastructure or directly through these activities. The reduction of cybercrime requires the development of a multidisciplinary strategy to destroy the infrastructure of cyber criminals effectively.

This paper is intended to explain the phenomenon and various types of cyber-crime, how the development of cyber-crime cases in banking (internet banking) occurred, analyze the causes of cyber-crime, and explain how the modus operandi is generally carried out by cyber-crime perpetrators. and provide alternative prevention to avoid or minimize the occurrence of cybercrime in Internet banking in Indonesia.

LITERATURE REVIEW

In discussing cybercrime, it is necessary to know several terms related to people (perpetrators) and actions committed in cybercrime, there are (Fuady, 2005; Sheetz, 2007):

a. Hacker
   Hacker are people who are experts and master computers, like to study the ins and outs of computer systems, experiment with them, and then carry out actions to infiltrate the communication network of an institution in cyberspace.
b. Cracker
   Cracker is the dark side of a hacker who illegally infiltrates and destroys websites and internet network security systems to gain pleasure and profit.
c. Carder
   Carders are people who crack credit cards to steal other people's card numbers and use them for personal gain.
d. Deface
   Defacing is the act of infiltrating a site and then changing the appearance of the page on the site with a specific purpose.
e. Phreaker
   Phreaker are people who crack the telephone network so they can call for free to any intended area.

Cybercrime can be categorized into two fields, there are: 1) computer-related crime, where computers are targeted by perpetrators for any illegal and criminal behavior by processing computer system data in an illegitimate way to commit computer crimes; and 2) computer-generated crime, where the computer becomes a tool or weapon used by perpetrators for illegal behavior to damage or steal some privacy and system data (Singh et al., 2021). As for cybercrime that attacks the banking industry, it falls into the category of computer-generated crime, in which computers are used as a tool by actors to steal customer banking account data and then use it to extract a certain amount of funds for personal gain, either directly withdrawing funds or using them for online shopping. Cybercrime in banking occurs in every service product provided by banks, especially related to digital customer services, which consist of SMS banking, mobile banking, and Internet banking services.

The following are several potential forms of cybercrime in banking activities, (Golose, 2006):

a. Typo Site
   The perpetrator will construct a false site name identical to the actual site's name and an address comparable to the accurate site's address. The offender watches for an opening if the victim types in the incorrect address and ends up on the bogus website he fabricated. If this occurs, the offender will gain

the username and password information of the victim, which can then be utilized to cause the victim harm.

b. Keylogger/Keystroke Logger
   It occurs frequently in locations providing public Internet access, such as Internet cafes. This program will keep a record of the characters that the user inputs in the hopes of obtaining vital information such as the user ID and password. When you access the internet in public areas more frequently, you put yourself in a position where you are more likely to become aware of the modus operandi.
c. Sniffing
   Attempts to obtain a user ID and password by observing data packets passing on a computer network.
d. Bruce Force Attacking
   Attacking Make an effort to decipher the passphrase or obtain the key by attempting every combination.
e. Web Deface
   an exploiting system designed to alter the visual presentation of a website's landing page.
f. Email Spamming
   Sending junk email in the form of product advertisements and the like to someone's email address.
g. Daniel of Service
   Intentionally overwhelming the targeted computer system with a large quantity of data to disable it.
h. Virus Worm, Trojan.

Using worms and trojan viruses to spread to bring down computer systems, stealing data from systems that have been compromised, and smearing the reputation of specific software developers.

METHODOLOGY

This article uses a descriptive qualitative method with a literature study approach. Descriptive qualitative research is research that aims to understand the phenomenon of what is experienced by research subjects using descriptions in the form of words and language to provide understanding and explanation so that readers can understand them well (Moleong, 2017). The literature study approach is intended to assist readers in understanding the entire body of research available on a topic discussed, which is obtained from various sources

of data and literature, informing them about the advantages and disadvantages of studies on that topic (Rhoades, 2011).

