JURNAL AL-HAKIM :
Jurnal Ilmiah Mahasiswa, Studi Syariah, Hukum dan Filantropi
Volume 5 No. 2, November 2023
ISSN 2685-2225 (P) ISSN 2722-4317 (E)

Personal Data Vulnerability in the Digital Era: Study of Modus Operandi and Mechanisms to Prevent Phishing Crimes

Ahmad Jamaludin
Universitas Islam Nusantara
Surel: jamaludinumam@gmail.com

Flea Akbar Permana
Universitas Islam Nusantara
Surel: fleaap@gmail.com

Abstract

The rapid digital transformation has significantly increased the vulnerability of personal data, leading to a worrisome rise in phishing crimes. This scientific article investigates the modus operandi and preventive mechanisms of phishing crimes in the digital transformation era. Phishing, a fraudulent practice aimed at obtaining sensitive information through deceitfully, has become a common cybercrime targeting individuals and organizations. This research utilizes a comprehensive literature review and analysis of various phishing attack scenarios to identify common strategies employed by cybercriminals. The analysis focuses on techniques used to manipulate unsuspecting victims, such as social engineering, email spoofing, and website forgery. Additionally, this study explores the exploitative nature of data breaches and their implications for personal privacy. The article highlights the importance of collaboration among stakeholders, including government agencies, technology providers, and individuals, in addressing the issue of personal data vulnerability. By sharing information, resources, and best practices, stakeholders can work together to enhance cybersecurity measures and effectively protect personal data. This research provides valuable insights into the modus operandi of phishing crimes and the preventive mechanisms necessary to safeguard personal data. By understanding the strategies employed by cyber criminals and implementing proactive measures, individuals and organizations can strengthen their defenses against phishing attacks.

Keywords: Cyber Crime; Personal Data Protection; Phishing Crime.

Abstrak

Transformasi digital yang pesat telah secara signifikan meningkatkan kerentanan data pribadi, yang menyebabkan peningkatan yang mengkhawatirkan dalam kejahatan phising. Artikel ilmiah ini bertujuan untuk menyelidiki modus operandi dan mekanisme pencegahan kejahatan phising di era transformasi digital *Phising*, praktik penipuan yang bertujuan untuk mendapatkan informasi sensitif melalui cara yang curang, telah menjadi kejahatan siber yang umum, menargetkan individu dan organisasi. Penelitian ini menggunakan tinjauan literatur komprehensif dan analisis dari berbagai skenario serangan phising untuk mengidentifikasi strategi umum yang digunakan oleh para penjahat siber. Analisis ini berfokus pada teknik yang digunakan untuk memanipulasi korban yang tidak curiga, seperti rekayasa sosial, pemalsuan email, dan pemalsuan situs web. Selain itu, penelitian ini mengeksplorasi sifat eksploitatif dari pelanggaran data dan implikasinya terhadap privasi pribadi. Artikel ini menyoroti pentingnya kolaborasi antara pemangku kepentingan, termasuk lembaga pemerintah, penyedia teknologi, dan individu, dalam mengatasi masalah kerentanan data pribadi. Dengan berbagi informasi, sumber daya, dan praktik terbaik, pemangku kepentingan dapat bekerja sama untuk meningkatkan langkah-langkah keamanan siber dan melindungi data pribadi dengan efektif. Temuan dari penelitian ini memberikan wawasan berharga tentang modus operandi kejahatan phising dan mekanisme pencegahan yang diperlukan untuk melindungi data pribadi. Dengan memahami strategi yang digunakan oleh para penjahat siber dan menerapkan langkah-langkah proaktif.

Kata Kunci: Kejahatan Siber; Perlindungan Data Pribadi; Kejahatan Phising.

INTRODUCTION

The advancement of technology has implications in various sectors of human life, offering convenience and introducing new patterns of interaction that were previously unprecedented. The recent technological progress is considered to bring significant benefits to life by providing ease in daily activities.[1] In Indonesia alone, the number of internet users reached 210 million people as of early 2022. This number continues to grow over time, and the usage becomes more diverse.

