Department of Digital Business
Journal of Artificial Intelligence and Digital Business (RIGGS)
Homepage: https://journal.ilmudata.co.id/index.php/RIGGS
Vol. 4 No. 1 (2025) pp: 50-55
P-ISSN: 2963-9298, e-ISSN: 2963-914X

Data Security Analysis on the Use of E-Commerce to Prevent Online Fraud

Tri Yusnanto[1], Fatkhurrochman[2], Muhammad Abdul Muin[3], Khaoirul Mustofa[4]
[1]Manajemen Informatic, STMIK Bina Pstria Magelang
[2]Informatic Systems, STMIK Bina Patria Magelang
[3]Informatic Systems, Politeknik Negri Cilacap
[4]Informatic Systems, Universitas Duta Bangsa Surakarta

[1]yusnanto@stmikbinapatria.ac.id*, [2]Fatkhurrochman@stmikbinapatria.ac.id, [3]abdulmuain@pnc.ac.id,
[4]Khoirulmustofa@udb.ac.id

Abstract

As the purchasing and selling process has changed, so too has electronic fraud, which has led to several individuals losing money to online frauds. The goal of this study is to ascertain how trust affects the high rate of e-commerce fraud when executing transactions. Qualitative interpretative methodologies are used in this investigation. Research that looks at phenomena having meaningful patterns and relationships is known as phenomenological research. Field research indicates that a lack of understanding, ignorance, the temptation of phony gifts, high unemployment and poverty rates, and weak government security measures are the main causes of fraud in e-commerce transactions. about the various forms of fraud that occur in online transactions.

Keywords: Froud, E-Commerce, Fenomologi, Elektronik

1. Introduction

Fraud The development of technology and information is currently experiencing very rapid progress. The rapid further development of information technology has caused significant changes in various fields, including business, education, social, and societal aspects. It is used only in the use of information technology in all countries[1]. This technology and information can be accessed by anyone on the internet anywhere. The Internet is a global electronic network that uses satellite technology to connect computers around the world. At this point, the Internet has become an essential tool for the general public in many countries, including Indonesia.

In Indonesia, almost every social level is optimistic. Technological advancement can also be compared to a double-edged sword that can be used not only to facilitate all aspects of users' lives but also for negative purposes, which can ultimately endanger many people[2]. Regarding digital business (eCommerce), e-commerce has now become a social trend. Following the development of technology, there has been a significant shift towards e-commerce in traditional trade.

E-commerce benefits both sellers and buyers. Buyers do not need to spend a lot of time and money searching for the products they want. In addition to these advantages, there are drawbacks when processing through the internet. However, behind all the conveniences offered by e-commerce, there are concerns about the responsibility of e-commerce companies towards the personal data collected from customers[3]. Personal data includes email conversations, identity names, passwords, debit and credit card numbers, and information related to consumer requests[4]. More services and feedback in the form of reviews from purchases that can be used as rejections.

The security of safety systems is an aspect of, and all e-commerce companies, namely customer data, transaction information, and other digital assets, are invaluable parts and

vulnerable to cyber threats. These cyber threats include data theft, online fraud, and can be. This is caused by significant financial losses and harm to individuals, loss of consumer trust, as well as the legal impact of violations, loss up to data protection. There were 405,000 reports of online transaction fraud from 2017 to 2024, according to data collected by the Ministry of Communication and Information (Kemenkominfo). In 2023, 13.1% of fraud occurred in e-commerce.

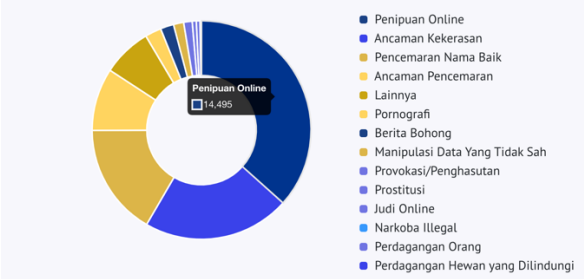

Figure 1: Online fraud case (patrolisiber.id).

