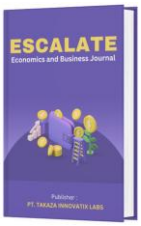
Escalate: Economics and Business Journal
https://journal.takaza.id/index.php/escalate

Vol. 01, No. 02, 2023, pp. 109-117
E-ISSN: 3025-4213

E-mail: escalate@takaza.id



Password Security & User Access: Is Human Negligence the Weakest Point in Accounting Information Systems

Ahmad Arif Aufar[1], Widanti Retno Palupi[2], Rina Tjandrakirana DP[3]
[123]Sriwijaya University
Corresponding Author e-mail: a.arifaufar121@gmail.com

Article History:
Received: 27-12-2023
Revised: 25-02-2024
Accepted: 26-02-2024

Keywords: *Accounting Information Systems, Cybersecurity, Human Negligence, Password Management, SLR.*

Abstract: *Currently in the digital era, Accounting Information Systems play an important role in managing confidential financial data. This study evaluates whether human negligence is the main vulnerability in Accounting Information Systems compared to technical factors. Using the Systematic Literature Review method of several reputable national & international journals, it was found that human factors contribute up to 85% to data leaks. Major problems include poor password management, security fatigue, vulnerability to phishing, and internal access abuse. The results of the study confirm that advanced technologies such as encryption are often paralyzed due to user negligence. In conclusion, strengthening SIA security requires a holistic approach that integrates technical solutions such as Role-Based Access Control & Multi-Factor Authentication with cyber awareness training to mitigate the risk of user behavior as the system's weakest point.*

How to Cite: Ahmad Arif Aufar, Widanti Retno Palupi, Rina Tjandrakirana DP. (2023). *Password Security & User Access: Is Human Negligence the Weakest Point in Accounting Information Systems. 01*(02). pp.109-117 https://doi.org/10.61536/escalate.v1i2.458

https://doi.org/10.61536/escalate.v1i2.458

Introduction

Digital changes in accounting have changed the way financial data is managed through Accounting Information Systems (SIA), which allows for direct access, more efficient processes, and data-driven decision-making (Lehenchuk et al., 2022)(Nurwanah, 2024). However, these developments also increase cybersecurity risks, especially due to the threat of serious financial data leaks. Internationally, reports show that more than 85% of data breach cases are caused by human factors (Yeng et al.,2022). In Indonesia, in 2023 there was a banking data hacking incident involving hundreds of millions of data records, causing

financial losses of trillions of rupiah and causing major concerns throughout the country regarding the security of the financial system (Muchtar et al., 2024). These statistics show that investments in advanced technology are often unable to prevent events due to user error, such as staying in the business (Basha, 2025)(Triplett, 2022).

Although there have been many studies that have discussed technical matters related to SIA security, such as data encryption & firewalls (Nyarko-Boateng et al., 2024)(Sanusi et al., 2025), there are still many gaps in more thorough research. This study wants to look thoroughly with the Systematic Literature Review (SLR) method, especially about how user behavior among accounting staff. Most research focuses more on technical solutions without deeply analyzing how human negligence, such as improper use of internal access or poor password management, becomes a major weak point in the system (Abuiteiwi & Santiago Escobar, 2025). This gap becomes even more important, especially in the context of organizations such as universities or companies in Indonesia, because the lack of cyber awareness training actually exacerbates vulnerabilities (Morić et al., 2025).

This research is important because accounting data is highly sensitive & confidential in nature, including financial information such as financial statements, transactions, & personal data of employees. If a violation occurs, this can lead to financial losses, legal penalties, and loss of trust from the parties involved (Sayuthi, 2021). In this case, SLR research is needed to find patterns of human error and ways to prevent them, in order to help create more comprehensive security policies. Issues examined include The most common types of human error in SIA use, such as saving default passwords or forgetting to update software (Basha, 2025)(Krause et al., 2025), How poor password management affects the security of accounting data, including the risk of phishing fraud & unauthorized access (Gemawaty & Yuliani, 2024)(Triplett, 2022), Effective non-technical mitigation strategies according to previous research are such as role-based awareness training & access management (Abuiteiwi & Escobar, 2025)(Morić et al., 2025).