Digital transformation is one technological advancement that involves changing how work is done through information technology, making it more efficient and effective. Various industries have transformed e-learning, businesses, banking, government, and many more. The core of this transformation is the improvement of work efficiency and effectiveness through the use of databases. The main objective is to eliminate the need for documents, with databases replacing all transactional evidence in documents, making it easier, more flexible, and accessible anytime.[2]

However, the presence of digital transformation also demands significant changes to

[1] Sayid Muhammad Rifqi Noval, "Evolusi Hak Pekerja Di Era Digital: Prawacana Right To Disconnect Di Indonesia," *Jurnal Bina Mulia Hukum* 6, no. 2 (March 31, 2022): 234–53, https://doi.org/10.23920/jbmh.v6i2.637.

[2] Bagus Dwi Krismono and Nasikh Nasikh, "Inovasi Teknologi Digital Untuk Pengentasan Kemiskinan Pada Pertanian Dataran Tinggi Saat Pandemi Covid-19," *Equilibrium : Jurnal Ilmiah Ekonomi, Manajemen dan Akuntansi* 11, no. 1 (April 21, 2022): 9, https://doi.org/10.35906/equili.v11i1.962.

address the accompanying negative impacts, such as cybercrime or internet-related crimes. Cybercrime refers to legal violations committed using the internet, resulting from technological advancements in computers and telecommunications, either for personal gain or to harm others. As a consequence of technological advancements, the internet enables criminals operating in the virtual world to commit crimes in a more hidden, organized, and extensive manner, operating across vast periods. [3]

Criminal activities on the internet occur in the virtual world and can threaten an individual's privacy. Cybercrimes have been increasing in both quantity and diversity of perpetrators. With the advancements in information technology, perpetrators can easily engage in criminal activities. One such crime is phishing, which is a form of cybercrime that involves falsifying data on fraudulent websites with the intention of obtaining someone else's identity information, which will be used illegally without the knowledge of the original website owner.[4]

Cybercrime can have two definitions, namely a narrow definition and a broad definition. The narrow definition refers to illegal actions that target or utilize computers to commit crimes, both in terms of system security and data. On the other hand, the broad definition encompasses all crimes targeting computers, computer networks, users, and traditional crimes involving computer equipment use or assistance.[5] Phishing is becoming increasingly prevalent and occurs globally. According to the monthly report by the Anti-Phishing Working Group (APWG), 42% of all reported fraud incidents involve phishing. The report notes that 12.845 new and unique phishing emails and 2.560 fraudulent websites were used for phishing.[6] The report's findings indicate that the number of phishing reports submitted to the APWG during the first quarter of 2018 was approximately 263.538 cases, representing

[3] Andrew Christian Banjarnahor and Puti Priyana, "Analisis Yuridis Cybercrime Terhadap Penanganan Kasus Phising Kredivo," *Hermeneutika : Jurnal Ilmu Hukum* 6, no. 1 (February 28, 2022), https://doi.org/10.33603/hermeneutika.v6i1.6754.

[4] mia Haryati Wibowo And Nur Fatimah, "Ancaman Phishing Terhadap Pengguna Sosial Media Dalam Dunia Cyber Crime" 1 (n.d.).

[5] Widodo, *Aspek Hukum Pidana Kejahatan Mayantara*, Yogyakarta: Aswaja Presindo, 2013, hlm. 7.

[6] Suhardi Rustam, "ANALISA CLUSTERING PHISING DENGAN K-MEANS DALAM MENINGKATKAN KEAMANAN KOMPUTER," *ILKOM Jurnal Ilmiah* 10, no. 2 (August 31, 2018): 175–81, https://doi.org/10.33096/ilkom.v10i2.309.175-181.

a 46% increase compared to the fourth quarter of 2017.[7]

The Indonesian Internet Domain Name Administrator (Pengelola Nama Domain Internet Indonesia or PANDI) reported that there had been approximately 5.579 phishing incidents in the country from April to June 2022.[8] The Directorate of Cyber Crime (Direktorat Tindak Pidana Siber or Dittipidsiber) of the Indonesian National Police's Criminal Investigation Unit (Bareskrim Polri) uncovered a fraud syndicate involved in modifying Android Package Kit (APK) and using phishing links. They have arrested 13 suspects in connection with these activities.[9] In West Java itself, a phishing case was uncovered by the Subdirectorate V Cybercrime Team of the Directorate of Special Criminal Investigation of the West Java Regional Police. They successfully apprehended a phishing criminal who originated from Palembang. The victims of this crime came from various provinces in Indonesia, including West Java.[10]

