|Jurnal Ilmu Komputer dan Sistem Informasi |JIKSI|Vol. 5| No. 1|Feb|Year 2024|

Hacking Techniques in Data Theft: A Literature Study on Ethical Problems in Information Technology

Rahman Rulli Arjiansa[1*]

Abstract

The advancement of information technology (IT), particularly in computing and internet-based communication, has significantly influenced modern human life. However, rapid digital development has also increased vulnerabilities, especially in data security. One of the most prominent ethical issues in today's IT landscape is data theft, encompassing a wide range of cybercrimes such as hacking, spyware, and phishing. These attacks employ sophisticated techniques including pharming, spoofing, and identity fraud that lead to serious consequences such as financial loss, privacy invasion, reputational damage, and compromised national security. This study explores the phenomenon of data theft, identifies various hacking techniques used to obtain information illegally, and discusses the ethical dimensions of IT practices. Using a literature-based descriptive qualitative approach, this study reviews prior research to synthesize preventive ethical strategies in information management. The findings reveal that enhancing ethical awareness, strengthening data protection measures, and fostering collaboration among IT stakeholders are crucial to mitigating data-theft risks and maintaining integrity in digital ecosystems.

Keywords

Ethics; Data Theft; Information Technology; Hacking Techniques

Article History

Received 11 December 2023
Accepted 01 February 2024

How to Cite

Arjianssa, R.R, (2024). Hacking Techniques in Data Theft: A Literature Study on Ethical Problems in Information Technology, (JIKSI), 5(1), [15-20].

[1*] Universitas Bina Darma, Indonesia, Corresponding email: rahmanrullia@gmail.com

Introduction

The rapid proliferation of information technology (IT) has profoundly transformed how humans live, work, and interact. Digital innovation has become a central driver of modern civilization, influencing the way people communicate, conduct business, access education, and manage governance. The digitalization of everyday activities has produced unprecedented levels of connectivity and efficiency, enabling instantaneous information exchange and global collaboration. However, behind these advantages lies a paradox: the same technologies that empower individuals and institutions also create complex vulnerabilities that can be exploited for unethical or criminal purposes. The emergence of data theft, cyber fraud, and digital manipulation exemplifies how technological advancement, when detached from ethical control, can generate significant societal risks.

Data theft represents one of the most critical ethical and security challenges of the digital era. It refers to the unauthorized acquisition, duplication, or misuse of confidential digital information stored within computer systems, cloud networks, or databases. The targets of such crimes range from individuals—whose personal identities and financial accounts are compromised—to corporations and government institutions whose internal systems are breached for espionage or sabotage. The consequences of data theft are far-reaching, including financial losses, reputational damage, violations of individual privacy, and even threats to national security (Kaspersky, 2024). In the context of the modern information society, data has become a vital asset, often described as "the new oil," meaning that its theft or misuse can have an impact equivalent to the loss of tangible resources.

As information systems grow increasingly interconnected, malicious actors have become more sophisticated in exploiting vulnerabilities. Cybercriminals utilize various methods such as hacking, phishing, spyware infiltration, and identity theft to infiltrate digital systems. Each of these attacks not only undermines the integrity and confidentiality of information but also exposes weaknesses in human behavior and institutional governance. According to Fitroh and Sugiantoro (2023), these incidents highlight the growing ethical burden placed upon IT professionals, who must uphold principles of responsibility, accountability, and respect for users' rights in every aspect of system design and data management. Ethical negligence in securing information systems can therefore be seen not only as a technical failure but also as a moral lapse that erodes trust in digital ecosystems.

Beyond the technical implications, data theft poses profound ethical challenges related to privacy, autonomy, and justice. The unauthorized use of personal data violates fundamental human rights and undermines the moral foundation of trust in digital interaction. When individuals' private information is commodified or exploited without consent, it reduces human identity to a data object—stripped of dignity and agency. Furthermore, organizations that fail to implement adequate cybersecurity measures share ethical responsibility for enabling such violations. Negligence in protecting sensitive data reflects institutional disregard for user welfare, which contradicts the ethical principles of beneficence and non-maleficence that should guide professional conduct in technology management.

On a broader societal scale, the normalization of data theft and privacy violations reflects a concerning decline in ethical digital citizenship. Many users unknowingly participate in practices that compromise data integrity—such as sharing unverified links, neglecting cybersecurity hygiene, or disregarding privacy policies. This behavior, while seemingly trivial, contributes to a culture of digital irresponsibility that perpetuates systemic risk. The ethical dimension of data theft therefore extends beyond perpetrators and victims, encompassing a

collective moral duty to uphold integrity, vigilance, and respect for digital rights. Promoting digital ethics education, strengthening public awareness, and integrating moral reasoning into technology curricula are essential to fostering a more conscientious digital society.