This research aims to analyze the issues of Personal Data and E-Commerce Privacy from three main perspectives. First, this research examines e-Commerce users' understanding of data protection issues and how they comprehend threats to data security. Second, solutions and best practices have been identified in this research. This can be used by e-commerce providers to protect the privacy and personal data of their users. Third, this research evaluates guidelines and practices that can be used in the future to enhance the protection of e-commerce user data. [1]. The analysis of information system security in e-commerce companies in Indonesia is essential to understand potential risks and the measures that can be implemented to mitigate those risks. Identity theft such as Personal Data, SIM, Account Number, Verification Code, ID Card, and other information.

This is a real threat to the use of e-commerce. online scammers can cut users with their scams. Credit card numbers or bank account information are used to conduct illegal transactions. This can lead to significant economic losses for users. Therefore, it is important to analyze the security procedures implemented by E-Commerce application providers to protect user data and prevent online fraud. This article discusses various types of threats faced by e-commerce companies, strategies for data protection, and the importance of security awareness among employees and customers. A deeper understanding of this topic will enable companies to enhance their resistance to cyber risks and build better trust among stakeholders.

2. Research Methods

This research was conducted using the journal review method. The aim of this research is to gain a better understanding of the data security and privacy issues identified in the academic literature, as well as the solutions to these problems. This research will reach conclusions about the importance of data privacy in the digital era, the main issues faced, and practical and policy recommendations to enhance data protection. Starting with identifying security issues such as cyber attacks, data breaches, and the protection of users' personal data. Next, the collected data is analyzed using qualitative descriptive analysis.

This provides an in-depth overview of the information system security conditions. This analysis discusses various issues faced by e-commerce businesses, such as the lack of employee security awareness, insufficient security infrastructure, and the need for stricter

DOI: https://doi.org/10.31004/riggs.v4i1.371

regulations. To conclude, we can provide practical suggestions such as offering security training for employees, using the latest technology to protect data, and making privacy and security policies clearer for users. Therefore, this article not only discusses current issues but also offers solutions to enhance the security of information systems in Indonesia's e-commerce sector.

3. Results and Discussions

Any form of action or effort carried out by certain individuals or groups that can endanger the safety of other individuals or groups is defined as a hazard. Digital attacks or crimes that threaten the security, privacy, and integrity of users are a threat to the personal data security of users in e-commerce. The main threats to the e-commerce security system that are apparent will negatively impact both businesses and consumers. This threat fundamentally impacts the security of e-commerce users' personal data because the more numerous or dangerous these threats are, the more the security of e-commerce users' data is compromised.

This is due to the fact that e-commerce is a type of online trade where consumers provide personal information such as name, address, phone number, credit card number, and so on to make transactions[5]. E-commerce users can suffer financial losses and their identities can be stolen and misused by irresponsible parties if the information falls into the wrong hands. To protect their data in the future, e-commerce companies must implement policies and best practices. Companies must follow the Privacy by Design policy, which means considering privacy from the design stage of goods and services. Examples include data encryption, access restrictions, and information transparency. Building customer trust through reliable privacy protection practices is also very important for companies[6].

3.1. Data security: A set of rules or technological procedures used to prevent data from being accessed by unauthorized individuals, damaged, altered, or stolen. This includes various techniques and tools to ensure the integrity, confidentiality, and availability of data when stored, processed, or transmitted[7]. In addition, data security can prevent viruses or unauthorized access by computers attempting to steal personal data. Data theft is one of the criminal acts that causes the most victims. In practice, we can use various types of data security, such as authentication, encryption, data access control, confidentiality, etc.

3.2. Authentication is a procedure to ensure that someone is who they claim to be. Basically, this authentication method is a security measure that can usually accurately identify users before granting them permission to view relevant data.

3.3. Encryption is the process of transforming data or information into an unreadable, incomprehensible, or unprocessable form without a key or specific decoding techniques. Protecting the confidentiality and integrity of data is the primary goal of encoding. Only organizations with the necessary access and knowledge can access and understand the relevant data.