An example of a phishing case involving the misuse of personal data is the incident experienced by users of the digital financing service Kredivo, where someone contacts the victims via phone and claims to have promotions, bonuses, or prizes. The victims subsequently receive inflated bills for purchases made through e-commerce platforms.[11] Based on the above explanation, the author of this article will discuss the implications of digital transformation and the vulnerability of personal data with the emergence of phishing as a form of cybercrime, its modus operandi in Indonesia, and the handling and prevention measures. The information and statements provided serve as the basis for this discussion.

[7] Ginanjar, Aseh, Nur Widiyasono, and Rohmat Gunawan. "ANALISIS SERANGAN WEB PHISHING PADA LAYANAN E-COMMERCE DENGAN METODE NETWORK FORENSIC PROCESS". *Jurnal Terapan Teknologi Informasi* 2, no. 2 (February 27, 2019): 147–157. Accessed June 13, 2023. https://jutei.ukdw.ac.id/index.php/jurnal/article/view/111.

[8] ANTARA News Agency, "5.579 Laporan 'Phising' Di Kuartal Kedua, Kata PANDI," ANTARA News Jawa Barat, accessed March 30, 2023, https://jabar.antaranews.com/berita/397305/5579-laporan-phising-di-kuartal-kedua-kata-pandi.

[9] "483 Orang Jadi Korban Penipuan Modus Link Phising Dan APK, Kerugian Rp12 Miliar | Merdeka.Com," accessed June 7, 2023, https://www.merdeka.com/peristiwa/483-orang-jadi-korban-penipuan-modus-link-phising-dan-apk-kerugian-rp12-miliar.html.

[10] Dony Indra Ramadan, "Polda Jabar Bekuk Warga Palembang yang Lakukan Phishing dan Phone Sex," detiknews, accessed March 21, 2023, https://news.detik.com/berita-jawa-barat/d-5838741/polda-jabar-bekuk-warga-palembang-yang-lakukan-phishing-dan-phone-sex.

[11] Aziz Rahardyan, "Kasus Phising Kredivo, Pengamat: Pelaku Manfaatkan Kebocoran Data," Bisnis.com, December 24, 2021, https://finansial.bisnis.com/read/20211224/563/1481571/kasus-phising-kredivo-pengamat-pelaku-manfaatkan-kebocoran-data.

This article aims to analyze the modus operandi of phishing crimes and the preventive efforts against them. The article seeks to address its urgency, at least for the following two reasons: First, to provide an overview of phishing crimes by exploring various modus operandi associated with phishing. Second, to formulate prevention efforts against phishing crimes as an alternative approach to combating such crimes. Thus, this study will contribute not only to the development of legal and constitutional knowledge but also to finding avenues that can be utilized to prosecute perpetrators of phishing crimes.

DISCUSSION

Almost every aspect of life is influenced by the ongoing rapid digital transformation. The business models are changing due to digital transformation, resulting from the disruption era or Industry 4.0. This transformation is reshaping the existing business landscape into a new environment that is more innovative, complex, and dynamic.[12] Digital transformation is the shift in how businesses leverage information technology to become more efficient and effective. Various industries have transformed areas such as e-learning, business operations, banking, government, and many more. The core of this transformation is the improvement of work efficiency and effectiveness through the utilization of databases. The primary objective is to eliminate the reliance on physical documents; with databases replacing traditional paper-based transaction records, making processes easier and more flexible.

Various industries have undergone transformations in areas such as e-learning, business operations, banking, government, and many more. The core of this transformation is to enhance work efficiency and effectiveness through the utilization of databases. The primary objective is to eliminate the reliance on physical documents, with databases replacing traditional paper-based transaction records, making processes more straightforward, more flexible, and accessible at any time. Every individual and company involved in the business process can experience the impact of these changes, both positively and negatively.[13]

[12] Shinta Winasis, “Transformasi Digital di Industri Perbankan Indonesia : Impak pada Stress Kerja Karyawan,” *IQTISHADIA Jurnal Ekonomi & Perbankan Syariah* 7, no. 1 (July 8, 2020): 55–64, https://doi.org/10.19105/iqtishadia.v7i1.3162.

