International Journal of Multicultural and Multireligious Understanding

http://ijmmu.com
editor@ijmmu.com
ISSN 2364-5369
Volume 11, Issue7
July, 2024
Pages: 371-381

Legal Protection Efforts for Victims of Cyber Crime in the Case of Mobile Malware in the Form of Digital Invitations in the Jurisdiction of the Banten Police Force

Arif Budianto[1]; Surya Nita[2]; Mulyadi[2]

[1] Police Science Study Program, School of Strategic and Global Studies, Universitas Indonesia, Jakarta, Indonesia

[2] Lecturer in Police Science Study Program, School of Strategic and Global Studies, Universitas Indonesia, Jakarta, Indonesia

http://dx.doi.org/10.18415/ijmmu.v11i7.6038

Abstract

This study discusses legal protection for victims of cybercrime, specifically in the context of wedding invitation fraud based on Mobile Malware in the jurisdiction of the Banten Regional Police. The background of this research is the increasing cybercrimes that threaten internet users, especially Android users, with financial losses and personal data breaches as its consequences. The aim of this research is to identify the available legal protection mechanisms for victims and evaluate their effectiveness. The research methods used include field research and normative legal research. The results show that victims can utilize various legal regulations such as Article 378 of the Criminal Code, Article 263 of the Criminal Code, Article 28 paragraph (1) of the ITE Law, Consumer Protection Law Number 8 of 1999, and Bank Indonesia Regulation Number 22/20/PBI/2020 to seek legal protection and recover losses. However, the existing legal protection is still ineffective due to the lack of specific regulations regarding digital application fraud, limited cyber investigator skills, and inadequate computer forensic facilities. Additionally, security verification for financial transactions needs to be strengthened, and victims' legal awareness needs to be enhanced.

Keywords: *Cybercrime Victim; Wedding Invitation Fraud; Mobile Malware*

Introduction

Individuals in the current digital era are facing an abundance of information due to the advancement of increasingly sophisticated technology. Particularly, advancements in the field of information technology, especially in computer science and the Internet, have given rise to new types of networks that affect various aspects of life (Assiffa, 2023). Despite Indonesia experiencing a remarkable surge in technology and information in 1994, the country has since lagged behind in terms of technological and Internet advancements compared to other industrialized nations. Older generations, often referred to as digital immigrants, often struggle to adapt to this new technology, viewing it as something intimidating (Apidana et al., 2020). Individuals born before 1994 and lacking technology

experience are more susceptible to fraud, whereas nowadays, laptops, netbooks, and mobile phones are all connected to the Internet (Sugeng, 2020).

Telematics, which refers to the integration of telecommunications and informatics, represents the fusion of computing and communication (Maskun, 2022). Despite the achievements of the Internet and technology in meeting human needs and enhancing quality of life, they also come with vulnerabilities, particularly in terms of cybercrime (Budiastanti, 2017). Cybercrime, as a form of computer crime, aims to tarnish the reputation of victims and can lead to direct or indirect physical and mental losses (Arradian, 2023). The rapid progress in technology and information has streamlined numerous aspects of modern human life (Marpaung, 2018).

The growth of Internet users and Information and Communication Technology (ICT) has made this technology an important instrument in various individual, community, and organizational activities (Lestari et al., 2022). According to the APJJI survey in 2019, social networking is the most common reason for Internet usage, with a percentage of 51.5% of respondents. The widespread presence of the Internet allows unlimited access to information from anywhere and at any time. The benefits of Internet usage depend on its implementation and level of accountability (Abidin, 2015). The online world, as a virtual domain, supports various activities, enhancing convenience and efficiency in the work process (Kshetri, 2013). However, the use of the Internet for personal or group interests that violate the law can have negative consequences (Rusydi et al., 2020) .

The progress of technology has led to the emergence of various new types of crimes that take place through the Internet, commonly referred to as cybercrimes. These illegal activities are conducted through online networks, often utilizing computer devices connected to the Internet. Given the extensive reach of the Internet, such crimes can transcend national boundaries.

Cybercrime management in Indonesia is governed by Law Number 19 of 2016, amending Law Number 11 of 2008 on Electronic Information and Transactions. Various methods can be utilized to present evidence in legal processes and police investigations related to cybercrimes. These methods involve enhancing the efficiency of current laws, improving cyber investigator expertise, and expanding computer forensic facilities within the Indonesian National Police. The prevalence of cybercrimes continues to rise annually, largely due to the rapid progress in computer technology, which has both positive and negative effects on society (Septiani et al., 2016).