3.4. Data access control is a type of safeguarding activity that prevents any breaches into other digital networks. This aspect is related to data control. Therefore, this is often associated with personal and confidentiality issues. Therefore, user IDs and passwords or alternative methods are used to control the process. Confidentiality: This is a way to protect confidential information that is owned by individuals who do not have the right to access it. In most cases, this information can only be accessed by authorized groups or groups with authorization. This confidentiality applies to data provided to other organizations. This concept aims to maintain data confidentiality and prevent unauthorized hackers from accessing it.

DOI: https://doi.org/10.31004/riggs.v4i1.371

3.5. Factors that cause fraud in online transactions Cybercriminals usually claim to be representatives of official e-commerce platforms, and they will attempt to create fake prizes with special offers by requesting the victim's confidential data, and possibly even their money[6]. Cybercrime usually has specific strategies to deceive its victims. What causes fraud in online transactions?

a. User data leaks are usually caused by our users' mistakes. It is very important to remember that personal information such as identity cards, account numbers, verification codes, ID cards, and other personal information should not be shared. After confidential data is leaked, irresponsible individuals can exploit it for cybercrime. In addition, hackers and data breaches can also cause data damage. Those who understand technology but do not use it correctly are usually the group capable of executing this aspect. Additionally, hackers can exploit our information by using links or websites. Therefore, if we receive an unclear email or link, do not click on it. This is because the link or email may have been created by hackers to commit online fraud.

b. Lack of user knowledge: In general, the public needs to be educated about the risks associated with cybercrime through online transactions. Because we live in the current technological era, everyone must use technology[8]. Nevertheless, elderly people may not yet be able to use digital devices well. Therefore, citizens must be socialized and educated about the dangers of crime in digital transactions. The community will gradually begin to understand the patterns of fraud motives in online transactions through this group interaction.

c. The government's policies and security systems are weak, as evidenced by the data breach from the e-commerce application Tokopedia. This shows that Indonesia's security system is unreliable. Cybercriminals take advantage of the government's weakness in policy-making.[9]. However, Indonesia has established several regulations and policies to maintain the security of online transactions[10]. However, this specific experiment did not succeed; this can be explained by the high level of cybercrime in online transactions[11]. As the general public, we must report such cases to the authorities to reduce the amount of cybercrime in digital transactions.

d. The high levels of poverty and unemployment: People facing economic difficulties due to unemployment or poverty might do anything to earn money. This factor is what drives their early involvement in cybercrime activities as an effort to obtain money easily and simply[12]. This can make them do illegal things like fraud, identity theft, or hacking. Online transaction scammers can only operate with false promises. The government must be vigilant against fraud in online transactions in this regard. The increase in job opportunities and the reduction of poverty are in line with the decrease in online fraud.

Efforts to Maintain Customer Data Security: The goal of data security is to keep the business running and reduce the loss of business value by mitigating the impact of security incidents. Efforts to maintain customer data security are crucial to ensure that user data functions well and their data is secure, as shown in the table below.

Tabel 1. Upaya Menjaga Keamanan data Pelanggan

No	Security	Goal	Benefits
1	Autentikasi Multi-Faktor (MFA)	Asking users to verify their identity through two or more factors (for example, OTP and password) Replacing sensitive data (such as credit card numbers) with random tokens that have no intrinsic value Customer Identity Verification, Validating customer identity through official documents or	Reducing the risk of account hacking even if the password is leaked.

DOI: https://doi.org/10.31004/riggs.v4i1.371

		biometrics Implementing a strong password policy (minimum 8 characters, combination of letters, numbers, and symbols) Securing sensitive data (such as credit card numbers) using encryption algorithms like AES or RSA Providing guidance to users on how to keep their accounts secure (for example, not clicking on suspicious links).	
2	Tokenization	Asking users to verify their identity through two or more factors (for example, OTP and password)	Reducing the risk of users' financial data theft
3	Customer Identity Verification	Replacing sensitive data (such as credit card numbers) with random tokens that have no intrinsic value	Reducing the risk of brute-force attacks and account hacking
4	Monitoring User Activity	Customer Identity Verification, Validating customer identity through official documents or biometrics	Reducing the risk of brute-force attacks and account hacking
5	Data Encryption	Implementing a strong password policy (minimum 8 characters, combination of letters, numbers, and symbols) Securing sensitive data (such as credit card numbers)	Prevent unauthorized access to user data during transmission.
6	User Education	Providing guidance to users on how to keep their accounts secure (for example, not clicking on suspicious links).	Increasing user awareness of phishing and social engineering threats.