[13] M. Danuri, “Development and Transformation of Digital Technology,” Infokam, vol. XV, no. II, pp. 116–123, 2019, [Online]. Available:

The banking sector has often been targeted by phishers as a place for exploitation. Data on electronic transaction records from a bank in Indonesia from 2016 to 2019 indicates an increase in fraud cases that correlates with the growing prevalence of electronic transactions, particularly e-commerce.[14]

Table 1. Comparison Data between Electronic Transactions and Fraud Transactions

No	Year	Electronic Transactions Data	Fraud Transactions Data
1	2016	0,3 Trillion	1,6 Billion
2	2017	0,6 Trillion	7,8 Billion
3	2018	3 Trillion	10,9 Billion
4	2019	18 Trillion	21,3 Billion

Source: Author's processed secondary data, 2023

Hackers continue to favor this type of cybercrime. As a result, internet crime still thrives, particularly in identity theft. A report states that phishing accounts for 67% of cybercrimes. Personal, account, and financial data are the targets of phishing. Phishing typically succeeds because perpetrators impersonate trustworthy individuals or official institutions, making the victims unsuspecting. The use of Paypal is one well-known case of phishing. Perpetrators send emails to victims, pretending to be representatives of Paypal. In the email, they claim that the victims have caused an issue due to policy violations. The perpetrators then ask the victims to update their accounts, providing a link redirecting them to a fake website. On this website, the victims unknowingly input their information as instructed, allowing the perpetrators to obtain the desired information.[15]

Phishing attacks actually have success rate of 30% or higher. It is very unreasonable that hackers can gain monetary benefits or other advantages with just a few clicks. As a result, sending millions of emails to victims, pretending to request government funds, can yield quick

https://www.researchgate.net/publication/346898118_perkembangan_dan_transformasi_teknologi_digital.

[14] Rhesita Yustitiana, "Pelaksanaan Pengaturan Hukum Tindak Kejahatan Fraud Phishing Transaksi Elektronik Sebagai Bagian Dari Upaya Penegakan Hukum Di Indonesia Dikaitkan Dengan Teori Efektivitas Hukum" 1 (2021).

[15] Tonny Rompi and Harly Stanly Muaja, "Tindak Kejahatan Siber Di Sektor Jasa Keuangan Dan Perbankan1 Oleh: Faysal Banua Suwiknyo2," no. 4 (n.d.).

and significant rewards.[16]

Phishing is the act of obtaining users' personal data by using fake emails and websites that appear to be genuine or official. Phishers collect or search for victims' account passwords or credit card numbers. They use emails, banners, or pop-up windows to lure users to fake websites where they request personal data. This is where phishers take advantage of users' carelessness and oversight on the fake website to obtain their data.[17]

First, the source of phishing consists of over 120.000 phishing attacks peaking at billions of emails in 2014. 65% of these attacks start with visiting a link sent through email. Furthermore, the Anti-Phishing Working Group received 229.265 reports of phishing emails from consumers in March 2016. 18,3% of Australians fell victim to email phishing. Second, through phishing websites, which combine advertisements with social media platforms like Facebook, Twitter, and Instagram. A survey conducted by Facebook indicated that 8,7% of 83.090.000 accounts were not genuine users. Additionally, an estimated 1,5% of the 14.320.000 accounts unknowingly spread harmful content, such as spam messages and suspicious links. The majority of phishing attacks occur through hacked web servers, affecting 73% of the targeted sites. Third, phishing attacks also occur through malware distribution, one example is Koobface malware, which victimized 81% of users.

