Diversitas Journal
ISSN 2525-5215
Volume 11, Number Special 1 (Mar./Apr. 2026) p. 0281 – 0295
https://diversitasjournal.com.br/diversitas_journal

User Experience: A Heuristic Approach to Evaluating IT Security Technologies

LUCILA, Noli Jr. B.[1]

[1] 0000-0003-3213-0347; Bicol University. Legazpi City, Philippines. nlucila@bicol-u.edu.ph

A B S T R A C T

As organizations increasingly depend on IT security solutions to safeguard sensitive data and critical infrastructure, usability has become as vital as technical robustness. Complex or poorly designed systems risk undermining security by discouraging proper use or prompting workarounds. This study examines user-centric security by assessing the usability of IT security technologies through Jakob Nielsen's heuristic evaluation framework. Drawing from usability engineering principles and human-computer interaction, the study investigates how end-users perceive and interact with security systems, focusing on key dimensions such as visibility of system status, match between system and the real world, and error prevention. The research was conducted among 201 personnel at Bicol University, Legazpi City, Philippines, employing a cross-sectional survey guided by Nielsen's heuristics. Results show that the average usability score across the evaluated technologies was 3.80 on a five-point scale, indicating a generally favorable perception of usability. Respondents highlighted strengths in areas such as system visibility and recognition rather than recall, suggesting that these tools reduced cognitive effort in performing security-related tasks. However, moderate ratings for flexibility, efficiency, and error recovery point to usability gaps that could limit effectiveness and user confidence. Furthermore, the results highlight the necessity of incorporating usability factors into IT security solutions' design, implementation, and training. This approach can improve user compliance, reduce errors, and strengthen organizational security.

RESUMO

À medida que as organizações dependem cada vez mais de soluções de segurança de TI para proteger dados sensíveis e infraestrutura crítica, a usabilidade tornou-se tão vital quanto a robustez técnica. Sistemas complexos ou mal projetados podem comprometer a segurança, desencorajando o uso adequado ou incentivando soluções alternativas. Este estudo examina a segurança centrada no usuário, avaliando a usabilidade de tecnologias de segurança de TI por meio da estrutura de avaliação heurística de Jakob Nielsen. Baseando-se em princípios de engenharia de usabilidade e interação humano-computador, o estudo investiga como os usuários finais percebem e interagem com os sistemas de segurança, com foco em dimensões-chave como visibilidade do status do sistema, correspondência entre o sistema e o mundo real e prevenção de erros. A pesquisa foi conduzida com 201 funcionários da Universidade de Bicol, em Legazpi City, Filipinas, utilizando um levantamento transversal guiado pela heurística de Nielsen. Os resultados mostram que a pontuação média de usabilidade entre as tecnologias avaliadas foi de 3,80 em uma escala de cinco pontos, indicando uma percepção geralmente favorável da usabilidade. Os respondentes destacaram pontos fortes em áreas como visibilidade e reconhecimento do sistema, em vez de memorização, sugerindo que essas ferramentas reduziram o esforço cognitivo na execução de tarefas relacionadas à segurança. Contudo, as classificações moderadas para flexibilidade, eficiência e recuperação de erros apontam para lacunas de usabilidade que podem limitar a eficácia e a confiança do usuário. Além disso, os resultados destacam a necessidade de incorporar fatores de usabilidade no projeto, implementação e treinamento de soluções de segurança de TI. Essa abordagem pode melhorar a adesão do usuário, reduzir erros e fortalecer a segurança organizacional.

ARTICLE INFORMATION

Article process:
Submitted: 11/29/2025
Approved: 04/06/2026
Published: 04/14/2026

Keywords:
usability heuristics, information security technologies, human factors, cybersecurity usability, Jakob Nielsen's heuristics

Palavras Chaves:
heurísticas de usabilidade, tecnologias de segurança da informação, fatores humanos, usabilidade em cibersegurança, heurísticas de Jakob Nielsen

DOI: 10.48017/dj.v11i2.3775

Introduction

Information security has emerged as a critical concern for organizations in the modern digital environment. The rapid expansion of digital technologies has broadened the threat landscape, introducing new challenges in protecting institutional information assets. The widespread use of cloud services, mobile technologies, and online collaboration platforms has enhanced organizational efficiency while simultaneously increasing exposure to cyber threats. Organizations increasingly face risks such as ransomware, phishing attacks, and social engineering schemes, which continue to evolve in sophistication and scale. Global estimates indicate that the annual cost of cybercrime is expected to reach USD 10.5 trillion by 2025, highlighting the magnitude of the cybersecurity challenge (Morgan, 2020). Educational institutions remain among the most targeted sectors due to their reliance on digital platforms and the large volumes of sensitive data they maintain (IBM, 2025).