The steps taken in the literature study in this article are: first, determining the topic or research question; second, identifying relevant information in the form of inclusion/exclusion criteria or keywords; third, performing a literature search with identified keywords; fourth, screening all and excluding irrelevant studies; fifth, researching relevant studies; sixth, synthesizing findings; and seventh, developing conclusions and recommendations (Rhoades, 2011)..

RESULT AND DISCUSSION

Cybercrime is classified as a type of white-collar crime. The perpetrators of cybercrimes are generally educated people who are proficient in operating computers. Fuady (2005) divides cybercrime actors into four categories, there are:

a. Organizational Occupational Crime
   In this category, cybercrime perpetrators are executives who commit illegal acts and harm other parties through the Internet for corporate interests or profits.
b. Government Occupational Crime
   In this category, cyber-crime perpetrators are officials or bureaucrats who carry out illegal acts via the internet with the approval or orders of the government, although in many cases this will be denied.
c. Professional Occupational Crime
   In this category, cybercrime perpetrators are professional actors from various professions who commit crimes intentionally (malpractice).
d. Individual Occupational Crime
   In this category, cybercrime perpetrators are individuals from business circles, owners of capital, or other independent people who choose a deviant path that violates the law or harms other parties.

The modus operandi of cybercrimes that are mostly carried out by perpetrators in carrying out their operations are as follows (Arifah, 2011):

a. Unauthorized Access to Computer System and Service
   Crimes committed by entering or infiltrating a computer network system This crime is becoming increasingly widespread with the development of intranet technology. We certainly haven't forgotten that when the East

Timor issue was being hotly discussed at the international level, several websites owned by the Indonesian government were damaged by hackers.

b. Illegal Contents
It is a criminal offense to post data or material on the internet that is false, unethical, or that may be perceived to be breaching the law or upsetting public order. For instance, spreading falsehood that lowers the other party's self-respect or dignity would be considered an act of low self-esteem. Matters about pornography or the loading of material that is a state secret, agitation and propaganda against the lawful government, and so on are all topics that fall within this category.

c. Data Forgery
Crime by falsifying data on important documents stored as scrupulous documents via the internet. This crime is usually aimed at e-commerce documents by making it appear as if there was a "typo," which in the end will benefit the perpetrator because the victim will enter personal data and credit card numbers that can be misused.

d. Cyber Espionage
Offenses involve the use of the internet network to engage in espionage activities against other parties by breaking into the computer network system of the target party. Typically, competitors in business with important papers or databases housed in a computerized system connected to a computer network are the targets of this type of criminal activity.

e. Cyber Sabotage and Extortion
This activity is carried out by creating disturbances or destroying data, computer programs, or network systems connected to the internet. Usually, this crime is committed by infiltrating a logic bomb, computer virus, or certain program so that data, computer programs, or computer network systems cannot be used, do not work as they should, or do not work as desired by the perpetrator. For example, with the spread of computer viruses when the victim is browsing the internet.

f. Offence Against Intellectual Property
This crime is directed against intellectual property rights owned by other parties on the internet. For example, impersonating the appearance of a web page on a site belonging to someone else illegally, broadcasting information on the Internet that turns out to be someone else's trade secret, and so on.

g. Infringements of Privacy
This crime is usually directed against a person's personal information stored on a personal data form that is computerized, which if known by another

person can harm the victim materially or immaterially, such as credit card numbers, ATM PINs, hidden defects or illnesses, and so on.

Umamit (2017) details some of the causes of cybercrime, which are rife and lately have become increasingly troubling to society, there are:

1. Access to the internet without limits.
2. The carelessness of those who utilize computers. This is one of the primary reasons why people commit crimes using computers.
3. It is simple to accomplish and requires little in the way of safety or ultra-modern apparatus. Criminals are likely to continue committing computer crimes since it can be challenging to track them down, although it is simple to commit computer crimes.
4. The perpetrators of this crime are persons who, on the whole, have a high level of intelligence, have much natural curiosity, and are devoted to computer technology. The knowledge that computer criminals possess on the operation of a computer is significantly higher than that of computer operators.
5. Inadequate network security systems and a lack of attention from Traditional public crimes continue to receive significant focus from society and law enforcement. Criminals who use computers to perpetrate crimes still do so today.