Phishing is one of the main methods of cybercrime that involves obtaining personal information by impersonating trusted businesses. The advancement in digital technology has made phishing attempts increasingly complex and difficult to detect, requiring strong law enforcement to combat such threats. The primary motivation for criminals using computer technology is the pursuit of profit. There are various ways in which criminal activities can be facilitated by exploiting vulnerabilities in computer networks through the infiltration of applications designed to steal information from electronic devices such as smartphones and tablets (Habib et al., 2024).

Mobile Malware, also known as malicious software, is designed to target mobile devices like smartphones and tablets. These harmful programs infiltrate files and use social engineering tactics to deceive users into running seemingly harmless files. The objectives of malware range from data theft to fraudulent transactions and ransom demands for device or data release. In 2015, G statistic Security Labs reported 3,045,722 new malware of this kind, underscoring the security risks posed by these malicious programs, which can result in substantial losses such as data breaches (Sastrawan, 2024).

According to the Security Advisory by the National Cyber and Encryption Agency (BSSN, 2023), a deceitful strategy involving the use of Android Package Kit (.apk) files disguised as wedding invitations has been discovered. This scam method allows the perpetrator to access the victim's text messages and obtain SMS banking tokens. The most vulnerable individuals to this type of fraud are active Android smartphone users across various social media platforms. Android Package Kit (.apk) is a file type used to install application software on devices running the Google Android operating system. For

instance, the scammer may use a WhatsApp message claiming to contain a wedding invitation. They then send an invitation SMS along with an attached .apk file (BSSN, 2023). Such scams pose a significant threat to inexperienced users of communication services like WhatsApp (Sastrawan, 2024)

The world of cybercrime consists of a series of steps. Once clicked, the program requests permission to access SMS or MMS activities. If permission is granted, the perpetrator can view stored SMS messages on the device and SIM card. As a result, they request authorization to perform Receive SMS activity, which allows them to monitor and potentially delete text messages discreetly. Furthermore, they request authorization to perform Send SMS action, enabling the attacker to send premium text messages without the victim's knowledge. After obtaining the necessary permissions and successfully installing the application on the victim's Android smartphone, the hacker gains access to previous banking SMS data, including the victim's PIN number typically stored. With this sensitive information, the attacker can carry out transactions in the victim's account without their knowledge (Arradian, 2023).

The rise in internet users and widespread adoption of Information and Communication Technology (ICT) are crucial elements in supporting various activities for society, communities, and institutions (Lestari et al., 2022). According to a survey conducted by APJJI in 2019, the most common reason individuals use the internet is for social media, with a percentage reaching 51.5%. Utilizing this technology provides unlimited access to information regardless of time and place. However, the benefits of internet use can only be optimal when done responsibly and within reasonable limits (Abidin, 2015). All kinds of activities can be carried out through cyberspace supported by the internet, offering dual advantages in terms of convenience and efficiency (Ketaren, 2016). Nevertheless, despite its advantages, the internet can also lead to disadvantages if individuals or groups exploit it for unlawful purposes (Danuri & Suharnawi, 2017; Rusydi et al., 2020).

The rise of cybercrimes, facilitated by technological advancements, has led to the emergence of new criminal activities that exploit computer networks. These crimes, such as online fraud schemes utilizing social engineering tactics on messaging apps like WhatsApp and Telegram, pose a threat to users by potentially draining their bank accounts. Wedding invitation scams, specifically targeting Android users through the APK application, are on the rise, particularly among less experienced individuals. WhatsApp scams primarily aim to achieve financial gains, taking advantage of the growing trend of digital banking and transactions conducted through mobile banking and digital wallets (Iskandar, 2023).

Alfons Tanujaya, a cybersecurity expert and digital forensics analyst at Akuncom, emphasizes the strong security verification process for financial transactions on Android smartphones. Users must input a PIN/secret password for each transaction, adding an extra layer of security (Iskandar, 2023). For crucial verifications like transferring accounts or changing phone numbers, a one-time password (OTP) is required as part of the two-factor authentication (TFA) process, known only to the account owner. However, Tanujaya notes that OTPs sent via SMS are considered weak due to the outdated and unencrypted nature of SMS communication, making them susceptible to theft and involving third parties in the delivery process.