Research Methods

This study uses the Systematic Literature Review to analyze neatly and comprehensively various references that discuss password security & user access methods in Accounting Information Systems, focusing on human negligence as the main weakness that often occurs. The SLR approach was chosen because it allows for the combination of empirical evidence from various sources in a clear, repeatable, and unbiased manner, thus providing a deeper understanding of user behavior patterns and their impact on the integrity of financial data (Abuiteiwi & Escobar, 2025)(Triplett, 2022).

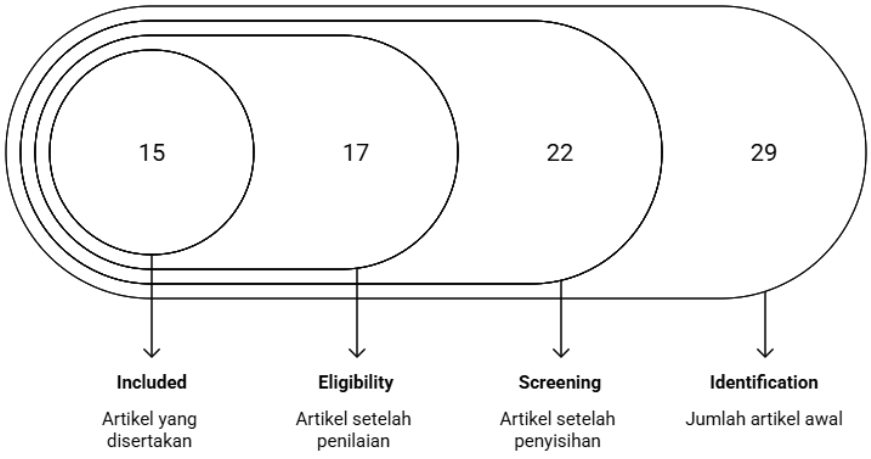
This study uses the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) protocol as a reference in compiling reports, so that the results are more complete, clear, and of high quality. The protocol uses the PRISMA flowchart to illustrate each stage of article selection, thereby increasing openness & reducing the likelihood of bias in selection.

https://doi.org/10.61536/escalate.v1i2.458

The strategy to search for data is carried out using several well-known academic databases, such as Google Scholar, Scopus, ScienceDirect, & Garuda (which are specifically used for the Indonesian context), in order to gain a relevant perspective on the local situation. The keywords used include "Accounting Information System Security", "Human Error in Accounting", and "Insider Threat in AIS".

The criteria for inclusion of articles include journals, conference proceedings, or theses published in the last 5-year period (2021–2026) to ensure findings are up-to-date, clearly address human factors such as negligence, password usage behavior, or insider threats within the SIA, and are available in English or Indonesian with a full-text version. The criteria for exclusion apply to articles that only discuss purely technical solutions such as encryption algorithms or firewalls without addressing aspects of user behavior, articles that are abstract only without full text, literature that has not been peer-reviewed verified, and articles that are duplicates or outside the specified year range.

The article selection process is carried out by following four stages from PRISMA in a row. The Identification stage is the initial search process within a database that generates article records based on the keywords used. The screening process is done by checking the headlines & abstracts to eliminate clearly inappropriate or repetitive articles. The Eligibility Stage consists of checking articles that have passed the screening stage, with the aim of ensuring that the article meets the entry criteria or does not enter strictly. The next stage is finally determining which articles are actually included in the process of synthesis & qualitative analysis. The entire process is recorded in a PRISMA flowchart to be clearly documented and accountable.