Cybercrime is a type of crime in cyberspace that is related to criminal acts and attempts to commit fraud. In the study of fraud, there is a theory that explains the causes of fraud known as the "fraud triangle theory" (Cressey, 1950). Cressey explained that there are three main causes of fraud: intention or pressure, opportunity, and rationalization of action. Without these three factors, fraud and cybercrime will be difficult to occur.

In cases of cybercrime, it generally occurs due to the intention or pressure from the perpetrator in the form of demands for the necessities of life either from himself or from demands from other people, coupled with the opportunity to commit acts of fraud in the form of negligence by computer users (victims) and also seeing a weak security system, and also with rationalization or justification for their actions that their actions were not unlawful or with many of the same perpetrators escaping the law. Another rationalization is based on calculating the cost and benefits of the perpetrators' actions by comparing the potential income from the crime to the costs incurred or the risks that will be faced, including the risk of legal action and prison sentences. If there is still a large amount of income to be generated, then the rationalization of the perpetrators

will continue the acts of fraud, especially crimes in the form of cybercrime in banking targeting customers with fat accounts, and the potential benefits that will be obtained are enormous. This is the biggest reason why cybercrime is still rife and difficult to stop.

Many writers have presented a variety of solutions to the challenge of ensuring the safety of online banking; however, some of these solutions are exclusively concerned with client authentication, whereas others are only concerned with the safety of data transfer routes. Tom et al. (2020) presented a protocol for reversible biometric-based authentication that assures secure mutual authentication, customer privacy, and secure end-to-end transmission of customer transaction data. This protocol was developed by Tom et al. This protocol was developed utilizing numerous cryptographic methods, including a combination of the Advanced Encryption Standard (AES) algorithm and the Data Encryption Standard (DES) algorithm.

Furthermore, Arifah (2011) proposes several prevention efforts for each individual that can be done to reduce the occurrence of cybercrime, there are:

a. Educate User, which is providing new knowledge about cybercrime and the world of the internet.
b. Use Hacker’s Perspective, which is using thinking from the hacker's side to protect the system
c. Patch System, which closes the holes in the weakness of the system
d. Policy, determining the policies and rules that protect the system from unauthorized people.
e. Firewall, which is a system specifically designed to prevent suspicious access to private networks
f. Antivirus, which is a computer program used to prevent, detect, and remove malware.

Wahyuningsih (2020) added that to avoid and minimize the occurrence of cyber-crime in banking, especially in Internet banking transactions, several things can be done, there are:

a. Enter the bank address URL correctly; make sure there is a padlock sign
b. Do not share your PIN, password, or OTP code with anyone
c. Be diligent in updating and changing your password or PIN regularly
d. Ensure that you always log out after completing banking transactions on your cellphone or laptop.

e. Be diligent in cleaning the internet history on your cellphone or laptop.
f. Avoid carelessly downloading software or applications
g. Avoid transactions by using public Wi-Fi, a free VPN, and people's cell phones.
h. It is not easy to be tempted by the temptation (lure) of irresponsible people.
i. Always routinely check balances and account mutations.

In the context of cybercrime prevention policies within a country, Arifah (2011) describes several steps that must be taken by policymakers (in this case, the government) in dealing with cybercrime, there are:

a. Bringing the national criminal law and its procedural law up to date so that they are in line with international treaties that are associated with criminal activity
b. Enhancing the level of protection provided by the national computer network by international standards
c. Increasing the understanding and expertise of law enforcement officers about efforts to investigate and prosecute instances related to cybercrime, as well as prevent and investigate cybercrime.
d. Raising public awareness about the issue of cybercrime and the significance of preventing this type of crime from occurring in the first place.