Further, Alfons advises both customers and banks to be cautious when using OTP sent via SMS due to serious security risks that may arise if the SMS is hacked. Furthermore, in case of OTP breaches, financial service providers, including banks and digital wallet operators, should take additional security measures, such as physical verification, especially for critical actions like transferring funds to a new phone number or device.

This problem statement highlights the serious challenges faced by digital wedding invitation fraud based on mobile malware, as well as the lack of legal protection for cybercrime victims within the jurisdiction of the Banten Regional Police (POLDA BANTEN). It underscores the increasing threat of cybercrime, especially through emerging strategies such as social engineering via instant messaging applications and exploiting vulnerabilities in digital banking security, particularly OTPs sent via SMS. The statement emphasizes the importance of legislative protection to safeguard cybercrime victims, especially those targeted by mobile malware scams, and proposes enhanced security measures.

Drawing from the information presented, the goal of this study is to assess the legal safeguards accessible to victims of cybercrime, particularly in cases of wedding invitation scams involving Mobile Malware within the legal jurisdiction of the Banten Regional Police (POLDA BANTEN). Furthermore, it aims to scrutinize the primary obstacles encountered by victims of Mobile Malware-based wedding invitation scams as they strive to attain justice and recover losses within the legal framework of POLDA BANTEN.

Method

This research utilizes a field research method, which involves systematically collecting information and data in the field (Arikunto, 1995). Field research is a qualitative study that directly observes and participates in small-scale social research and observes local culture (Assiffa, 2023). Additionally, this research also employs normative legal research. The research method employs a qualitative approach with qualitative data collection tools such as interviews, observations, documents, literature, and library resources.

This research adopts a normative legal approach by using both a statutory approach and a conceptual approach to test the norms related to the analyzed legal issues. In practice, this legal approach provides opportunities for researchers to examine the consistency and compatibility between regulations. The outcome of this research is an argument for solutions to the problems at hand (Marzuki, 2021). Furthermore, this research falls under the qualitative approach, which involves descriptive data in the form of written or oral information regarding individuals and their attitudes that can be observed.

Careful identification of data sources is crucial to gain a comprehensive understanding of legal protection for cybercrime victims in cases of mobile malware in the jurisdiction of the Banten Regional Police (POLDA BANTEN). In the context of this research, primary legal materials primarily come from interviews with direct stakeholders, such as cybercrime victims, law enforcement officials, and legal experts. The interviews are conducted to gather information about the experiences, perceptions, and challenges faced by cybercrime victims in cases of mobile malware-based wedding invitations. Secondary legal materials are used to analyze the existing legal framework related to the legal protection of cybercrime victims in the jurisdiction of POLDA BANTEN. This involves examining laws, regulations, and policies related to the handling of cybercrime cases, particularly in the context of victim protection. For example, analysis is conducted on laws governing cybercrime offenses, personal data protection, and the rights of victims in the judicial process. Tertiary data sources include books, legal journals, articles, and relevant documents discussing legal protection for cybercrime victims.

The key to obtaining relevant and in-depth information about legal protection for cybercrime victims in cases of mobile malware in the digital invitation form in the jurisdiction of the Banten Regional Police (POLDA BANTEN) lies in data collection techniques. Here are the data collection techniques used: direct observation of relevant situations, such as the interaction between victims and technology systems, as well as law enforcement efforts in handling similar cases (Sugiyono, 2018). Interviewing becomes a crucial method in collecting relevant and in-depth data regarding legal protection for cybercrime victims in cases of mobile malware in the digital invitation form in the jurisdiction of POLDA BANTEN. Documentation technique is also important in collecting data related to legal protection for cybercrime victims in cases of mobile malware in the digital invitation form in the jurisdiction of POLDA BANTEN.

Moleong (2009) emphasizes the importance of using various techniques for data verification to ensure reliability. This includes considering criteria such as confidence level, transferability, dependency, and confirmability. These criteria guide the verification process, which involves data reduction, presentation, and drawing conclusions in the data analysis (Miles & Huberman, 1992).

Results and Discussion

A. Legal Protection for Victims of Wedding Invitation Fraud Based on Mobile Malware at the Banten Regional Police

Fraudulent activities through digital applications continue to occur, causing harm to many parties who are referred to as victims. Moreover, cases of fraud through digital apps are on the rise, with one example being the use of digital wedding invitations as a modus operandi. Recently, a vehicle accessories entrepreneur from Malang fell victim to a scam involving digital wedding invitations via WhatsApp. As a result, the victim suffered financial losses.