These concerns are particularly relevant in developing countries such as the Philippines, where higher education institutions are undergoing rapid digital transformation. Universities increasingly rely on digital systems for academic management, financial transactions, research administration, and online learning services. While these developments improve efficiency and accessibility, they also introduce new vulnerabilities that require effective and sustainable information security practices. Bicol University exemplifies this dependence on digital infrastructure, managing large volumes of institutional and personal data that must be protected against unauthorized access and misuse.

Information security is increasingly recognized as a socio-technical issue that involves not only technological safeguards but also human behavior and system usability. Traditional security approaches have emphasized technical solutions such as firewalls, encryption mechanisms, and intrusion detection systems. However, research has consistently shown that human behavior plays a crucial role in determining the effectiveness of these controls (Triplett, 2022). Security failures often arise not from technical weaknesses but from user errors, misunderstandings, or non-compliance with established procedures. This perspective has led to growing interest in human-centered approaches that consider users as active participants in maintaining organizational security.

Human Factors in Information Security

Human factors represent one of the most significant determinants of information security effectiveness. In fact, security incidents frequently result from unintentional mistakes, inadequate knowledge, or unsafe practices rather than from technical failures alone. Lee and Hwang (2021) emphasize that both internal and external actors contribute to security risks, with employee behavior representing a substantial proportion of incidents. Similarly, Khando et al. (2021) argue that improper handling of digital resources creates persistent vulnerabilities

within organizations. Financial losses associated with security breaches have also been linked to inadequate user awareness and accountability (Farahbod et al., 2020).

Despite being frequently described as the “weakest link” in information security, users also serve as the first line of defense. Center for Internet Security (2026) suggests that well-trained and supported users can significantly strengthen organizational security. Bush and Mashatan (2025) similarly highlight the importance of user competence and attentiveness in maintaining secure systems. These findings suggest that improving information security requires not only technical controls but also systems that support effective and error-resistant user interaction.

Information Security in Higher Education

Usability and Information Security

An essential dimension of human-centered security is usability. Jakob Nielsen defines usability as the extent to which users can effectively and efficiently interact with digital systems. Nielsen’s Ten Usability Heuristics provide a widely recognized framework for evaluating interface quality and user interaction (Nielsen, 1994). The framework emphasizes principles such as visibility of system status, consistency, error prevention, and user control, all of which influence how users interact with software systems.

Usability plays a particularly important role in information security because users may avoid or circumvent systems that are difficult to understand or operate. Complex or poorly designed security technologies can lead users to adopt unsafe practices, thereby weakening organizational protection. Confusing interfaces may result in errors such as improper configuration settings, weak password management, or failure to recognize security warnings. In contrast, usable systems support correct behavior by making secure practices easier to follow.

Improved usability can also enhance organizational productivity. Systems that provide clear instructions and intuitive navigation reduce cognitive effort and improve task efficiency. Usability evaluation therefore provides practical insights into both interface design and user training requirements. Identifying usability barriers allows institutions to refine system interfaces and improve support mechanisms to better align with user capabilities.

Research Gap and Contribution

Despite increasing recognition of the human dimension in cybersecurity, empirical research on the usability of IT security technologies in higher education remains limited. Existing studies have largely focused on technical effectiveness or user awareness programs, while fewer investigations have examined how users interact with security technologies in their

daily work. As a result, institutions may implement technically robust security systems that are not fully utilized or properly applied by end-users.

Although usability frameworks such as Nielsen's heuristics are widely used in human-computer interaction research, their systematic application to institutional information security technologies remains relatively limited. This gap is particularly significant in higher education environments, where users possess varying levels of technical expertise and interact with security systems in diverse contexts.

This study contributes empirical evidence by applying Jakob Nielsen's usability heuristics (Nielsen, 1994) to evaluate end-user interactions with IT security technologies in a university setting. By examining usability as a determinant of effective security practices, the study strengthens socio-technical perspectives on information security and provides practical insights for improving user-centered cybersecurity in higher education.

Research Objectives

The primary objective of this study is to evaluate the usability of IT security technologies used by university personnel using Jakob Nielsen's usability heuristics as an analytical framework. The study examines how users interact with institutional security control systems and identifies usability strengths and limitations that may influence effective security practices.

Specifically, the study aims to:

1. Assess the usability of institutional IT security technologies across the ten dimensions of Nielsen's usability heuristics.
2. Identify usability strengths and weaknesses in the interaction between university personnel and security control systems.
3. Examine how usability characteristics may influence the effective use of information security technologies in a higher education environment.

By focusing on the usability dimension of information security technologies, the study emphasizes the role of user experience in supporting secure behavior and effective system use.

