Damhil Law Journal

e-ISSN 2808-7143

Riri S. Modeong., Fenty U. Puluhulawa. 2025. "The Responsibility of Social Media Platform Providers in Protecting Users through Username Management" *Damhil Law Journal* 5 (1): 1-17

The Responsibility of Social Media Platform Providers in Protecting Users through Username Management

Riri S. Modeong

Faculty of Law Universitas Negeri Gorontalo. Indonesia. Correspondence E-mail: ririmodeong7@gmail.com

Fenty U. Puluhulawa

Faculty of Law Universitas Negeri Gorontalo. Indonesia. E-mail: fentypuluhulawa@ung.ac.id

Abstract:

This article examines the responsibility of social media platforms, like Facebook, in managing and safeguarding usernames, a key aspect of digital identity. With the rising global use of social media, misuse of usernames such as identity theft and account impersonation poses significant threats to user privacy and reputation. This study emphasizes the need for platforms to implement effective policies for username protection, in line with broader personal data protection efforts. It reviews regulations such as Indonesia's Personal Data Protection Law (UU PDP) and the European Union's General Data Protection Regulation (GDPR) to understand how platforms are legally required to protect user data, including usernames. Through a qualitative approach, including literature review, policy analysis, and interviews with data security experts, the research identifies existing gaps in protection and the challenges faced by platform providers. The findings reveal that while current policies and technologies are generally adequate, several vulnerabilities remain that can be exploited for identity abuse. The study proposes strategies to improve username protection, including stronger verification systems, advanced security technologies, and enhanced abuse reporting mechanisms. These recommendations aim to support ongoing discussions on data privacy and contribute to better safeguarding digital identities on social media platforms.

***Keywords**: Personal Data; Providers; Social Media; Security; Username*

How to cite **(Chicago Manual Style)**:
Modeong, Rini. S., and Fenty U. Puluhulawa. 2025. "The Responsibility of Social Media Platform Providers in Protecting Users through Username Management" *Damhil Law Journal* 5 (1): 1-17

Introduction

The rapid growth of social media in recent decades has transformed it into an integral part of daily life for millions globally. Platforms like Facebook, Twitter, Instagram, and TikTok offer spaces for communication, social interaction, entertainment, and business. Over 4.5 billion people worldwide are now using social media, and this number continues to grow every year. Facebook, as one of the largest platforms, boasts over 2.8 billion active monthly users. However, the vast number of users brings about significant security challenges, especially concerning the protection of personal data. Among these, the misuse of usernames which serve as the primary digital identity of users has become a major concern (Tandirerung and Mangesa 2023).

A username on a social media platform represents a user's digital identity, distinguishing one individual from another. It not only provides access to the platform but also functions as a key symbol of a user's online persona. Many times, usernames are linked to a person's personal and professional life, connecting them to friends, family, colleagues, and various services. Due to their importance, usernames become targets for misuse, including identity theft, fraud, cyberbullying, and defamation, with serious consequences for the affected individuals.

Social media companies, including Facebook, have a responsibility to protect users' personal information and digital identities. This responsibility is rooted in regulations across the globe that govern personal data protection and human rights in cyberspace. Various countries have enacted laws requiring digital companies to safeguard user data and prevent its misuse. A critical aspect of user protection is managing usernames. Inappropriate or harmful usernames, especially those impersonating others, can lead to potential damage to a user's reputation. Platform providers must address these risks to prevent harm (Rosyida, Kusumaningrum, and Anggraheni 2020).

In Indonesia, personal data protection is regulated under Law Number 27 of 2022 concerning Personal Data Protection (UU PDP). This law requires electronic system providers, including social media platform providers such as Facebook, to protect users' personal data from misuse. The law stipulates that the use of usernames that could harm other users or lead to identity misuse must be addressed by platform providers in a clear and effective manner. The UU PDP also outlines users' rights to access, correct, and delete their personal data from the systems managed by platform providers.

Meanwhile, at the international level, the General Data Protection Regulation (GDPR) in the European Union provides a strict legal framework for personal data protection, including data related to usernames. The GDPR requires online service providers to obtain explicit consent from users before collecting or processing their personal data and gives users the right to access, correct, and delete this data. One of the fundamental principles of the GDPR is "privacy by design," meaning that platform providers must integrate privacy and data protection measures from the product and service design stages (Permana 2025).