The legal protection against wedding invitation fraud based on mobile malware involves safeguarding against malicious activities that target smartphones, which store sensitive and important information for transactions (Minarosa, 2022). As technology advances, the legal framework adapts to protect software investments, including sophisticated mobile operating systems that are vulnerable to malware attacks (Jing et al., 2019). The development of behavior-based mobile malware analysis methods and defense systems is crucial in efficiently detecting and blocking new malware, ensuring user security and privacy (Graham, 1984; Sui & Guo, 2012). By implementing regulations, the scope can be expanded to combat mobile malware designed to exploit events like wedding invitations, protecting users from fraudulent activities and data breaches.

Establishing a legal framework for victims of wedding invitation fraud based on Mobile Malware is crucial to ensure justice and recovery of losses. Firstly, Article 378 of the Criminal Code serves as the main legal basis in combating fraud, where perpetrators who commit fraudulent acts causing harm to victims can be prosecuted with criminal penalties. This provides a strong foundation for victims to report fraudulent activities to the authorities and ensure that the perpetrators are brought to justice. Additionally, the Latest Article 263 of the Criminal Code plays a significant role in addressing the spread of fake news that can lead to losses. This article is relevant when fake wedding invitations are circulated through digital applications, so that individuals intentionally spreading false information can face sanctions.

Furthermore, Article 28 paragraph (1) of the ITE Law strengthens consumer protection in electronic transactions by emphasizing that anyone who intentionally spreads false and misleading news without authority, resulting in consumer losses, can be sentenced to up to 6 years in prison and/or fined up to Rp. 1 billion. This provides a strong legal instrument to prosecute perpetrators who exploit technology to commit fraud. The Consumer Protection Law Number 8 of 1999 also grants clear rights to consumers to receive legal protection, including the right to accurate information and the right to compensation, ensuring that victims have a strong legal basis to seek recovery (Bessie & Rudy, 2024).

Furthermore, Bank Indonesia Regulation Number 22/20/PBI/2020 on Consumer Protection in Indonesia's Banking Sector adds an extra layer of protection for customers as financial consumers. This regulation ensures that customers receive their rights, including transparent information about banking products, good services, and proper handling of customer complaints. In the context of Mobile Malware-based fraud, customers who have been harmed by fraudulent activities utilizing digital banking services can assert their rights for compensation or reimbursement.

Legal remedies for victims involve reporting to authorities such as the police for investigation and prosecution of the perpetrator, as well as filing a civil lawsuit to seek compensation. This process is crucial to ensure that fraudsters receive appropriate sanctions and victims obtain justice and recovery for their losses. By utilizing existing laws and appropriate legal measures, victims of wedding invitation-based Mobile Malware scams can strive to obtain fair justice and adequate compensation for their damages.

The legal protection for victims of fraud through digital applications can be based on several articles in existing legislation. For example, Article 378 of the Criminal Code, the latest Article 263 of the Criminal Code, and Article 28 paragraph (1) of the ITE Law. This protection includes imposing criminal sanctions on the perpetrators as a form of accountability towards the victims. In addition, Law Number 8

of 1999 concerning Consumer Protection can also be used to demand accountability from service providers, such as banks, for the losses suffered by the victims.

However, the legal protection framework is still experiencing normative ambiguity. Victims of fraud through digital applications cannot be clearly categorized as consumers, because there is an agreement or covenant between the victim and the bank that creates certain terms and conditions. Furthermore, the lack of clarification on rules regarding fraud through digital applications makes these cases difficult to prove. Therefore, it is necessary to improve and limit one article in the legislation specifically addressing the rights of victims of fraud through digital applications.

The laws in Indonesia have clearly regulated the crime of fraud in Article 378 of the Criminal Code (Susanto et al., 2022). This article states that fraud is an act of unlawfully benefiting oneself or others by using false identities or deceptive tricks to persuade others to surrender goods, provide loans, or cancel debts. However, this article does not specifically address online fraud, leaving a legal loophole in dealing with fraud that occurs online, such as fake job postings, online businesses, giveaways, and wedding invitations. To address this issue, the Indonesian government has issued specific regulations regarding cybercrime through Law Number 19 of 2016, which is a revision of Law Number 11 of 2008 concerning Information and Electronic Transactions. This law aims to ensure the recognition and respect for the rights and freedoms of others, as well as meet the demands of justice in accordance with considerations of security and public order in a democratic society, in order to create justice, public order, and legal certainty.

