JOURNAL OF INTERNATIONAL SCIENTIFIC RESEARCH
Volume 4, Issue 6, July- August 2026 Online ISSN: 3030-3508
https://spaceknowladge.com

PERSONAL DATA THEFT AND MISUSE THROUGH INTERNET NETWORKS IN THE ERA OF ADVANCED DIGITAL TECHNOLOGIES: A JAPAN-INFORMED SOCIO-TECHNICAL ANALYSIS

Toshmamatov Shakhzod Ermamat Ugli
Affiliation: Fergana State Technical University, Center for Digital Educational Technologies, Engineer-Programmer
Email: shahzodtoshmamatov042@gmail.com
Field: Information Security, Digital Society and Cyber Ethics

MAQOLA MALUMOTI

MAQOLA TARIXI:
Received:13.07.2026
Revised: 14.07.2026
Accepted:15.07.2026

KALIT SO'ZLAR:
personal data; cybersecurity; phishing; unauthorized login; data leakage; AI risk; privacy governance; Japan; digital trust

ANNOTATSIYA:

The development of cloud platforms, mobile services, artificial intelligence, online banking, digital learning systems and e-government has increased the social value of personal data. At the same time, internet networks have created new conditions for the theft, aggregation and misuse of such data. This article analyzes personal data theft not as an isolated technical incident, but as a networked socio-technical process that combines deception, credential abuse, vulnerability exploitation, weak organizational governance and secondary misuse. The study uses qualitative document analysis of public Japanese cybersecurity and privacy sources, including materials from the Information-technology Promotion Agency (IPA), the Personal Information Protection Commission (PPC), the National Institute of Information and Communications Technology (NICT), JPCERT/CC and the Council of Anti-Phishing Japan. Based on these sources, the article proposes a Networked Personal Data Misuse Cycle and a practical D-TRUST protection framework. The findings show that effective protection requires more than passwords or user warnings; it requires data minimization, technical hardening, resilient authentication, user-

centered education, supplier governance and transparent incident response.

1. Introduction

Modern society increasingly depends on internet networks for education, communication, finance, public administration, commerce, health services and research. Each digital interaction may generate, transmit or store personal data, including names, email addresses, phone numbers, identity documents, payment details, account credentials, location information, behavioral traces and device identifiers. These elements may appear harmless when viewed separately, yet they can become powerful tools of identification, profiling and manipulation when they are connected across platforms.

The theft and misuse of personal data is therefore one of the most important risks of the advanced digital age. It affects individuals, universities, public organizations, private companies and states. A single compromised account can expose academic records, financial files, private correspondence, cloud documents or administrative systems. Moreover, stolen data often remains useful long after the initial incident. An email address, phone number or scanned identity document can be reused for phishing, impersonation, account recovery fraud, social engineering or unauthorized access to other services.

This article argues that personal data theft should be understood as a lifecycle rather than a single event. In many incidents, attackers first manipulate trust through phishing or smishing, then capture credentials, access accounts, copy personal data, combine it with other leaked information and finally use it for financial, reputational or operational harm. Technical controls are necessary, but they are insufficient without privacy governance, user education, institutional responsibility and transparent response. Japan is a useful case for this discussion because Japanese organizations publish detailed public materials on cyber threats, phishing trends, privacy incidents and network-scale observation.

2. Methodology and Source Base

The study applies qualitative document analysis. The selected sources were public Japanese cybersecurity and privacy documents that describe recent threat trends, personal data leakage, phishing, unauthorized access, vulnerability exploitation and governance measures. The source base includes IPA's Information Security 10 Major Threats 2026, PPC materials on personal information protection and leakage reporting, NICTER observation reports on large-scale internet scanning, JPCERT/CC explanations of phishing, and monthly phishing reports from the Council of Anti-Phishing Japan.

The documents were analyzed for recurring themes and practical implications. Four categories were identified: deceptive collection, credential and identity abuse, infrastructure exploitation and governance response. These categories were then organized into a conceptual model called the Networked Personal Data Misuse Cycle. The article does not provide

offensive technical instructions. Its purpose is academic and preventive: to explain how personal data becomes vulnerable in internet environments and to propose measures that can reduce harm for institutions and users.

3. Personal Data as a Networked Asset

Personal data should not be limited to obvious identifiers such as a passport number or national identification number. In digital systems, identity is often reconstructed from fragments: an email address, a phone number, a username, a student number, a device fingerprint, a browser cookie, a delivery address or a transaction history. Even when one fragment is not sensitive by itself, its combination with other fragments may reveal a person's identity, habits, relationships, location, financial behavior or institutional role.

Internet networks increase the value and risk of personal data because accounts and services are interconnected. An email account is often the recovery channel for banking, cloud storage, social media, university portals and e-commerce. A compromised phone number may be used to reset accounts or receive malicious links. A leaked database from one service may allow attackers to test the same credentials on many other services. Thus, personal data becomes a networked asset: useful for legitimate services, but also attractive for attackers who exploit connectivity.