In addition, Facebook, as one of the largest social media platforms globally, is also subject to the California Consumer Privacy Act (CCPA) in the United States. The CCPA grants consumers in California the right to know what data is being collected about them, to delete their personal data, and to prevent companies from sharing personal data without explicit consent. With regulations like the CCPA, Facebook and other social media platforms are required to provide greater transparency and control to users regarding how their personal data, including usernames, is managed.

However, despite the presence of personal data protection regulations, many loopholes remain that can be exploited by irresponsible parties. One of these issues is identity impersonation, where individuals or groups can create accounts with usernames similar to or identical to someone else's real identity. This can cause confusion among other users or the public about who actually owns the account, potentially damaging the reputation and credibility of the original user. Such incidents often do not receive sufficient attention from social media platforms, which tend to focus more on feature development or increasing user numbers than on deeply protecting their users' identities.

On the other hand, Facebook, as a platform used by millions of people worldwide, should set a good example in terms of protecting user privacy and personal data. Various policies and features have been introduced by Facebook to help protect its users, such as privacy settings that allow users to choose who can view their profiles, as well as controls over who can send friend requests or messages. However, despite these features, the policy concerning username management has not fully prevented misuse. Usernames that are very similar or even identical to others often appear without any system in place to identify potential identity abuse (Parulian, Pratiwi, and Yustina 2021).

Furthermore, the presence of search algorithms on social media platforms like Facebook also significantly impacts username usage. For example, Facebook often suggests usernames based on users' previous searches or interests, making people more likely to choose an already existing name. In many cases, a person may not realize that the name they choose could potentially confuse or even harm others with similar names. This shows that despite technological advancements, protection against username misuse and the digital identities of users still requires further attention.

In addition to individual misuse, social media platforms also face issues regarding the enforcement of their internal policies. Many large tech companies have strict policies regarding violations of their rules, but their implementation is often not optimal. An example of this is in the management of usernames that violate platform rules, such as using fake names or impersonating others. Facebook has a policy that usernames must reflect a person's real name, but this policy is not always well-implemented in practice. Some users can easily bypass this policy by using variations of names or symbols to deceive the system's name recognition.

This problem is also related to the phenomenon of cyberbullying that is rampant in the virtual world. A username that is misused to impersonate someone can be used to carry out cyberbullying, which often leads to insults, harassment, or even threats against other users. This can cause significant harm to the victim, who may experience long-term psychological effects due to such actions. The security of username usage should be a priority for platform providers, as such behavior can damage relationships between users and tarnish the reputation of the individuals or organizations involved (Komalasari 2018).

Platform providers like Facebook must also consider the protection of the personal data contained within users' social media accounts. A username is essentially part of personal data because it often reflects an individual's identity in the online social context. Therefore, managing usernames is not just about aesthetics or ease of use but also about security and the protection of personal data. Security in this context includes monitoring to prevent username misuse, such as identity theft or fraud involving fake accounts that use similar names (Juledi et al. 2024).

Overall, while large companies like Facebook have implemented various policies to protect personal data and users' privacy, many challenges remain in managing usernames. The responsibility of platform providers to safeguard and protect usernames is not just about compliance with the law but also involves continuous efforts to raise awareness and protect users from various forms of identity misuse. In this regard, social media platform providers must collaborate with various parties, including regulators, security experts, and civil society organizations, to create a safer and more trustworthy online environment for all users.

Method

The research methodology used in this study is a qualitative approach (Ali 2021), employing literature review and policy analysis to understand the responsibility of social media platform providers, particularly Facebook, in protecting users with regard to the use of usernames. This study collects data from various primary and secondary sources, including regulations related to personal data protection, social media platform privacy policies, and previous research on digital identity security. The data is analyzed through policy analysis to evaluate the effectiveness of existing policies in preventing username misuse. Additionally, this study involves interviews with legal and cybersecurity experts to gain insights into the challenges faced by platform providers in safeguarding users' identities. The findings of this study are expected to provide policy recommendations to enhance user protection in the online world.

The Responsibility of Social Media Platform Providers in Managing Usernames (Username)

In today's digital era, almost every individual has an account on various social media platforms. Platforms like Facebook, Instagram, Twitter, and many others provide spaces for interaction, sharing information, communicating with friends, and even building identities and careers online. In this context, a username is an important element that identifies an individual in the digital world. A username represents a person's digital identity, making it crucial to keep it secure and prevent misuse.