In an effort to protect the community from online crime threats, the government revised Law Number 11 of 2008 to Law Number 19 of 2016 on Electronic Information and Transactions, which provides a strong legal basis for prosecuting digital criminals. Despite efforts to strengthen penalties for online criminals, some parties criticize the changes because the definition and explanation of online fraud are considered unclear and lacking in detail. The revision does not explicitly explain the definition of fraud, leading to doubts in determining the boundaries and relevant legal references.

The absence of the term "fraud" in several articles of Law Number 19 of 2016 has become a serious concern for the legal community and society, as it creates a loophole that criminals can exploit to evade legal responsibility. However, certain provisions in the law, particularly Article 28 Paragraph (1), provide a reference point for combating crimes in the digital world. This article states that anyone who intentionally and without authority accesses an electronic system will be subject to criminal sanctions. Although it does not directly mention fraud, this article serves as the legal basis for addressing digital crimes.

In order to enhance legal protection, it is necessary to review and improve the provisions in the law. It is also important to increase legal understanding and awareness among the public regarding the threats of cybercrime. Strong collaboration between the government, legal institutions, and society is required to create a safe and trustworthy digital environment for everyone. Article 45A, Paragraph (1) of Law Number 19 of 2016 explains that violations of Article 28, Paragraph (1) can be punished with imprisonment of up to six years and a maximum fine of one billion rupiah. Although it does not specifically refer to fraud, this article pertains to online fraud through the dissemination of false and misleading information that results in consumer losses. The implementation of the Information and Electronic Transactions Law (ITE) No. 19 of 2016, particularly in relation to fraud using mobile malware, is crucial in addressing the increasing issue of cybercrime in Indonesia. This law, enacted in 2016, aims to regulate electronic transactions and protect individual rights in the digital environment. Specifically, it addresses issues related to data protection, electronic signatures, and the legal framework for electronic transactions. The law provides a legal framework for prosecuting fraud cases involving mobile malware. For example, Article 45A of the law, which deals with electronic transactions, outlines the legal requirements for conducting electronic transactions and the responsibilities of the parties involved in these transactions. This includes requirements for electronic signatures and the need for parties to ensure the security and integrity of transactions.

In the context of mobile malware, laws can be used to prosecute cases of fraud where malware is used to compromise the security of mobile devices and steal sensitive information. The law requires parties involved in electronic transactions, including those using mobile devices, to ensure the security and integrity of these transactions. This includes implementing measures to prevent unauthorized access to devices and data, as well as reporting any security breaches to the appropriate authorities.

The enforcement of laws in relation to cases of mobile malware fraud involves several key steps. Firstly, law enforcement agencies must be able to identify and trace the source of the malware, which can be challenging given the anonymity of the internet. Secondly, they must gather evidence of the fraud, including any data that may have been stolen or compromised during the attack. Lastly, they must prosecute the perpetrators under relevant laws, which include penalties for unauthorized access to electronic data and the use of unauthorized electronic signatures.

B. Challenges Faced by Victims of Wedding Invitation Fraud Based on Mobile Malware in Seeking Justice at the Banten Regional Police

Victims of mobile malware-based wedding invitation scams face significant challenges in seeking justice and recovering their losses. The marginal importance of criminal law to victims and the losses they experience exacerbates the difficulties faced by victims (Vincent, 2017), compounded by the anonymity and impermanence of online evidence that hinders criminal punishment. Online fraud victims often experience negative interactions in the "fraud justice network" and lack adequate support services (Cross et al., 2016). The impact of online fraud is not only limited to financial losses, but also to physical and emotional health decline, relationship breakdowns, and even suicide (Cross, 2018). The global challenge of cybercrime, including economic losses and reputation damage, persists despite existing laws, as cybercriminals continue to evolve their techniques (Ajayi, 2016). Organizations in the fraud justice network also struggle to effectively address individual victimization, highlighting tensions and areas for improvement (Cross, 2019).

Victims of mobile malware-based wedding invitation scams face various major challenges in their efforts to seek legal justice and recover their losses under the existing legal framework. One of the biggest challenges is the ambiguity of the laws governing fraud through digital applications. This ambiguity makes it difficult to legally prosecute fraudsters, leaving victims struggling to obtain the justice they deserve. Additionally, the difficulty of providing evidence poses a significant problem as digital fraud cases often lack concrete proof. Mobile malware can easily erase its digital traces, making it challenging for authorities to conduct effective investigations and prosecutions.