Japanese privacy and cybersecurity materials emphasize this interconnected nature of risk. PPC guidance focuses on safety control measures according to the nature, scale and volume of personal data handled by an organization. IPA's threat ranking shows that individual and organizational risks overlap: phishing, unauthorized login, ransomware, supply-chain attacks, vulnerability exploitation, information leakage and AI-related cyber risks all involve personal or confidential data.

4. The Networked Personal Data Misuse Cycle

Based on the source analysis, this article proposes the Networked Personal Data Misuse Cycle. The cycle contains seven stages. First, data exposure occurs when individuals share information through websites, applications, forms, cloud services or public profiles. Second, collection occurs through phishing, smishing, malware, compromised websites, breached databases, scraping or misconfigured services. Third, credential abuse follows when attackers use stolen passwords, session tokens, one-time codes or recovery information to access accounts. Fourth, data extraction occurs when files, messages, identity records or administrative databases are copied. Fifth, enrichment occurs when stolen information is combined with other sources. Sixth, exploitation occurs through fraud, impersonation, blackmail, spam, unauthorized purchases or institutional intrusion. Seventh, secondary harm continues when the same data is resold, reused or stored for future attacks.

This cycle explains why simply changing a password after an incident is often not enough. A password can be replaced, but a leaked phone number, email address, scanned document or personal profile may continue to circulate. The cycle also shows why organizations must protect both systems and processes. If an institution collects unnecessary data, stores it

without retention limits, gives excessive access rights or ignores supplier risks, it increases the damage that may occur after compromise.

5. Main Pathways of Theft and Misuse

Phishing and smishing remain among the most visible forms of personal data theft. JPCERT/CC describes phishing as a method in which attackers impersonate legitimate services and guide users to fake websites in order to steal credentials or personal information. Japanese anti-phishing reporting shows that this threat is large and persistent: recent monthly reports record high volumes of phishing submissions, unique phishing-site URLs and abused brands. The danger is not only the fake message itself, but the trust mechanism behind it. Attackers imitate banks, delivery companies, online shops, payment services, cloud platforms, universities or government portals because users already expect communication from these entities.

Unauthorized login is closely connected with phishing and credential reuse. Many users reuse the same or similar passwords across personal and institutional services. When one service leaks credentials, attackers may test them elsewhere. This is especially dangerous in universities and public institutions where the same email account may connect to learning systems, cloud storage, administrative panels and communication tools. Multi-factor authentication reduces risk, but weak or poorly implemented authentication can still be bypassed by social engineering, fake login pages or stolen session data.

A second pathway is technical exploitation. Not all data theft depends on deceiving the user. Attackers also search the internet for outdated software, exposed databases, weak remote access, vulnerable plugins, unsecured APIs and misconfigured cloud storage. NICTER reports demonstrate the continuous nature of network observation and scanning on the global internet. For organizations, this means that personal data protection is inseparable from system administration. A database is only as secure as the application, server, access control and backup environment around it.

A third pathway is organizational and supply-chain weakness. IPA ranks ransomware and attacks against supply chains or contractors among the leading organizational threats. These risks are directly linked to personal data because many institutions outsource email, payroll, cloud storage, payment processing, learning platforms or software maintenance. If a contractor is compromised, the primary organization may still suffer legal, financial and reputational consequences. PPC's annual reporting on personal data leakage illustrates that incidents are numerous and often involve both technical and human factors.

A fourth pathway is AI-enabled deception. Generative AI can improve legitimate security monitoring, but it can also make fraudulent messages more fluent, realistic and multilingual. Deepfake audio, synthetic profiles, automated phishing texts and AI-assisted social engineering may reduce the visible errors that once helped users detect suspicious messages. IPA's inclusion of AI-related cyber risks in its 2026 organizational threat list reflects this emerging concern.

6. Consequences for Individuals and Institutions

The misuse of personal data produces several forms of harm. Financial harm may include unauthorized purchases, fraudulent transfers, payment card abuse or fake loan applications. Reputational harm may occur when stolen accounts are used to send malicious messages, spread false information or impersonate trusted people. Institutional harm may include service disruption, loss of research data, exposure of student records, regulatory investigation and loss of public trust.

Psychological harm is also important. Victims may experience fear, shame and uncertainty because stolen data cannot easily be recovered. A leaked phone number or email address may cause repeated scam messages for years. A stolen identity document may be used in future attempts to bypass verification. For this reason, personal data protection is not only an IT issue; it is also an ethical obligation. Institutions that collect data for education, administration or services have a responsibility to limit collection, control access and respond honestly when incidents occur.

7. D-TRUST Protection Framework

To interrupt the misuse cycle, this article proposes a six-layer framework called D-TRUST: Data minimization, Technical hardening, Resilient authentication, User-centered education, Supplier governance and Transparent response. These layers combine privacy principles with cybersecurity practice. They are designed for universities, public organizations and small or medium institutions that may not have large security budgets but still process sensitive personal data.

Table 1. D-TRUST framework for reducing personal data theft and misuse

Layer	Meaning	Practical focus
D	Data minimization	Collect only necessary data; define retention periods; delete outdated records.
T	Technical hardening	Patch systems, secure configurations, monitor logs, protect backups and segment networks.
R	Resilient authentication	Use strong MFA or passkeys; reduce password reuse; apply least privilege.
U	User-centered education	Teach realistic scenarios and make suspicious-message reporting simple.
S	Supplier governance	Control outsourced systems, contracts, subcontractors and breach notification duties.
T	Transparent response	Prepare incident roles, notification steps, evidence preservation and public communication.