Given these challenges, it becomes imperative to examine data theft not merely as a technical or legal issue but as a multidimensional problem encompassing ethical, social, and governance aspects. This study seeks to analyze the ethical implications of data theft within the context of information technology and to identify preventive strategies grounded in ethical awareness, organizational responsibility, and regulatory compliance. By understanding data theft through both moral and practical lenses, the research aims to contribute to the development of sustainable cybersecurity governance that aligns technological innovation with human values and social justice.

Methodology

This research adopts a descriptive qualitative method through a literature study approach, emphasizing conceptual exploration and theoretical synthesis to understand the ethical and security dimensions of data theft in the digital era. The descriptive qualitative method aims to provide an in-depth, systematic, and factual depiction of a phenomenon without manipulating variables. According to Dewanto (2015), descriptive research seeks to explain a situation as it naturally occurs, allowing the researcher to interpret meanings, relationships, and emerging patterns from existing information. This approach is suitable for examining topics involving ethical implications and cybersecurity governance, which require interpretive understanding rather than empirical measurement.

The literature study component involves the systematic collection, evaluation, and synthesis of data from various academic and institutional sources. Dewanto (2015) highlights that a literature-based approach enables researchers to integrate knowledge from existing theoretical and empirical studies to construct new insights. In this study, literature serves as both the primary data source and the analytical foundation for exploring concepts of data ethics, information security, and cybercrime prevention. By analyzing and synthesizing existing knowledge, the research aims to identify conceptual linkages and formulate recommendations that align ethical principles with technological practices.

The data sources for this research were drawn from a wide range of reputable references, including textbooks, peer-reviewed journal articles, conference proceedings, government policy documents, and verified online cybersecurity databases. Sources were selected based on their academic credibility, relevance, and recency to ensure the validity and reliability of findings. Special attention was given to materials discussing patterns of data theft, digital privacy, ethical frameworks in IT governance, and preventive cybersecurity measures. To maintain the study's rigor, only sources published by recognized institutions and indexed journals were included, while non-academic or unverified web content was excluded.

The analytical process was conducted in several structured stages. First, the researcher conducted a data identification and selection stage, in which relevant literature was compiled using keyword searches such as data theft, information ethics, cybersecurity, and digital governance. Second, the data classification stage organized the collected sources into thematic categories—ethical dimensions, types of data theft, legal frameworks, and prevention mechanisms. Third, during the data interpretation and synthesis stage, the researcher examined the interrelationship between ethical theory and practical cybersecurity issues to identify recurring patterns and conceptual gaps in previous studies. This process culminated in the

formulation of an integrated analytical framework highlighting both the ethical implications and strategic responses to data theft.

Through this qualitative-descriptive and literature-based methodology, the study aims to present a comprehensive understanding of data theft as a multifaceted issue that intersects technology, ethics, and governance. Rather than relying solely on statistical measurement, this approach emphasizes the contextual and normative interpretation of data theft phenomena within contemporary digital ecosystems. The combination of descriptive analysis and literature synthesis enables the research to produce a nuanced perspective that not only explains the phenomenon but also contributes to the ongoing discourse on ethical digital practices and cybersecurity policy development.

Results and Discussion

According to Kaspersky (2024), data theft is the unauthorized act of obtaining confidential information from digital systems, often exploiting system weaknesses or social-engineering tactics. Targets include personal identity data, corporate intellectual property, and financial records. Similarly, identity theft a subcategory of data theft involves the illegal use of another person's information to commit fraud or deception (USA.gov, 2024). IT service providers therefore have a moral and contractual duty to safeguard users' data and maintain trust.

Vacca (2012) classifies data-theft activities into several major categories:

1. Hacking: Unauthorized access to digital systems for stealing or altering data.
2. Identity Theft: Illegitimate acquisition of personal information to impersonate victims.
3. Carding: Misuse of stolen credit-card credentials for online transactions.
4. Spyware: Malicious software that monitors and records user activities covertly.
5. Cyber Extortion: Threatening to release or destroy stolen data unless ransom is paid.

Cybercriminals employ various methods to infiltrate systems, including:

1. Eavesdropping: Intercepting communications via telephone, email, or chat platforms.
2. Snooping: Unauthorized surveillance using keyloggers or monitoring tools.
3. Identity Spoofing: Falsifying IP addresses or device identities to bypass authentication.
4. Email Spoofing: Sending deceptive messages disguised as legitimate correspondence.
5. Phishing: Using fraudulent websites or messages to obtain sensitive information.
6. Pharming: Redirecting legitimate website traffic to fake domains.
7. Password-Based Attacks: Exploiting weak or repeated passwords using brute-force programs.
8. Denial-of-Service (DoS): Flooding servers to disable access for legitimate users.
9. Zero-Day Exploits: Leveraging unpatched software vulnerabilities before detection.