4. Conclusion

Shopping habits have shifted from retail shopping to more efficient and practical online shopping thanks to technological advancements. But hackers can also use this convenience to commit online fraud. Therefore, data security when conducting shopping transactions through e-commerce is an important issue in the rapidly evolving digital era. Research shows that e-commerce itself is equipped with security mechanisms such as data encryption, user authentication, and transaction validation. However, users remain at risk if they do not follow proper security measures, such as using secure devices, updating software, and being cautious of phishing scams. The measures taken to prevent e-commerce fraud include raising user awareness, implementing strict security policies, and collaborating with the government, service providers, and the community.

DOI: https://doi.org/10.31004/riggs.v4i1.371

Reference

[1] T. Yusnanto, K. Mustofa, M. A. Mahmudi, and S. Wahyudiono, "Fenomena Keamanan Informasi Pasca Era Revolusi Industri 5.0," vol. 17, no. 2, 2021.
[2] T. Yusnanto, M. A. Muin, and S. Waluyo, "Pelatihan Dasar Kemanan Digital Untuk Mengurangi Pencurian Data Yang Berdampak Pada UMKM".
[3] I. Kurnia and I. Martinelli, "permasalahan tansakasi pada e commerce," *JBMI*, vol. 4, no. 2, Sep. 2021, doi: 10.24912/jbmi.v4i2.11457.
[4] F. Tamzil and T. D. A. Ningrum, "TINGKAT KEAMANAN TEKNOLOGI E-COMMERCE DAN CASHLESS PADA PENGGUNA ANDROID (STUDI KASUS TEKNOLOGI INFORMASI PERUSAHAAN DAN E-BUSSINES)," vol. 19, 2022.
[5] M. H. Rustam, H. Hamler, T. Marlina, D. Handoko, and R. Alamsyah, "Peran dan tanggung jawab konsumen untuk mencegah praktik penipuan dalam transaksi online dari perspektif hukum perlindungan konsumen," *RLJ*, vol. 7, no. 1, p. 1, May 2023, doi: 10.30652/rlj.v7i1.8050.
[6] Chapple, M. and Seidl, D., *Cybersecurity operations handbook.* McGraw Hill Professional., 2019.
[7] R. D. Agustanti and A. N. Setiawan, "Tindak pidana penipuan pada transaksi e-commerce di masa pandemi covid-19," vol. 19, pp. 184–202, 2021.
[8] I. Hadi Ramadhan and E. Kumalasari Nurnawati, "ANALISIS ANCAMAN PHISHING DALAM LAYANAN E-COMMERCE," *SNAST*, pp. E31-41, Nov. 2022, doi: 10.34151/prosidingsnast.v8i1.4169.
[9] A. Muhammad, T. Marnasar, and .P Gomgom Siregar, "Akibat Hukum Bagi Pelaku Tindak Pidana Penipuan Online Melalui Modus Arisan Online Di Media Sosial Elektronik," vol. 4, no. 2, pp. 182-188., 2022.
[10] T. H. Sitabuana and D. Sanjaya, "Penyuluhan perlindungan hukum konsumen terhadap masyarakat pengguna layanan transaksi perdagangan elektronik (e-commerce)," vol. 5, no. 3, 2022.
[11] A. P. Aryani and L. E. Susanti, "Pentingnya Perlindungan Data Pribadi Konsumen dalam Transaksi Online pada Marketplace terhadap Kepuasan Konsumen," *Ahmad Dahlan Leg. Perspect.*, vol. 2, no. 1, pp. 20–29, Dec. 2022, doi: 10.12928/adlp.v2i1.5610.
[12] B. Surya and T. David, "Keamanan Data Pribadi Dalam Sistem Pembayaran E-Wallet Terhadap Ancaman Penipuan Dan Pengelabuan (Cyber Crime)," *Jurnal Fakultas Hukum,* p. Hal. 298-306., 2022.

DOI: https://doi.org/10.31004/riggs.v4i1.371