Increasing cooperation between countries in efforts to deal with cybercrime, both bilaterally, regionally, and multilaterally, including through extradition treaties and mutual assistance treaties

CONCLUSIONS

Cybercrime is a white-collar crime; the perpetrators are educated people who have a great curiosity about computer technology, who see an opportunity for negligence from computer users (especially banking access) and also a weak network security system, and with rationalization, get a sizable benefit for their actions with low risk. Things that need to be done to avoid cybercrime crimes are: always increasing knowledge of the modus operandi of cybercrime and how to deal with it; being extra careful in every transaction and access to banking either through cellphones or computers (laptops); being extra careful of every data, password, PIN, and other banking codes; making changes periodically, and not being easily tempted by temptation (lure) from irresponsible persons.

Subsequent research was carried out on non-banking financial institutions to obtain sufficient information on the modus operandi and solutions for dealing with it. Thank you to all those who have assisted in this research, either directly or indirectly. Hopefully, this research will be useful in the development of digital forensic science, especially in cybercrime prevention.

REFERENCES

Aini, P. N., & Taman, A. (2020). *Jurnal Pendidikan Akuntansi Indonesia, Vol. 18, No. 1, Tahun 2020*. *18*(1), 48–65.

Arifah, D. A. (2011). Kasus Cybercrime di Indonesia Indonesia's Cybercrime Case. *Jurnal Bisnis Dan Ekonomi (JBE)*, *18*(2), 185–195.

Cressey, D. R. (1950). The Criminal Violation of Financial Trust. *American Sociological Review*, *15*(6), 738–743.

Fuady, M. E. (2005). "Cybercrime" Fenomena Kejahatan melalui Internet di Indonesia. *Mediator*, *6*(2), 255–264.

Golose, P. R. (2006). Perkembangan CyberCrime dan Upaya Penanganannya di Indonesia oleh Polri. *Buletin Hukum Perbankan Dan Kebanksentralan*, *4*(2).

Moleong, L. J. (2017). *Metodologi Penelitian Kualitatif* (Revisi). Remaja Rosdakarya.

Rhoades, E. A. (2011). Commentary: Literature reviews. *Volta Review*, *111*(1), 61–71. https://doi.org/10.17955/tvr.111.1.677

Setiawan, N., & Wahyudi, I. (2023). Pencegahan fraud pada kejahatan siber perbankan. *Kabilah: Journal of Social Community*, *8*(14), 508–518.

Sheetz, M. (2007). Computer Forensics, An Essential Guide for Accountants, Lawyers, and Managers. In *John Wiley & Sons, Inc*. John Wiley & Sons, Inc. https://doi.org/10.1002/9781119202011

Singh, A., Singh, S. K., Nayak, S. K., & Singh, N. (2021). *Cyber-Crime and Digital Forensic : Challenges Resolution*. *January*.

Tom, J., Alese, B. K., & Thompson, A. (2020). A Cancelable Biometric Based Security Protocol for Online Banking System Cloud Computing Security View project Computer Security View project. *Article in International Journal of Computer Science and Information Security*, *June*. https://sites.google.com/site/ijcsis/

Umamit, Z. (2017). *Cyber Crime*. Kompasiana.Com. https://www.kompasiana.com/zulkifliumamit/593803914f4edb085912ce

a2/cyber-crime?page=all

Wahyuningsih, R. (2020). *Waspadai Modus Cyber Crime, Ini Cara Aman Transaksi Internet Banking*. Cermati.Com. https://www.cermati.com/artikel/waspadai-modus-cyber-crime-ini-cara-aman-transaksi-internet-banking

Wang, V., Nnaji, H., & Jung, J. (2020). Internet banking in Nigeria: Cyber security breaches, practices and capability. *International Journal of Law, Crime and Justice*, *62*(June), 100415. https://doi.org/10.1016/j.ijlcj.2020.100415