https://doi.org/10.61536/escalate.v1i2.458

Result and Discussion

The Dominance of Human Negligence & the Phenomenon of Security Fatigue

From a search of 26 relevant articles, one pattern appeared repeatedly. The most fragile point is not in the technology, but in the people who use it. The figure of 85% of data leaks triggered by human factors is disturbing and reasonable at the same time.Yeng et al. (2022) Indicates that most international data breaches originate from user actions, not from algorithm failures. In Indonesia, Muchtar et al. (2024) Reviewing the case of a major banking hack in 2023 that caused losses of trillions of rupiah. The system is modern, the infrastructure is expensive, but one procedural error opens access that should be closed. In that context, the argument Basha, A. M. (2025) & Triplett, W. J. (2022) It feels strong. They see user behavior and awareness as a much more decisive variable than just firewall strength or software sophistication.

The theoretical explanation can be drawn to Human Factor Theory. Triplett, W. J. (2022) together Abuiteiwi, A., & Santiago Escobar, . (2025) affirms that human error, whether due to negligence or ill will, is often the main cause of the collapse of the security system. It feels trivial. Use the system's default default password. Share credentials via instant messaging because colleagues are in a hurry. Or clicking on an email that looks like an official bank notification when it's phishing. Morić et al. (2025) A reminder that a single click can cripple the technical defenses built over years. In SIA practice, Krause et al. (2025) & Sayuthi (2021) Note that accounting staff have extensive access to transaction & payroll data, so minor misconfigurations or omissions to change passwords can lead to large-scale leaks. It is difficult to deny that the hypothesis about humans as the main vulnerability does have a strong empirical basis.

The problem doesn't stop there. There is a psychological dimension that is often missed, namely security fatigue. Krause et al.(2025) describing it as mental exhaustion due to repetitive security procedures. Imagine having to enter the MFA code every time you log in, changing your password every month with more complicated combinations, and having to complete your financial statements before five o'clock in the afternoon. In such conditions, the desire to find shortcuts feels very human. Basha, A. M. (2025) & Nurwanah, A. (2024) Finding the tendency of users to disable protection features or use the same password across platforms for work efficiency. Sanusi et al.(2025) It even noted that the pressure of accounting work makes staff sometimes delay system updates or forget to record crucial trail audits.

Finally, the problem is not just whether the technology is sophisticated enough. Sanusi et al. (2025) & Nurwanah, A. (2024) shows that without more humane behavior management and policy design, even the most advanced SIA systems remain at high risk. So maybe the

https://doi.org/10.61536/escalate.v1i2.458

question needs to be shifted. It's no longer just how strong the encryption is installed, but how realistic the system is designed for the humans who use it every day.

Password Management Vulnerabilities & Phishing Threats

Many security incidents in Accounting Information Systems actually start from trivial things. Password. Not a super-sophisticated attack, not a movie-style hack. Just a combination of letters & numbers that is too easy to guess, or stored in small notes pasted near the monitor. The literature shows a recurring pattern. Staff use the default password because they find it bothersome to change it. Some store credentials in Excel files without protection. System updates are delayed for fear of disrupting work. Krause et al. (2025) Note that in a fast-paced accounting environment full of deadlines, efficiency often takes precedence over prudence. Even though that's where the gap opens. One account with a weak password can give access to cash statements, vendor data, and even employee payroll.

The problem doesn't stop at loose password management. The gap is often magnified through phishing that is more subtle and convincing. Emails that look exactly like bank notifications. The message that seems to come from the boss asks for account verification immediately due to the sudden audit. In busy situations, people tend to react quickly without checking small details like the sender's address. Gemawaty, C. A., & Yuliani, Y. (2024) together Triplett, W. J. (2022) Pointing out that weak password management makes this kind of attack much more effective. Once credentials are granted, even expensive technical defenses can be penetrated. Morić et al. (2025) adding that the lack of cyber awareness training makes many employees not really understand how social engineering works. They feel that they have been careful, even though the attacker's tactics continue to evolve.