However, as the number of social media users increases, various challenges related to managing and protecting digital identities arise. One of the main challenges is the risk of username misuse, which can lead to serious problems for the individuals involved, such as identity theft, account impersonation, and cyberbullying. This is where the role of social media platform providers becomes very important. Platforms like Facebook, used by over 2.8 billion people worldwide, bear a significant responsibility in managing and protecting the use of usernames to preserve the integrity of users' digital identities (Hidayat et al. 2023).

A username is one of the first elements created when someone registers on a social media platform. It serves as a unique address for each individual to access their account. However, a username not only functions as a login tool but also as a person's digital identity. Every time someone searches for an account or visits a user profile on social media, the username becomes the primary way to recognize them in the virtual world. Therefore, the username is often the first thing people see when interacting with an individual or organization on the platform.

Because of the large number of registered users, it is not uncommon for the desired username to already be taken by someone else, forcing users to choose variations of their original name. This is where issues can arise—usernames similar to someone else's identity can easily be used to impersonate or steal someone's identity. In some cases, this misuse of usernames can lead to the loss of credibility, damage to reputation, or even financial losses for the individuals or businesses involved (Hapsari and Pambayun 2023).

One of the greatest risks in managing usernames on social media is identity misuse. Social media platform providers are responsible for protecting their users from actions that could harm their digital identities. In many cases, username misuse occurs when someone intentionally creates an account with a name that closely resembles or even matches another user's username for fraudulent or bullying purposes.

For example, someone could create an account with a username very similar to that of a famous person or an ordinary user to deceive others, request personal information, or even commit financial fraud. In this scenario, the victim may feel confused and struggle to differentiate the legitimate account from the fraudulent one, which in turn could damage the reputation of the person whose identity was stolen. If someone experiences this, they may feel threatened, embarrassed, or even emotionally hurt. Therefore, platform providers like Facebook must have clear policies and effective mechanisms to prevent this harmful identity impersonation (Fikri et al. 2023).

Moreover, in an increasingly connected world, search algorithms on platforms like Facebook often influence how people choose their usernames. These algorithms may suggest names that are similar to existing usernames, and in some cases, this could lead to mistakes or misuse. For instance, someone searching for a specific username may not realize that the name is already taken by someone else, and as a result, they may choose a very similar name. In some cases, this could cause confusion or even conflict between users with similar names.

Social media platform providers, particularly those with millions to billions of active users, must implement effective policies to manage and protect usernames. One of their primary responsibilities is to ensure that no usernames can be misused to impersonate or harm others. Therefore, platform providers should have stringent verification systems in place during the registration and username management process (Dewanto et al. 2024).

Additionally, platform providers should develop systems capable of detecting and preventing fake accounts attempting to impersonate another user's username. One possible solution is to implement verification mechanisms, such as identity verification using legitimate personal data or even biometric technology, to ensure that the chosen username truly belongs to the legitimate user.

Platform providers must also consider using smarter algorithms in managing usernames. For example, search algorithms can be designed to alert users when they choose a name that is similar to an already existing username. This can reduce the likelihood of unintentional mistakes or misuse. Furthermore, platform providers should have policies in place to address reports of identity misuse quickly and efficiently. With an easily accessible reporting system, username misuse can be handled promptly, and appropriate action can be taken to protect users from further harm (Tomasoa 2024).

The ever-evolving technology can assist platform providers in better managing and protecting usernames. For example, artificial intelligence (AI) and machine learning can be used to detect suspicious patterns in username selection, such as the use of names that are very similar to the identities of famous people or other users. This technology can automatically identify potential problems before the account is published, thus preventing more significant misuse.

Additionally, blockchain technology could provide a more secure solution for managing digital identities. By using a blockchain-based system, users can have full control over their usernames and personal data. This technology can provide greater transparency regarding who has the rights to a username and prevent others from misusing or impersonating someone else's identity. Although blockchain technology is still under development for this application, its potential could significantly advance digital identity protection on social media (Sinaga et al. 2023).

Social media platform providers must establish clear policies related to the use of usernames. One important policy is to ensure that the username selected by each individual reflects their identity in a legitimate way. Platform providers must also provide mechanisms to help users resolve issues if their username is misused, such as offering a simple and secure account recovery process.