Phishing Modus Operandi And Perpetrator's Methods

In 2001, a case resembling phishing occurred in Indonesia. At that time, several banks in Indonesia had just introduced internet banking services, and one of the affected banks was Bank Central Asia (BCA). In this case, the perpetrator purchased six domains with names similar to the genuine BCA website, www.klikbca.com. This led unsuspecting BCA customers to believe that one of the fake websites was BCA’s actual internet banking website. As a result, when customers entered their user ID and Personal Identification Number (PIN) into the fake website, the data was successfully recorded by the perpetrator and stored on their computer's

[16] Yudi Herdiana, Zen Munawar, and Novianti Indah Putri, “Mitigasi Ancaman Resiko Keamanan Siber Di Masa Pandemi Covid-19,” *Jurnal ICT : Information Communication & Technology* 20, no. 1 (July 5, 2021): 42–52, https://doi.org/10.36054/jict-ikmi.v20i1.305.

[17] Wenceslaus Candraditya Pamungkas and Fahmy Trimuti Saputra, “Analisa Mobile Phishing Dengan Incident Response Plan dan Incident Handling” 7, no. 4 (2020).

hard disk. The case caused a significant uproar at the time and continues to serve as an example of a phishing case that occurred in Indonesia.[18]

In the world of web phishing, the term "Web Forgery" is used because these websites are created solely to deceive visitors. The phishing process begins with the perpetrator creating a domain that serves as the host, which can be a paid or free domain. Next, the perpetrator designs the website to closely resemble the genuine website, including the layout, logo, color scheme, objects, and other small details. This is done to trick victims into providing their personal data, such as usernames and passwords, on the form present on the fake website. The victim's data is then automatically stored in the database of the fraudulent website.[19]

According to several sources, phishing attacks typically start with an email that appears to come from an organization closely related to the victim. The attack then prompts them to update their information by following a URL link provided in the email. Phishing essentially utilizes complex attack vectors and social engineering to make the email recipients feel entirely unaware of what is actually happening. Attackers will send millions of emails to millions of users, and the engineering will deceive at least thousands of people. These attacks always use fake emails to trick users into sharing their personal information. Secondly, you will be asked to provide your personal information, such as passwords and bank account numbers, on a website. This information will ultimately be used for identity theft. Additionally, phishers use tools to steal the source code of genuine websites and replace them with fraudulent ones. Furthermore, embedded links are created by phishers to gather the personal information of victims. Thirdly, malware attack techniques involve pretending to ask staff members to download files sent by phishers to neutralize malware, which ultimately leads to compromising their systems.[20]

Phishers use various strategies to target their victims, such as:

1. Email spoofing

[18] "NEWS : Ada Situs Citibank Palsu, Mirip Kasus BCA Yang Menghebohkan | Cyberthreat.Id," accessed June 13, 2023, https://m.cyberthreat.id/read/4842/Ada-Situs-Citibank-Palsu%20Mirip-Kasus-BCA-yang-Menghebohkan/,.

[19] Vikran Fasyadhiyaksa Putra Y, "Modus Operandi Tindak Pidana Phising Menurut UU ITE," *Jurist-Diction* 4, no. 6 (November 5, 2021): 2525–48, https://doi.org/10.20473/jd.v4i6.31857.

[20] Wibowo and Fatimah, "Ancaman Phishing Terhadap Pengguna Sosial Media Dalam Dunia Cyber Crime."

Phishers commonly use email spoofing to send emails to millions of users, pretending to be from official institutions. The emails usually request users to download specific forms or provide credit card information.

2. Web-based delivery

   Web-based delivery is one of the most sophisticated phishing methods. Hackers, also known as "man-in-the-middle," operate between the phishing system and the genuine website.
3. Instant messaging phishing

   Users receive instant messages with links that redirect them to fake phishing websites designed to resemble authentic ones.
4. Host Trojan

   Phishers attempt to access user accounts and collect credentials through the local machine using a host Trojan.
5. Phishers send acquired data to another phisher: In this scenario, phishers create links to websites that direct users to the phisher's site instead of the legitimate one, enabling them to obtain sensitive information.
6. Phishing malware

   Phishing malware consists of malicious software that needs to be installed on the user's computer. Phishers often include this malware in emails sent to users. Victims are required to click on a link to initiate the malware. Sometimes, the downloaded file contains malware.

It is crucial to remain vigilant and exercise caution when dealing with suspicious emails, links, and downloads to protect yourself from phishing attacks.