The absence of specific regulations governing legal protection for victims of fraud through digital applications results in inadequate protection for the victims. The legal protection regulations for victims of fraud through digital applications are still unclear and there is no specific regulation governing this matter. As a result, victims do not receive the necessary protection, as existing regulations such as Article 378 of the Criminal Code, the latest Article 263 of the Criminal Code, and Article 28 paragraph (1) of the ITE Law do not specifically define the proportion of "fraud," especially for fraud unrelated to buying and selling. This situation leads to victims' rights to seek accountability from perpetrators not being fulfilled and legal protection for victims of fraud through digital applications becoming difficult to achieve.

The lack of clarity in the legal norms regarding fraud through digital applications has resulted in several difficulties in legally prosecuting perpetrators and providing adequate protection to victims. The regulations concerning fraud through digital applications have not been clearly defined in existing articles, such as Article 378 of the Criminal Code, the latest Article 263 of the Criminal Code, and Article 28 paragraph (1) of the ITE Law. This has made it difficult to impose criminal penalties on fraudsters and the victims' rights to seek accountability from the perpetrators have not been fulfilled.

Furthermore, there is no specific regulation that governs legal protection for victims of fraud through digital applications, leaving the victims without the proper protection they deserve. The difficulty in providing evidence also poses a challenge due to the lack of clear rules regarding fraud through digital

applications, which allows the digital footprints of the perpetrators to be easily erased, complicating the investigation process.

Victims of fraud through digital applications cannot be categorized as general consumers because of the specific agreements/contracts between the victims and the bank, which impose certain conditions and terms that are not clearly regulated in consumer protection laws. With the ambiguity of these legal norms, victims of fraud through digital applications often do not receive adequate protection and face difficulties in legally prosecuting the perpetrators.

Furthermore, the lack of protection from the bank adds complexity to this issue. Despite the victims having rights as consumers, banks often do not provide adequate protection, due to the bank's minimal responsibility in safeguarding customers from digital fraud. The lengthy and complicated legal process also poses a significant obstacle. Victims must go through various stages, from reporting to the police, investigation, to the court process, all of which require time and considerable costs. Regulations regarding fraud through digital applications are not clearly defined in existing articles, such as Article 378 of the Criminal Code, the latest Article 263 of the Criminal Code, and Article 28 paragraph (1) of the ITE Law. This causes difficulty in imposing criminal penalties on fraudsters and victims' rights to seek accountability from the perpetrators remain unfulfilled. These articles do not specifically regulate fraud through digital applications, so the elements of the criminal act required to prosecute the perpetrators are often not met. As a result, victims of fraud through digital applications do not receive adequate legal protection and face difficulties in fighting for their rights.

Despite the fact that victims are entitled to consumer rights, the protection regulations for victims of fraud through digital applications, as outlined in Article 4 of Law Number 8 of 1999 concerning Consumer Protection, are still not precise enough. This is due to the fact that victims cannot be classified as consumers in a general sense, as there are agreements/contracts between the victim and the bank that establish specific terms and conditions. Consequently, the bank's responsibility towards its customers is not clearly regulated.

The current protection regulations for victims of fraud through digital applications, based on Article 4 of Consumer Protection Law No. 8 of 1999, are not entirely appropriate due to the ambiguity of its norms. This is because the article states that one of the consumer's rights is the right to express their opinions and complaints about the goods and/or services used, as well as the right to receive compensation, damages, and/or replacements if the received goods and/or services do not comply with the agreement or as they should be. However, victims of digital application fraud cannot be categorized as consumers in general, as there is an agreement/contract between the victim and the bank, while there is no binding agreement between the seller and the consumer/buyer. Therefore, this agreement creates responsibilities for each party, including the bank's responsibility to its customers and the customers' responsibility to the bank. If the legal protection for victims of digital application fraud is based on the Consumer Protection Law, the victims cannot be fully categorized as consumers, making it difficult for them to easily claim compensation from the bank as the responsible party, as there are certain conditions arising from the agreement between the bank and the customer regarding rights and obligations.

Furthermore, the lack of awareness and legal knowledge among victims worsens the situation. Many victims do not have sufficient understanding of their rights and the legal procedures to be followed, so they are unaware of what steps to take to seek justice.