Additionally, platform providers must ensure that they comply with existing personal data protection regulations, such as the General Data Protection Regulation (GDPR) in the European Union and the Personal Data Protection Law (UU PDP) in Indonesia. These regulations require platforms to protect users' personal data and provide users with the right to access, modify, and delete their personal data, including usernames, when necessary. Platform providers must also ensure they have adequate systems in place to protect users' personal data from unauthorized access and misuse (Saputra and Marpaung 2023).

In an increasingly digital world, managing and protecting usernames on social media platforms is crucial to maintaining the integrity of users' digital identities. Platform providers like Facebook bear a significant responsibility to ensure that usernames are not misused by others to harm the individuals concerned. By implementing proper policies, using advanced technologies, and complying with data protection regulations, platform providers can help protect users from the risk of identity misuse and ensure the security and comfort of the online environment. Through these efforts, social media platforms can continue to grow into safe and trusted spaces for users worldwide.

Personal Data Protection and User Rights in Username Usage

In today's highly connected world, social media has become an inseparable part of our lives. Every day, billions of people around the world access platforms like Facebook, Instagram, Twitter, and others to interact, share information, and even conduct their professional lives. These platforms have one thing in common: to access them, we need a unique username, which becomes our identity in the digital world. This username is not just a tool to log into an account but also a symbol representing ourselves in the digital space. Therefore, it is crucial to keep this username safe and protected from misuse that could harm us as individuals (Maulana et al. 2023).

However, with the growing popularity of social media, significant issues related to usernames have emerged. The usernames used on social media platforms are often targeted for misuse, which can damage the reputation and personal lives of their users. One of the most common forms of misuse is identity theft, where someone creates an account with a username similar to or even identical to someone else's, and then uses it for malicious purposes. In some cases, this impersonation can cause significant damage, including financial loss, reputational harm, and even psychological effects for the victim.

As platforms used by millions, even billions of people, social media providers like Facebook, Instagram, and Twitter have a massive responsibility in managing and protecting the use of usernames. They not only have to ensure that the selected usernames are not misused, but also must provide overall protection for users' personal data. The protection of usernames is, in essence, part of personal data protection, which has become a major concern in the digital world today. Considering the importance of digital identity in modern life, the protection of usernames must not be overlooked (Gloria 2024).

A username is the primary identity we have in the digital world. When someone accesses our social media account, the username is the first thing they see, and it's what they use to recognize us. This name represents who we are in the digital space and is often linked to other personal information such as profile photos, contacts, and even location data or other personal details we voluntarily share on these platforms. Therefore, the username is not just an access tool but a crucial part of our digital identity that needs to be protected.

However, despite this, many people tend to choose usernames that are very similar to their real names, making them vulnerable to misuse. For example, someone might select a username based on their full name or simply use their first or last name. While this makes it easier for others to find and recognize them, this choice actually opens the door for misuse. A username that is too common or very similar to someone else's name can easily be exploited by others to impersonate someone's identity (Firly 2023).

Impersonation is a common problem on social media platforms. This occurs when someone creates an account with a username almost identical to another person's with the intent to deceive, commit fraud, or even damage the other person's reputation. This action can have severe consequences for the victim, both personally and professionally. For instance, if someone imitates the username of a famous person or influencer on social media, they may misuse that name to carry out fraudulent actions or tarnish the individual's reputation. This is a serious issue that must be addressed by platform providers.

Username misuse on social media can result in various harmful effects for the user. One of the biggest impacts is identity theft, which can cause serious damage to a person's personal or professional reputation. For example, someone who becomes a victim of impersonation on social media may feel they have lost control over their digital identity, which can impact their social relationships and career. In some cases, identity impersonation may be used to carry out fraud, such as asking for money or personal information from people who believe they are communicating with the legitimate person (Fahrezy, Hari, and Rosyidi 2024).

Additionally, misuse of usernames can also lead to cyberbullying. If someone creates a fake account with a username similar to another person's and uses that account to insult, spread hatred, or bully others, the consequences can be devastating. Victims of cyberbullying often feel isolated and powerless to protect themselves in the digital space. Without adequate protection, they become highly vulnerable to psychological impacts that can last for a long time. This is why it is important for social media platform providers to offer systems that not only allow users to report fake accounts or misuse but also take immediate action to protect the victims.

Username misuse can also lead to financial loss. Many cases of identity impersonation are carried out with the goal of gaining access to the victim's personal information, such as credit card data or bank account details. Fraudsters can use fake accounts to ask for money or personal information from the victim's friends, leading to theft of money or sensitive data. This is harmful, both materially and emotionally, as the victim feels betrayed and loses trust in the platform they once relied on (Fahmi et al. 2024).