When these two factors meet, weak passwords and persuasive phishing, the impact can be systemic. Unauthorized access allows manipulation of transaction data, changes in report numbers, or removal of audit trails. Within the framework of the CIA Triad, the aspects of confidentiality, integrity, & availability are directly threatened. Sayuthi (2021) explains that even small distortions in accounting data can result in wrong strategic decisions. Investors can misread performance. Management took the wrong step. Not to mention the risk of legal sanctions & the decline of the company's reputation in the eyes of the public. Once trust is lost, restoring it is not an easy matter.

Internal Access Risk & Role-Based Control Urgency (RBAC)

Often we focus too much on the shadow of anonymous hackers out there, even though threats to the Accounting Information System can also arise from within the office itself. It's not always because of malicious intent, sometimes it's just because access is too loose. A staff member who actually only needs to look at the daily cash report can also open payroll data or

https://doi.org/10.61536/escalate.v1i2.458

download the complete list of vendors. Situations like this create a dangerous space of ashes. Abuiteiwi, A., & Santiago Escobar,. (2025) Remind that insider threats are among the most destructive risks precisely because the perpetrators have legitimate access & trust to the organization. There is no need to break into the system, just take advantage of the rights that have been given.

Less disciplined management of access permits magnifies this risk. Sanusi et al. (2025) note that in many cases, access rights are rarely re-evaluated when an employee moves divisions or promotions. As a result, one can accumulate privileges from various positions that have been held. The principle of secrecy is slowly eroding. Sensitive financial data, such as accounts payable details or bank reconciliations, can be accessed by parties who are no longer actually interested. It feels trivial, but that's where the potential for manipulation or leakage comes in.

At this point, Role Based Access Control to be relevant. The concept of least privilege sounds simple, only provide access according to the needs of the task. However, the implementation is often inconsistent. Maulany et al. (2025) emphasizing that the integration of accounting information technology needs to be accompanied by clear restrictions on activities based on roles. This means that the transaction recording staff cannot automatically approve the payment, and the financial manager does not need to access the technical system configuration. Faridawati et al. (2024) Demonstrating that implementing proper access controls not only improves security, but also makes workflows more efficient as responsibilities become more structured. When access rights are set automatically & standardized, the room for bias or manual omission can be suppressed.

Even so, restricting access alone is not enough. Credentials can still be stolen or misused. This is where Multi Factor Authentication comes into play. Khoiriah et al. (2025) explains that multi-layered verification, such as a combination of password & OTP codes, significantly lowers the risk of account takeover. Even if the password is leaked, there is an additional layer that prevents unauthorized access. On the other hand, a consistent trail audit is no less crucial. Sayuthi (2021) confirms that any changes in data & transactions need to be recorded in a log that cannot be manipulated. With a clear activity track, organizations can track anomalies faster and determine who is doing what, when, and from where.

Ultimately, SIA's security is not just about advanced technology, but about discipline in regulating who can see and do what. The combination of RBAC, MFA, & audit trails forms a complementary oversight framework. Without it, internal threats will always be a latent risk that is difficult to control, even when external defenses look very strong.

Conclusion and Recommendation

Penelitian ini menemukan bahwa kelalaian manusia merupakan titik lemah utama dalam keamanan Sistem Informasi Akuntansi (SIA), dengan kontribusi hingga 85% terhadap kebocoran data akibat pengelolaan password yang buruk, kelelahan keamanan, kerentanan

https://doi.org/10.61536/escalate.v1i2.458

phishing, dan penyalahgunaan akses internal. Temuan dari tinjauan literatur sistematis menegaskan bahwa meskipun teknologi canggih seperti enkripsi sering kali gagal karena perilaku pengguna, strategi mitigasi seperti Role-Based Access Control (RBAC), Multi-Factor Authentication (MFA), dan pelatihan kesadaran siber dapat secara signifikan mengurangi risiko ini. Implikasi praktisnya mencakup kebutuhan organisasi untuk mengadopsi pendekatan holistik yang mengintegrasikan solusi teknis dengan budaya keamanan yang kuat, sehingga melindungi data keuangan sensitif dari kerugian finansial dan hukum.