Conclusion

Legal protection for victims of cybercrime, especially in cases of wedding invitation fraud based on Mobile Malware in the jurisdiction of the Banten Regional Police (POLDA BANTEN), involves several legal protection mechanisms that victims can use to seek justice and recover losses. Victims can refer to Article 378 of the Criminal Code and Article 263 of the Criminal Code as the legal basis for prosecuting fraudsters causing losses. In addition, Article 28 paragraph (1) of the ITE Law also serves as

a relevant legal basis in cybercrime cases, including Mobile Malware-based fraud. Law Number 8 of 1999 concerning Consumer Protection provides protection for victims to demand accountability from service providers, such as banks, for the losses suffered. Furthermore, Bank Indonesia Regulation Number 22/20/PBI/2020 can also be a reference in cases of fraud involving financial transactions. Despite the available legal protection mechanisms, victims still face challenges such as difficulties in collecting evidence, anonymity, and the impermanence of online evidence that can hinder the legal process. Therefore, cooperation between authorities, legal institutions, and the community is crucial to create a safe and trustworthy digital environment for everyone.

The primary challenge faced by victims of wedding invitation fraud based on Mobile Malware in their efforts to seek justice and obtain legal compensation under the applicable legal framework in the jurisdiction of POLDA BANTEN encompasses several complex aspects. Firstly, victims encounter difficulties in receiving adequate attention from the criminal justice system regarding the losses they have suffered, as the marginal interests of criminal law towards cybercrime victims are often unmet. Secondly, the limitations in gathering electronic evidence needed to strengthen fraud cases pose a serious challenge, considering online evidence tends to be unstable and difficult to authenticate. Additionally, the lack of cyber investigators' skills and adequate computer forensic facilities also hinder law enforcement processes against cybercrime cases, including Mobile Malware-based fraud. Lastly, the anonymity of cyber criminals makes it harder to identify and prosecute them, slowing down legal proceedings and complicating victims' quest for justice. Therefore, cooperation among authorities, legal institutions, and the community is crucial to address these challenges and enhance legal protection for cybercrime victims in the jurisdiction of POLDA BANTEN.

To enhance the effectiveness of legal protection for victims of wedding invitation fraud based on Mobile Malware, it is crucial to improve the capacity of law enforcement in handling cybercrime cases. This can be achieved through specialized training in digital forensics and cybercrime investigations, as well as providing adequate technological facilities. As a result, law enforcement can be more effective in collecting and preserving the electronic evidence needed to strengthen fraud cases. Considering that the existing legal protection is still ineffective due to the lack of specific regulations regarding digital application fraud, the development of more specific and comprehensive regulations is necessary. These regulations should include clear definitions of various forms of digital fraud, including wedding invitations based on Mobile Malware, as well as more efficient mechanisms for recovering losses for victims.

Victims often struggle with gathering and preserving electronic evidence crucial for strengthening fraud cases. Online evidence is usually unstable and challenging to authenticate, which can impede the legal process. Hence, enhancing cyber investigator skills and having proper computer forensic facilities are essential to tackle this issue. The anonymity of cyber criminals complicates their identification and prosecution, leading to delays in legal proceedings and making it harder for victims to seek justice. To overcome this challenge, closer collaboration among authorities, legal bodies, and the community is necessary to identify and prosecute cybercrime offenders.

References

Abidin, D. Z. (2015). Kejahatan dalam Teknologi Informasi dan Komunikasi. *Jurnal Processor, 10*(2), 509–516.

Ajayi, E. F. G. (2016). Challenges to enforcement of cyber-crimes laws and policy. *Journal of Internet and Information Systems*, *6*(1), 1–12.

Apidana, Y. H., Suroso, A., & Setyanto, R. P. (2020). Model penerimaan teknologi mobile payment pada digital native dan digital immigrant di Indonesia. *Jurnal Ekonomi, Bisnis, Dan Akuntansi*, *21*(4).

Arradian, D. (2023). *Waspada, Malware APK Berbahaya Disebar dalam Bentuk Undangan Nikah lewat WhatsApp*.

Assiffa, B. A. (2023). *Perlindungan Hukum Terhadap Nasabah Bank Syariah Indonesia Dari Serangan Cybercrime*. Fakultas Syariah dan Hukum UIN Syarif Hidayatullah Jakarta.

Bessie, J. C. D. H., & Rudy, D. G. (2024). Consumer Protection For Losses Arising From The Use Of Auto Pilot-Based Technology In Indonesia. *Policy, Law, Notary and Regulatory Issues (POLRI)*, *3*(1), 106–112. https://doi.org/10.55047/polri.v3i1.964.