8. Recommendations for Universities and Public Organizations

First, institutions should create and maintain a personal data inventory. They should know which systems contain student, employee, applicant, alumni, research participant and

financial data. Without such an inventory, it is impossible to apply retention limits, access control or incident response correctly.

Second, every public-facing system should have a responsible owner. The owner should ensure patching, backup testing, access review, log monitoring and reporting. Many breaches occur not because systems are unknown, but because responsibility for them is unclear. Third, organizations should strengthen authentication for administrators, finance staff, teachers and users with access to large datasets. Passkeys, phishing-resistant multi-factor authentication and least-privilege access should be preferred where possible.

Fourth, cybersecurity education should be practical and repeated. Users should see realistic examples such as fake scholarship messages, delivery notifications, cloud document links, online payment warnings and university login pages. Training should not blame victims; it should make reporting easy and fast. Fifth, supplier contracts should include security and privacy obligations, including breach notification, access control, subcontractor management and data deletion after service completion.

Finally, institutions should prepare incident response before a crisis. The plan should identify who receives reports, who disables accounts, who communicates with affected people, who contacts regulators or law enforcement, and who approves public statements. Transparent response protects not only legal compliance but also trust.

9. Discussion

The main contribution of this article is the shift from a single-incident view of personal data theft to a lifecycle view. A phishing email, an exposed database or a stolen password is only one part of a longer process. Defense must therefore be layered. User education can reduce deception, but it cannot fix unpatched servers. Technical hardening can reduce exploitation, but it cannot prevent excessive data collection. Privacy policies can explain rights, but they cannot protect information without implementation.

Japanese public reporting also demonstrates the value of visibility. IPA, PPC, NICT, JPCERT/CC and the Council of Anti-Phishing Japan provide data and guidance that help organizations understand risk. Similar transparency is important in other countries and institutions. When incidents are hidden or treated only as technical failures, society loses the opportunity to learn from them.

10. Limitations and Future Research

This study has several limitations. It relies on public documents and therefore does not measure the hidden number of unreported incidents, private organizational failures or victim experiences that never reach public statistics. It also uses Japan as an evidence-informed case rather than as a complete representation of all countries. Nevertheless, the Japanese source base is valuable because it combines national threat rankings, privacy authority reporting, phishing monitoring and internet-scale observation.

Future research should compare Japan-informed findings with data from Central Asia, Europe and other regions. Empirical studies in universities would be especially useful:

surveys of password reuse, phishing reporting behavior, data retention practices and incident response readiness could test how the D-TRUST framework works in practice. Such research would help transform personal data protection from a general recommendation into a measurable institutional standard.

11. Conclusion

Personal data theft through internet networks is one of the defining security and privacy challenges of the digital era. It is driven by the combination of human trust, technical vulnerability, credential reuse, automated scanning, cloud dependence, outsourced services and increasingly realistic AI-enabled deception. Japanese cybersecurity and privacy sources show that phishing, unauthorized login, ransomware, supply-chain compromise, vulnerability exploitation and leakage reporting must be considered together.

The Networked Personal Data Misuse Cycle explains how personal data moves from ordinary digital use to long-term harm. The D-TRUST framework offers a practical response based on data minimization, technical hardening, resilient authentication, user-centered education, supplier governance and transparent response. For universities and public organizations, the central lesson is clear: protecting personal data is not only the duty of IT staff. It requires leadership, legal awareness, procurement discipline, secure system administration, user support and ethical responsibility. In this sense, cybersecurity is a foundation of digital trust.

References

[1] Information-technology Promotion Agency, Japan (IPA). (2026). Information Security 10 Major Threats 2026.
https://www.ipa.go.jp/security/10threats/10threats2026.html

[2] Personal Information Protection Commission, Japan (PPC). (2025). FY2024 Annual Report.
https://www.ppc.go.jp/aboutus/report/annual_report_2024/

[3] National Institute of Information and Communications Technology (NICT). (2026). NICTER Observation Report 2025.
https://www.nicter.jp/en/report

[4] JPCERT Coordination Center (JPCERT/CC). (2024). Phishing FAQ.
https://www.jpcert.or.jp/ir/faq3.html

[5] Council of Anti-Phishing Japan. (2026). 2026/04 Phishing Report.
https://www.antiphishing.jp/report/monthly/202604.html

[6] Personal Information Protection Commission, Japan (PPC). Guidelines on the Act on the Protection of Personal Information: General Rules.
https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/

[7] Miyamoto, D. (2020). Cybersecurity Education. KANRIN: Bulletin of the Japan Society of Naval Architects and Ocean Engineers, 91, 36-43.
https://doi.org/10.14856/kanrin.91.0_36
[8] Japan Law Translation. Act on the Protection of Personal Information.
https://www.japaneselawtranslation.go.jp/en/laws/view/4241/en