Protecting usernames as part of personal data is a crucial aspect of safeguarding users' privacy on social media. Personal data, including usernames, is incredibly valuable to individuals and must be protected carefully. Therefore, the role of social media platform providers in safeguarding this personal data is essential.

In Indonesia, personal data protection is regulated under Law No. 27 of 2022 on Personal Data Protection (UU PDP). This law provides a strong legal foundation to protect personal data, including usernames, from misuse. UU PDP governs how personal data should be collected, processed, stored, and used by platform providers.

Service providers such as Facebook or Instagram are required to obtain explicit consent from users before collecting or processing their personal data, including usernames. Additionally, users are given the right to access, correct, and delete their personal data, including usernames, if necessary (Endah, Dimas, and Akmal 2017).

At the international level, the General Data Protection Regulation (GDPR) in the European Union also regulates personal data protection strictly. One of the main principles of GDPR is "privacy by design," which requires platform providers to incorporate personal data protection into the design and operations of their products. GDPR grants users control over their personal data, including the right to delete it (right to be forgotten). This means users can request platforms to delete their usernames if they feel their identity has been misused or if they no longer wish to use the platform. GDPR also requires platforms to notify users if their personal data has been breached or misused.

As platform providers with millions to billions of users, social media providers like Facebook and Instagram bear significant responsibility for protecting usernames and users' personal data. Platform providers must have clear policies regarding the management and protection of usernames and ensure that the usernames chosen by users are not misused by third parties (Banjarnahor et al. 2024).

Platform providers must be able to detect and prevent fake accounts attempting to impersonate another user's username. This can be done using security technologies such as two-factor authentication (2FA), which enables platforms to verify that only legitimate users have access to their accounts. Providers should also implement systems to report fake accounts or username misuse easily, allowing users to quickly report issues and receive the necessary assistance.

Additionally, platform providers must give users full control over their usernames. Users should be able to change or delete their usernames if they feel it has been misused or if they wish to change their digital identity. This process must be easily accessible and performed quickly, without complicated procedures or worsening the existing problem (Yel and Nasution 2022).

Technology plays a key role in protecting usernames and users' personal data on social media platforms. One technology that can be utilized is artificial intelligence (AI) and machine learning, which can help platforms detect suspicious patterns in username selection. These technologies can monitor accounts created with usernames that are similar or identical to other users' names and provide warnings if identity misuse is detected.

Moreover, blockchain technology could potentially provide a solution to this issue. With its high level of security, blockchain can ensure that the chosen username is legitimate and correctly registered, without any parties being able to misuse or impersonate that identity. This technology allows users to have full control over their digital identity, and platform providers can ensure that their personal data is not misused (Wulan et al. 2023).

Usernames on social media platforms are part of digital identity and must be taken seriously in terms of protection. Username misuse can negatively impact individuals in terms of reputation, privacy, and finances. Therefore, social media platform providers have a significant responsibility to ensure that usernames are well protected. Providers must implement clear policies, use advanced security technologies, and give users the right to manage and delete their usernames when necessary. With proper protection, both in terms of policies and technology, username misuse can be minimized, and users can feel safe while interacting in the digital world.

Conclusion

In the rapidly evolving digital world, the protection of usernames on social media platforms has become crucial for safeguarding users' digital identities and privacy. A username not only functions as a tool to access an account but also serves as a representation of one's identity in the virtual world, which is at risk of being misused, such as in cases of identity theft or impersonation. Social media platform providers, like Facebook, have a significant responsibility to ensure that the usernames selected are not misused by third parties, as well as to provide robust protection mechanisms for users' personal data. Through regulations such as the

Personal Data Protection Law (UU PDP) in Indonesia and the General Data Protection Regulation (GDPR) in the European Union, users are granted the rights to manage and delete their personal data, including usernames, when necessary. Technologies such as artificial intelligence and blockchain also hold potential to enhance security in username management by detecting misuse and ensuring transparency. Overall, effective protection of usernames and personal data is essential for creating a safe digital space, strengthening user trust, and reducing potential risks that could harm individuals in the online world.