Enforcement Against Perpetrators Of Phishing Crimes

To take action against phishing criminals, Article 35, in conjunction with Article 51 Section (1) of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) can be applied, which states

> *"Any person who intentionally and without right or unlawfully engages in*

> *manipulation, creation, alteration, deletion, or destruction of Electronic Information and/or Electronic Documents with the intention of making the Electronic Information and/or Electronic Document appear as if it is authentic data shall be subject to penalties under the ITE Law."*

> *"Any person who meets the elements as referred to in Article 35 shall be punished with a maximum imprisonment of 12 (twelve) years and/or a fine of up to IDR 12.000.000.000,00 (twelve billion Indonesian Rupiah)."*

The reasoning behind this is that creating fake websites resembling genuine ones and engaging in activities that deceive individuals into accessing false links and providing their confidential information, which should remain private, can be subject to Article 28 Section (1) in conjunction with Article 45A Section (1) of the ITE Law. With appropriate legal policies in place, effective measures can be taken to combat cybercrime, and the prosecution of such crimes can be conducted effectively. In line with this, Article 1 Section (3) of the 1945 Constitution of the Republic of Indonesia states that Indonesia, as a legal state, must uphold the law in every action taken by the state without exception. Therefore, the writer believes that laws should govern activities conducted in the virtual realm, such as electronic transactions, so that individuals engaging in electronic transactions can determine which laws are applicable and which are not, particularly in Indonesia.

One of the other laws that can be used to address the crime of phishing fraud in electronic transactions is the Indonesian Criminal Code (Kitab Undang-Undang Hukum Pidana or KUHP). However, the Criminal Code does not explicitly mention phishing fraud as an electronic transaction crime. To handle phishing fraud, the Criminal Code applies methods of interpretation or analogy to articles that can still fall under the category of electronic transaction crimes, such as theft, embezzlement, defamation, and slander, which can be committed without territorial or locational limits. To address phishing fraud, Article 362 of the Criminal Code states:

> *"Any person takes someone else's property, either wholly or in part, with the intention of unlawfully possessing it, shall be subject to the crime of theft,*

> *punishable by a maximum imprisonment of five years or a fine of up to nine hundred Indonesian Rupiah.*"

Article 378 of the Indonesian Criminal Code (KUHP) states:

> *"Any person, with the intention of unlawfully benefiting themselves or others, intentionally exploits opportunities, mistakes, negligence, carelessness, or the trust of others to engage in trickery that causes harm to others, shall be subject to the offense of fraud, punishable by a maximum imprisonment of four years and six months or a fine of up to nine hundred Indonesian Rupiah."*

Therefore, the crime of phishing in electronic transactions is typically carried out by two or more individuals who assist in its commission. Hence, Article 363 Section (4) and Article 55 of the Criminal Code are usually applied regarding involvement in resolving cases of phishing fraud. The use of the Criminal Code in addressing cases of electronic transaction crimes is considered one of the efforts to fill the legal gap.

Prevention and Mitigation of Phishing

To prevent or anticipate phishing, the following steps can be used and maximized:[21]

1. Using toolsdetect to identify phishing attempts is an effective preventive measure. The internet has become an essential part of our daily lives, and for some individuals, it is indispensable. While the internet allows us to do many things, such as searching and sharing information, we often find attractive but unwanted websites. It can be tempting to input necessary information without realizing it is a phishing site. To prevent this, we can utilize detection tools that can distinguish between genuine and fake websites. These tools help identify and avoid potential phishing attacks, safeguarding our personal and sensitive information.
2. Using additional web browsers that protect against tabnabbing is another important measure. Phishers continuously develop new attacks each year, and tabnabbing is one of the newer techniques. This phishing attack occurs online, where phishing sites appear

[21] Wibowo and Fatimah.

in between other tabs when users have multiple tabs open. The attack begins when the user is distracted and opens a new tab. The fake tab then switches with one of the tabs the user has opened, making the genuine tab disappear. This attack is considered clever because it no longer relies on previously clicked links to lure users into the phisher's trap. By using web browsers that provide protection against tabnabbing, users can mitigate the risk of falling victim to such phishing attacks and maintain a safer browsing experience.