Meskipun demikian, keterbatasan penelitian ini terletak pada fokus utamanya pada literatur periode 2021-2026 yang mungkin belum mencakup kasus empiris terbaru atau konteks industri spesifik di luar akuntansi, serta ketergantungan pada data sekunder tanpa analisis kuantitatif primer. Untuk penelitian selanjutnya, disarankan melakukan studi kasus longitudinal atau survei terhadap staf akuntansi di Indonesia guna mengukur efektivitas intervensi pelatihan, serta mengeksplorasi integrasi kecerdasan buatan dalam mendeteksi pola kelalaian manusia. Pendekatan ini akan memperkaya pemahaman tentang dinamika manusia-teknologi dalam SIA secara lebih komprehensif.

References

Abuiteiwi, A., & Santiago, E. (2025). Evaluating the human factor in cybersecurity threats (a Systematic Literature Review). SSRN. https://ssrn.com/abstract=5576064

Arliana, S. A., & Fatrizia, S. (2023). SLR: SPI & accounting fraud against data security in SIA in the age of big data. Journal of Accounting and Financial Research, 11(2), 45–58. https://doi.org/10.17509/jrak.v11i2.56781

Basha, A. M. (2025). Human factors in IoT security: Addressing user behavior and awareness. International Journal of Creative Research Thoughts (IJCRT), 13(7), 112–125. www.ijcrt.org

Daeli, I. S., Ramadhan, S., Nur, K., Laila, L., & Jaya, D. (2026). Cybersecurity strategies for accounting data protection: A systematic literature review 2021-2025. Land Journal, 7(1), 88–102. https://ejurnal.ulbi.ac.id/index.php/jurnalland

Dani, M. R., Simatupang, E. M., Anakampun, A., Pratiwi, Y., Natalia, D., Perangin-angin, R., & Darma, J. (2025). The role of accounting information systems in identifying and preventing fraud in the abuse of internal access of companies. Journal of Economics and Accounting Publications (JUPEA), 5(2), 145–158. https://doi.org/10.55606/jupea.v5i2.3876

Faridawati, S. A., Herdi, H., & Lamawitak, P. L. (2024). Analysis of the application of accounting information systems to improve the efficiency and financial security of MSMEs (Cafe Rindu Lokaria). Journal of Economics, Accounting, and Taxation, 1(4), 189–215. https://doi.org/10.61132/jeap.v1i4.443

Gemawaty, C. A., & Yuliani, Y. (2024). Identity & access management in information systems security (literature review approach). Journal of Informatics Management Jayakarta, 4(4), 396–403. https://doi.org/10.52362/jmijayakarta.v4i4.1527

Kafi, A., & Akter, N. (2023). Policy and practice reviews securing financial information in the digital realm: Case studies in cybersecurity for accounting data protection.

Global Journal of Accounting and Economy Research, 4(1), 15–29.

Khoiriah, S., Salsabila, A., Camberra, D. D., Syafri, E., Layyin, H. L., Fathurrahman, R., & Marjohan, M. (2025). Security & privacy in digital finance. Journal of Information Systems and Business Management Publications, 4(2), 409–418. https://doi.org/10.55606/jupsim.v4i2.4524

Krause, A., Suray, J., Schmüser, L., Oltrogge, M., Wiese, O., Golla, M., & Fahl, S. (2025). An in-depth systematic analysis of the security, usability, and automation capabilities of password update processes on top-ranked websites. arXiv. http://arxiv.org/abs/2511.10111

Lailiyah, N., & Supranata, M. (2025). The role of accounting information systems in improving security through data encryption. Journal of Managerial Accounting (JAM), 10(1), 48–62. http://journal.uta45jakarta.ac.id/index.php/JAM/index