Recommendation

As a step to enhance the protection of usernames and personal data on social media platforms, several suggestions can be implemented by platform providers. First, platform providers should tighten the identity verification process, such as by implementing two-factor authentication (2FA), to ensure that only legitimate users can access and manage their usernames. Second, the system for reporting username abuse should be improved to be more accessible and responsive, allowing users to immediately report fake accounts or identity impersonation. Third, user education is essential. Platform providers must provide clear guidelines on how to choose a secure username and raise awareness about the potential risks of identity misuse. Fourth, the use of technologies such as artificial intelligence (AI) and machine learning can help detect patterns of abuse and prevent identity impersonation before it occurs. Finally, there should be collaboration between platform providers and regulators to ensure compliance with existing personal data protection regulations, such as the PDP Law and GDPR, as well as to continuously update data security policies in line with technological advancements and emerging threats.

References

Ali, Zainuddin. 2021. *Metode Penelitian Hukum*. Sinar Grafika.

Banjarnahor, Daulat Nathanael, Firinta Togatorop, Doris Yolanda Saragih, Sepriandison Saragih, and Jan Sardo Pratama Purba. 2024. "Edukasi Tangkas Berinternet Dan Bijak Bersosial Media Bagi Anak Dan Remaja Sebagai Upaya Perlindungan Data Pribadi Untuk Pencegahan Kejahatan Siber." *Community Development Journal: Jurnal Pengabdian Masyarakat* 5 (4): 8221–27.

Dewanto, Muhammad Arif Bagus, Muhammad Fathurrahman, Danar Restu Firdaus, and Aep Setiawan. 2024. "Penipuan Penambah Followers Instagram: Analisis Serangan Phising Dan Dampaknya Pada Keamanan Data." *Journal of Internet and Software Engineering* 1 (4): 11–11.

Endah, Triastuti, Adrianto Dimas, and Nurul Akmal. 2017. *Kajian Dampak Penggunaan Media Sosial Bagi Anak Dan Remaja*. Vol. 1. 1. Puskakom UI. https://repository.unugha.ac.id/16/1/seribukuliterasidigital-kajiandampakmediasosialbagianakdanremaja-puskakomui-180201035158.pdf.

Fahmi, Rayhan Abdul Jabbar, Wahib Muhibi Nur, Dee Canawine, Muhammad Naufal Kusumajaya, Ahmad Faris Fadhlillah, and Nur Aini Rakhmawati. 2024. "Analisis Sentimen Masyarakat Terhadap UU Perlindungan Data Pribadi Pada Media Sosial Twitter Menggunakan Metode Support Vector Machine." *METHODIKA: Jurnal Teknik Informatika Dan Sistem Informasi* 10 (1): 6–10.

Fahrezy, Ilham Hashfy, Putra Siyang Hari, and Aunur Rosyidi. 2024. "Sosialisasi Keamanan Data Pribadi Dan Bijak Bersosial Media Di Karang Taruna Desa Karangkiring, Kecamatan Kebomas, Kabupaten Gresik." In *Prosiding Seminar Hasil Pengabdian Kepada Masyarakat Dan Kuliah Kerja Nyata*. Vol. 2. https://journal.umg.ac.id/index.php/prosidingkkn/article/view/8924.

Fikri, Adi Wibowo Noor, Achmad Fauzi, Aldi Alfathur Rachman, Anggita Khaerunisa, Dhea Puspita Sari, Puput Vernanda, Raudhatul Hikmah, and Tiara Putri Fadyanti. 2023. "Analisis Keamanan Sistem Operasi Dalam Menghadapi Ancaman Phishing Dalam Layanan Online Banking." *Jurnal Ilmu Multidisplin* 2 (1): 84–91.

Firly, Achmad. 2023. "Implementasi Clickjacking Dalam Serangan Tautan Palsu Untuk Eksplorasi Media Sosial." *Jurnal TIMES* 12 (2): 15–18.

Gloria, Velycia Debora. 2024. "Analisis Pembuktian Isu Pengambilalihan Akun Oleh Pihak Ketiga Aplikasi Zenly Melalui Pemberlakuan UU Perlindungan Data Pribadi." *SABER: Jurnal Teknik Informatika, Sains Dan Ilmu Komunikasi* 2 (4): 12–22.

Hapsari, Rian Dwi, and Kuncoro Galih Pambayun. 2023. "Ancaman Cybercrime Di Indonesia: Sebuah Tinjauan Pustaka Sistematis." *Jurnal Konstituen* 5 (1): 1–17.