3. Using anti-phishing pre-filters is another effective method for preventing phishing. These pre-filters consist of three prevention components: site identifier, login form finder, and webpage feature generator. The prevention process occurs in stages. Additionally, detection is performed through streaming analysis, where many individuals are researching to develop tools or applications. People are also exploring various methods of detection. Furthermore, this anti-phishing approach utilizes streaming analysis called PhisStrom to detect phishing attempts. By implementing anti-phishing pre-filters, users can enhance their protection against phishing attacks and minimize the risk of falling victim to fraudulent schemes.

The Organization for Economic Cooperation and Development (OECD) report titled "Computer-Related Crime: Analysis of Legal Policy" in 1986 outlined several important steps that every country should take to combat cybercrime. These steps include increasing awareness among law enforcement agencies regarding prevention efforts, investigation techniques, and prosecution of cybercrimes, as well as raising public awareness about the importance of preventing the spread of cybercrime. By doing so, countries can effectively address cybercrime and create awareness among citizens about the significance of preventing the proliferation of cybercrime.[22]

CONCLUSION

This article discusses the modus operandi of phishing crimes and various prevention methods. Phishing is an online fraud where attackers attempt to obtain sensitive information

[22] “Interpol Indonesia,” accessed June 12, 2023, https://interpol.go.id/kejahatanduniamaya2.php.

such as passwords, credit card numbers, or other personal data by impersonating trusted entities. The conclusion of this article emphasizes the importance of individual awareness in recognizing and protecting oneself from phishing attacks. By implementing appropriate prevention measures, we can reduce the risk of falling into phishing traps and safeguard our personal information from malicious attackers. To prosecute phishing criminals, existing legal regulations in Indonesia optimize both repressive and preventive measures through provisions in Law Number 11 Year 2008 concerning Electronic Information and Transactions (UU ITE), as amended by Law Number 19 Year 2016, along with the Indonesian Criminal Code (Kitab Undang-Undang Hukum Pidana or KUHP). However, it is noted that the current legal framework, which mainly focuses on conventional crimes, may not always fit the category of electronic transaction crimes in the Criminal Code. This highlights the need for relevant regulations addressing electronic crimes to ensure comprehensive legal coverage.

REFERENCES

"483 Orang Jadi Korban Penipuan Modus Link Phising Dan APK, Kerugian Rp12 Miliar | Merdeka.Com." Accessed June 7, 2023. https://www.merdeka.com/peristiwa/483-orang-jadi-korban-penipuan-modus-link-phising-dan-apk-kerugian-rp12-miliar.html.

Agency, ANTARA News. "5.579 Laporan 'Phising' Di Kuartal Kedua, Kata PANDI." ANTARA News Jawa Barat. Accessed March 30, 2023. https://jabar.antaranews.com/berita/397305/5579-laporan-phising-di-kuartal-kedua-kata-pandi.

Banjarnahor, Andrew Christian, and Puti Priyana. "ANALISIS YURIDIS CYBERCRIME TERHADAP PENANGANAN KASUS PHISING KREDIVO." *HERMENEUTIKA : Jurnal Ilmu Hukum* 6, no. 1 (February 28, 2022). https://doi.org/10.33603/hermeneutika.v6i1.6754.

Efendy, Zainul, Ilham Eka Putra, and Rangga Saputra. "ASSET RENTAL INFORMATION SYSTEM AND WEB-BASED FACILITIES AT ANDALAS UNIVERSITY." *Jurnal Terapan Teknologi Informasi* 2, no. 2 (February 15, 2019): 135–46. https://doi.org/10.21460/jutei.2018.22.103.

Ginanjar, Aseh, Nur Widiyasono, and Rohmat Gunawan. "ANALISIS SERANGAN

WEB PHISHING PADA LAYANAN E-COMMERCE DENGAN METODE NETWORK FORENSIC PROCESS”. *Jurnal Terapan Teknologi Informasi* 2, no. 2 (February 27, 2019): 147–157. Accessed June 13, 2023. https://jutei.ukdw.ac.id/index.php/jurnal/article/view/111.

Herdiana, Yudi, Zen Munawar, and Novianti Indah Putri. “Mitigasi Ancaman Resiko Keamanan Siber Di Masa Pandemi Covid-19.” *Jurnal ICT : Information Communication & Technology* 20, no. 1 (July 5, 2021): 42–52. https://doi.org/10.36054/jict-ikmi.v20i1.305.