Lehenchuk, S. F., Vygivska, I. M., & Hryhorevska, O. O. (2022). Protection of accounting information in the conditions of cyber security. Problems of Theory and Methodology of Accounting, Control and Analysis, 2(52), 40–46. https://doi.org/10.26642/pbo-2022-2(52)-40-46

Mahmood, S., Chadhar, M., & Firmin, S. (2024). Addressing cybersecurity challenges in times of crisis: Extending the sociotechnical systems perspective. Applied Sciences (Switzerland), 14(24), 11610. https://doi.org/10.3390/app142411610

Makidong, S., & Putra, I. F. U. R. (2025). Web-based accounting information system for recording & financial management at the GPIBK Synod Office. Journal of Information Systems and Business Management Publications (JUPSIM), 4(3), 226–238. https://doi.org/10.55606/jupsim.v4i3.53573

Maulany, S. C., Meikhati, E., & Prastiwi, P. I. (2025). Integration of accounting information technology & accounting information system protection against cybersecurity accounting in the digital era. Tax Accounting and Digital Economy Policy, 2(3), 216–231. https://doi.org/10.61132/apke.v2i3.1429

Morić, Z., Dakić, V., Plećaš, M., & Biškupić, I. O. (2025). Evaluating end-user defensive approaches against phishing using education and simulated attacks in a Croatian university. Journal of Cybersecurity and Privacy, 5(3), 450–468. https://doi.org/10.3390/JCP5030038

Morshed, A., & Khrais, L. T. (2025). Cybersecurity in digital accounting systems: Challenges and solutions in the Arab Gulf region. Journal of Risk and Financial Management, 18(1), 41. https://doi.org/10.3390/jrfm18010041

Muchtar, A. M., Sari, R. V., & Santoso, S. H. (2024). Securing accounting information systems (AIS). KnE Social Sciences, 9(25), 112–126. https://doi.org/10.18502/kss.v9i25.16952

Nurwanah, A. (2024). Cybersecurity in accounting information systems: Challenges and solutions. Advances in Applied Accounting Research, 2(3), 157–168. https://doi.org/10.60079/aaar.v2i3.336

Nyarko-Boateng, O., Nti, I. K., Mensah, A. A., & Gyamfi, E. K. (2024). Controlling user access with scripting to mitigate cyber-attacks. Journal of Computer and Communications, 12(4), 101–115. https://doi.org/10.4236/jcc.2024.124008

Sanusi, I., Sanusi, A. R., Shamwill, A. K., Yinusa, S., & Iliyasu, R. (2025). Evaluation of cloud based computing in security accounting information system. World Journal of Advanced Research and Reviews, 25(3), 1073–1086. https://doi.org/10.30574/wjarr.2025.25.3.0734

Sayuthi. (2021). The concept of internal control for information system security. Scientific African, 17, e02355. https://doi.org/10.1016/j.sciaf.2024.e02355

Simanjuntak, H. E., Purba, H. C., Ginting, J. T. B., Aruan, P. A., Panjaitan, R. J. N., & Darma, J. (2025). Security of accounting information systems in the digital age: Concept & implementation. Indo-MathEdu Intellectuals Journal, 6(2), 2695–2705. https://doi.org/10.54373/imeij.v6i2.2950

Simatangkir, D. W. E., Afifah, E. F. N., & Nafiza, S. F. (2025). Cybersecurity in banking as well as challenges & solutions in the digital era. Journal of Management Informatics and Accounting (JMIA), 2(1), 33–42. https://doi.org/10.61722/jmia.v2i1.3119

Triplett, W. J. (2022). Addressing human factors in cybersecurity leadership. Journal of Cybersecurity and Privacy, 2(3), 573–586. https://doi.org/10.3390/jcp2030029

Yeng, P. K., Fauzi, M. A., & Yang, B. (2022). A comprehensive assessment of human factors in cyber security compliance toward enhancing the security practice of healthcare staff in paperless hospitals. Information (Switzerland), 13(7), 335. https://doi.org/10.3390/info13070335