Hidayat, Wahyu, Hartini Ramli, Pedang Mata Bulan Ikhram, Ahmad Radif Ridhawi, Nur Aisyah Mukhtar, and Renaldy Junedy. 2023. "Analisa Clustering Phising Untuk Meningkatkan Kesadaran Mahasiswa Terhadap Keamanan Data Pribadi Mahasiswa Universitas Negeri Makassar." *Vokatek: Jurnal Pengabdian Masyarakat*, 28–33.

Juledi, Angga Putra, Marnis Nasution, Syaiful Zuhri Harahap, Deci Irmayani, and Ibnu Rasyid Munthe. 2024. "Pelatihan Basic Cyber Security Untuk Keamanan Dan Perlindungan Data Pribadi Di Dunia Digital." *IKA BINA EN PABOLO: PENGABDIAN KEPADA MASYARAKAT* 4 (2): 57–65.

Komalasari, Rita. 2018. "Kesadaran Akan Keamanan Penggunaan Username Dan Password." *TEMATIK* 5 (2): 141–52.

Maulana, Ghifari Robby, Saskya Widya Aqila, Nur Hijriyah Sakinah, Nanda Ika Wulandari, and Citra Nurhayati. 2023. "Manfaat Manajemen Keamanan Informasi Terhadap Pengamanan Data Pribadi Mahasiswa Prodi Akuntansi Angkatan 2021 Fakultas Ekonomi Dan Bisnis Di Universitas Trunojoyo Madura." *Jurnal Ilmiah Rekayasa Dan Manajemen Sistem Informasi* 9 (2): 89–96.

Parulian, Sahat, Devi Anassafila Pratiwi, and Meiliya Cahya Yustina. 2021. "Studi Tentang Ancaman Dan Solusi Serangan Siber Di Indonesia." *Telecommunications, Networks, Electronics, and Computer Technologies (TELNECT)* 1 (2): 85–92.

Permana, Made Ody Gita. 2025. "Analisis Keamanan Platform E-Commerce Di Indonesia Terhadap Risiko Serangan Password Harvesting Fishing (Phishing) Dengan Metode Action Research Menggunakan Aplikasi Social Engineering Toolkit (Set)." PhD Thesis, UNIVERSITAS PENDIDIKAN GANESHA. https://repo.undiksha.ac.id/id/eprint/23157.

Rosyida, Hamdan Nafiatur, Demeiati Nur Kusumaningrum, and Palupi Anggraheni. 2020. "Mengajak Generasi Z SMA 1 Muhammadiyah Malang Berinternet Secara Bijak." *Aksiologiya: Jurnal Pengabdian Kepada Masyarakat* 4 (2): 199–212.

Saputra, Dewana, and Zaid Alfauza Marpaung. 2023. "Analisis Yuridis Penanggulangan Penyalahgunaan Data Pribadi Dalam Bentuk Phising Yang Dilakukan Oleh Paid Verified Account Di Media Sosial Menurut Undang-Undang Perlindungan Data Pribadi." *UNES Law Review* 5 (4): 4764–75.

Sinaga, Muliada Pardomuan, Erwin Ginting, Muhammad Rizal Nurdin, and M. Dimas Putra. 2023. "Analisis Ancaman Phising Terhadap Layanan Online Perbankan." *UNES Journal of Scientech Research* 8 (1): 041–047.

Tandirerung, Veronika Asri, and Riana T. Mangesa. 2023. "Pengenalan Cyber Security Bagi Siswa Sekolah Menengah Atas." *TEKNOVOKASI: Jurnal Pengabdian Masyarakat*, 89–94.

Tomasoa, Gelsy Olivia. 2024. "Perlindungan Hukum Terhadap Kebocoran Data Pribadi Pada Platform Media Sosial." *PAMALI: Pattimura Magister Law Review* 4 (1): 24–29.

Wulan, PIDC, Danis Putra Perdana, Rofiq Fauzi, and Rivort Pormes. 2023. "Edukasi Undang Undang Informasi Dan Transaksi Elektronik Serta Perlindungan Data Pribadi Dari Kejahatan Digital Di Desa Kirig Kudus." *KACANEGARA Jurnal Pengabdian Pada Masyarakat* 6 (2): 185–92.

Yel, Mesra Betty, and Mahyuddin KM Nasution. 2022. "Keamanan Informasi Data Pribadi Pada Media Sosial." *Jurnal Informatika Kaputama (JIK)* 6 (1): 92–101.