“Interpol Indonesia.” Accessed June 12, 2023. https://interpol.go.id/kejahatanduniamaya2.php.

Krismono, Bagus Dwi, and Nasikh Nasikh. “INOVASI TEKNOLOGI DIGITAL UNTUK PENGENTASAN KEMISKINAN PADA PERTANIAN DATARAN TINGGI SAAT PANDEMI COVID-19.” *Equilibrium : Jurnal Ilmiah Ekonomi, Manajemen dan Akuntansi* 11, no. 1 (April 21, 2022): 9. https://doi.org/10.35906/equili.v11i1.962.

“NEWS : Ada Situs Citibank Palsu, Mirip Kasus BCA Yang Menghebohkan | Cyberthreat.Id.” Accessed June 13, 2023. https://m.cyberthreat.id/read/4842/Ada-Situs-Citibank-Palsu%20Mirip-Kasus-BCA-yang-Menghebohkan/,.

Pamungkas, Wenceslaus Candraditya, and Fahmy Trimuti Saputra. “Analisa Mobile Phishing Dengan Incident Response Plan dan Incident Handling” 7, no. 4 (2020).

Rahardyan, Aziz. “Kasus Phising Kredivo, Pengamat: Pelaku Manfaatkan Kebocoran Data.” Bisnis.com, December 24, 2021. https://finansial.bisnis.com/read/20211224/563/1481571/kasus-phising-kredivo-pengamat-pelaku-manfaatkan-kebocoran-data.

Ramadan, Dony Indra. “Polda Jabar Bekuk Warga Palembang yang Lakukan Phishing dan Phone Sex.” detiknews. Accessed March 21, 2023. https://news.detik.com/berita-jawa-barat/d-5838741/polda-jabar-bekuk-warga-palembang-yang-lakukan-phishing-dan-phone-sex.

Rifqi Noval, Sayid Muhammad. “EVOLUSI HAK PEKERJA DI ERA DIGITAL: PRAWACANA RIGHT TO DISCONNECT DI INDONESIA.” *Jurnal Bina Mulia Hukum* 6, no. 2 (March 31, 2022): 234–53. https://doi.org/10.23920/jbmh.v6i2.637.

Rompi, Tonny, and Harly Stanly Muaja. “TINDAK KEJAHATAN SIBER DI SEKTOR JASA KEUANGAN DAN PERBANKAN1 Oleh: Faysal Banua Suwiknyo2,” no. 4 (n.d.).

Rustam, Suhardi. “ANALISA CLUSTERING PHISING DENGAN K-MEANS DALAM MENINGKATKAN KEAMANAN KOMPUTER.” *ILKOM Jurnal Ilmiah* 10, no. 2 (August 31, 2018): 175–81. https://doi.org/10.33096/ilkom.v10i2.309.175-181.

Wibowo, Mia Haryati, and Nur Fatimah. “ANCAMAN PHISHING TERHADAP PENGGUNA SOSIAL MEDIA DALAM DUNIA CYBER CRIME” 1 (n.d.).

Widodo, *Aspek Hukum Pidana Kejahatan Mayantara*, Yogyakarta: Aswaja Presindo, 2013, hlm. 7.

Winasis, Shinta. “Transformasi Digital di Industri Perbankan Indonesia : Impak pada Stress Kerja Karyawan.” *IQTISHADIA Jurnal Ekonomi & Perbankan Syariah* 7, no. 1 (July 8, 2020): 55–64. https://doi.org/10.19105/iqtishadia.v7i1.3162.

Y, Vikran Fasyadhiyaksa Putra. “Modus Operandi Tindak Pidana Phising Menurut UU ITE.” *Jurist-Diction* 4, no. 6 (November 5, 2021): 2525–48. https://doi.org/10.20473/jd.v4i6.31857.

Yustitiana, Rhesita. “PELAKSANAAN PENGATURAN HUKUM TINDAK KEJAHATAN FRAUD PHISHING TRANSAKSI ELEKTRONIK SEBAGAI BAGIAN DARI UPAYA PENEGAKAN HUKUM DI INDONESIA DIKAITKAN DENGAN TEORI EFEKTIVITAS HUKUM” 1 (2021).