BSSN. (2023). *Imbauan Keamanan*. Jakarta: Badan Siber Dan Sandi Negara.

Budiastanti, D. E. (2017). Perlindungan Hukum Terhadap Korban Tindak Pidana Penipuan Melalui Internet. *Jurnal Cakrawala Hukum*, *8*(1), 22–32.

Cross, C. (2018). Denying victim status to online fraud victims: the challenges of being a 'non-ideal victim.' In *Revisiting the 'Ideal Victim'* (pp. 243–262). Policy Press.

Cross, C. (2019). Responding to individual fraud: Perspectives of the fraud justice network. In *The human factor of cybercrime* (pp. 359–388). Routledge.

Cross, C., Richards, K., & Smith, R. (2016). *Improving responses to online fraud victims: An examination of reporting and support. Final report for Criminology Research Grant 29/13-14*.

Danuri, M., & Suharnawi, S. (2017). Trend cyber crime dan teknologi informasi di indonesia. *Jurnal Ilmiah Infokam*, *13*(2).

Graham, R. L. (1984). The legal protection of computer software. *Communications of the ACM*, *27*(5), 422–426.

Habib, H. N., Efendi, A., & Prasetyo, D. E. (2024). Sosialisasi Fenomena Kejahatan Cyber dan Langkah Penanggulangan Sebagai Bentuk Antisipasi. *APPA: Jurnal Pengabdian Kepada Masyarakat*, *1*(5), 393–399.

Iskandar. (2023). *Begini Cara Kerja Pelaku Penipuan Undangan Pernikahan via WhatsApp yang Incar Pengguna Android*.

Jing, R., Chen, J., & Liu, Y. (2019). *Proactive protection of mobile operating system malware via blocking of infection vector*. Google Patents.

Ketaren, E. (2016). Cybercrime, cyber space, dan cyber law. *Jurnal Times*, *5*(2), 35–42.

Lestari, U., Hamzah, A., & Sholeh, M. (2022). Sosialisasi Fenomena Cyber Crime dan Penanggulangannya Bagi Pengelola Informasi Publik Kapanewon Mlati Sleman Yogyakarta. *NEAR: Jurnal Pengabdian Kepada Masyarakat*, *1*(2), 100–106.

Marzuki, P. M. (2021). *Penelitian Hukum* (15th ed.). Kencana.

Maskun. (2022). *Kejahatan Siber (Cyber Crime): Suatu Pengantar*. Prenada Media.

Miles, M. B., & Huberman, A. M. (1992). *Analisis data kualitatif*. Jakarta: UI press.

Minarosa, M. (2022). Legal Protection of Personal Data Owners as Cybercrime Victims Based on regulations regarding Electronic Information and Transactions. *Proceedings of the First Multidiscipline International Conference, MIC 2021, October 30 2021, Jakarta, Indonesia*.

Moleong, L. J. (2009). Penelitian kualitatif. *Jakarta: Rineka Cipta*.

Rusydi, I., Agustiana, Z., & Satria, W. (2020). Sosialisasi Dalam Mengantisipasi Kejahatan Internet di Era Internet of Think dan Revolusi Industri 4.0. *RESWARA: Jurnal Pengabdian Kepada Masyarakat*, *1*(2), 129–135.

Sastrawan, W. D. (2024). *Implementasi Undang-Undang ITE No 19 Tahun 2016 Terkait Penipuan Menggunakan Mobile Malware Pada Aplikasi Whatsapp Di Kabupaten Buleleng*. Universitas Pendidikan Ganesha.

Septiani, D., Widiyasono, N., & Mubarok, H. (2016). Investigasi Serangan Malware Njrat Pada PC. *J. Edukasi Dan Penelit. Inform. JEPIN*, *2*.

Sugeng, S. P. (2020). *Hukum Telematika Indonesia*. Prenada Media.

Sui, A.-F., & Guo, T. (2012). A behavior analysis based mobile malware defense system. *2012 6th International Conference on Signal Processing and Communication Systems*, 1–6.

Susanto, H., Sinaulan, R. L., & Ismed, M. (2022). Legal Certainty Regarding The Imposition Of Criminal Extortion Sanctions Involving Community Organizations (ORMAS). *Policy, Law, Notary And Regulatory Issues (POLRI)*, *1*(2), 37–54.

Vincent, N. A. (2017). Victims of cybercrime: Definitions and challenges. In *Cybercrime and its victims* (pp. 27–42). Routledge.

Copyrights