Discussion

Ethics represents the moral compass guiding human behavior in determining what is right and wrong. In IT, ethics governs the responsible use of data and technology. Fitroh and Sugiantoro (2023) emphasize that professionals must adhere to ethical standards that promote respect for privacy, intellectual property, and lawful access. Core ethical obligations include:

Ensuring technology serves legitimate and constructive purposes. Avoiding unauthorized system access or data manipulation. Protecting digital assets and respecting intellectual property. Preventing intentional system damage or disruption. Maintaining civility and professionalism in all online activities.

Importance of Ethics in Data Management

Ethical frameworks support secure and sustainable data practices by:

1. Protecting Privacy: Limiting unauthorized use and disclosure of personal data.
2. Serving Public Interest: Ensuring that data-driven innovation benefits society.
3. Fostering Trust: Building confidence among users and organizations.
4. Preventing Identity Fraud: Ensuring secure storage and access of personal information.
5. Complying with Law: Aligning with international data-protection regulations such as the GDPR.
6. Promoting Integrity: Upholding accountability and transparency in IT management.

Data theft has serious and far-reaching consequences for individuals, organizations, and even governments. One of the primary impacts is the loss of consumer trust and the damage to an organization's reputation, which may take years to rebuild. Financially, companies often face costly recovery efforts, legal proceedings, and regulatory fines. Moreover, the misuse of personal information can lead to identity fraud, illegal transactions, and violations of privacy rights. The exposure of sensitive medical or research data can further result in ethical breaches and exploitation.

Additionally, data theft can cause significant losses in intellectual property, thereby reducing an organization's competitiveness and innovation potential. Business operations and productivity may also be disrupted due to compromised systems or downtime during the recovery process. On a broader scale, such breaches pose risks to national and public security, especially when critical infrastructure or government information is involved. Therefore, understanding and addressing the consequences of data theft are essential to maintaining trust, stability, and resilience in today's digital environment.

Conclusion and Recommendations

Data theft remains one of the most critical challenges in modern information technology. Its prevention requires not only technological safeguards but also strong ethical foundations. Cyberattacks whether through phishing, spoofing, or zero-day exploits highlight the necessity for integrity, accountability, and proactive ethics in IT practice. Integrating ethics with information-security policies enhances user trust, protects privacy, and supports sustainable digital development. Continuous awareness, transparency, monitoring, and collaboration among stakeholders are indispensable to building a secure and ethical technological environment.

Disclosure Statement

The author declares no conflict of interest concerning the research, authorship, or publication of this article.

Acknowledgments

The author extends gratitude to Universitas Bina Darma (Bina Darma University), Palembang, for academic support and to scholars whose works contributed to the development of this research.

References

Abdullah, P. M. (2015). Quantitative Research Methodology.

Aswandi, R., Muchsin, P. R., & Sultan, M. (2020). Protection of personal data and information through the Indonesian Data Protection System (IDPS). Legislatif, 167–190.

Dewanto, F. (2015). The importance of ethics in corporate technology. Journal of Management Ethics, 5(3), 248–253.

Fitroh, Q. A., & Sugiantoro, B. (2023). The role of ethical hacking in combating cyber threats. Journal of Cybersecurity Studies, 3(2), 1–10.

Fuady, M. E. (2005). Cybercrime: Internet-Based Crimes in Indonesia. MediaTor, 6(2), 255–264.

Gunawan, I. (2021). Data Security: Theory and Implementation. Sukabumi: CV Jejak.

Kaspersky. (2024). What Is Data Theft and How to Prevent It. Retrieved from https://www.kaspersky.com/resource-center/threats/data-theft

Nissenbaum, H. (2010). Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press.

Raharjo, B. (2017). Information Security. Bandung: PT Insan Infonesia.

Rumlus, M. H., & Hartadi, H. (2020). Policy for addressing personal data theft in electronic media. Jurnal HAM, 285–299. Source Defense. (2024). What Is Data Theft? Retrieved from https://sourcedefense.com/glossary/what-is-data-theft

Biographical Notes

RAHMAN RULLI ARJIANSA is a postgraduate student at the Master of Information Technology Program, Universitas Bina Darma (Bina Darma University), Palembang, Indonesia. His research focuses on information ethics, cybersecurity, and data-privacy management, emphasizing ethical frameworks and preventive strategies to combat cybercrime and digital data theft.