Significance of the Study

This study addresses the identified gaps by doing a heuristic-based usability assessment of IT security solutions at Bicol University, utilizing Jakob Nielsen's methodology as guidance. Its importance is rooted in three interconnected contributions. This expands Nielsen's heuristics into information security, enhancing socio-technical viewpoints by demonstrating how usability directly influences the efficacy of security methods in higher education.

The results provide practical insights for university leaders and IT administrators in selecting, designing, and improving security measures. Enhancing usability mitigates risks, fosters user compliance, and fosters a culture of shared accountability within the institution.

The research emphasizes the necessity of incorporating usability into cybersecurity strategies at the institutional and national levels. Institutions such as CHED, DICT, and other regulatory bodies can benefit from this study by developing policies and frameworks that promote sustainable information security practices in academia.

The report argues that a paradigm shift is required to achieve effective cybersecurity in academic institutions from viewing end-users as liabilities to recognizing them as essential collaborators in digital security. Institutions can improve protection, reduce vulnerabilities, and encourage their members to actively contribute to preserving valuable digital assets by guaranteeing that IT security solutions are user-centric and resilient.

Methodology

Research Design

This study employed a cross-sectional survey design to evaluate the usability of institutional IT security technologies from the perspective of university personnel. The design was appropriate because it allowed the collection of data on users' perceptions and experiences with security control systems at a single point in time. The approach enabled the study to describe current usability conditions and identify areas for improvement in institutional information security practices. The study focused specifically on the usability dimension of information security technologies rather than on technical security performance. The evaluation examined how users perceive and interact with security control systems installed on institutional computers.

Research Setting and Participants

The study was conducted at Bicol University in Legazpi City, Philippines, a public higher education institution that relies extensively on digital systems for academic and administrative operations. The target population consisted of university personnel, including faculty members, administrative staff, and support personnel who regularly use institutional information systems.

A minimum sample size was calculated using a 95% confidence level and a ±5% margin of error, resulting in a required sample of 201 respondents, which was considered adequate for statistical analysis and representation of the university personnel population. Participants were selected using convenience sampling, allowing the researcher to obtain responses from personnel who were available and willing to participate. This sampling approach was considered appropriate due to practical constraints such as time, accessibility, and the need to include respondents from multiple campuses and offices. The final sample included personnel from academic departments, administrative offices, and service units, ensuring representation of users with varying levels of experience with IT security technologies.

Participation in the study was voluntary. Respondents were informed about the purpose of the study before completing the survey. No personally identifiable information was collected, and results were reported in aggregated form to ensure anonymity and confidentiality.

Research Object

In this study, the term security control systems refers to the end-user-facing information security applications installed on university personnel computers. These include institutional endpoint protection software, antivirus platforms, firewall interface modules, authentication systems, and related security management applications used in daily operations. Rather than evaluating a single proprietary product, the study examined users' interaction experiences with the security control systems deployed within the university's IT infrastructure. The evaluation focused on the usability characteristics of these systems' interfaces as perceived by end-users. The study did not assess backend security architecture or technical performance but instead examined how users understand and interact with the visible components of institutional security applications. This definition clarifies that the research object is usability rather than technical security performance.

Research Instrument

Data were collected using a structured questionnaire based on Jakob Nielsen's Ten Usability Heuristics, which served as the theoretical framework for evaluating user interaction with IT security technologies. Each heuristic dimension was operationalized into multiple Likert-scale statements representing usability characteristics such as system visibility, consistency, error prevention, user control, and help documentation.

Participants rated each statement using a five-point Likert scale, where: 1 = Strongly Disagree, 2 = Disagree, 3 = Moderately Agree, 4 = Agree, and 5 = Strongly Agree. The questionnaire was designed to measure respondents' perceptions of usability across the ten heuristic dimensions.

Instrument Validation and Reliability

To establish content validity, the questionnaire was reviewed by two faculty experts in information security and human-computer interaction. The reviewers evaluated the clarity, relevance, and alignment of the items with Nielsen's usability principles. Revisions were made to improve wording clarity and ensure accurate representation of usability constructs.

A pilot test was conducted with approximately 20 university personnel who were not included in the final sample. The pilot test evaluated item clarity, questionnaire flow, and response time. Minor revisions were implemented based on participant feedback, particularly in simplifying technical terminology and improving instructions.

In addition, internal consistency reliability was assessed using Cronbach's alpha coefficient. The instrument obtained a reliability coefficient of $\alpha = 0.939$, indicating excellent internal consistency. According to commonly accepted standards ($\alpha \geq 0.70$), the questionnaire demonstrates sufficient reliability for research purposes. This result confirms that the items consistently measure perceived usability across heuristic dimensions.

Data Collection Procedure

Data were collected over one academic semester using an online questionnaire administered through Google Forms. Participants were invited to participate through institutional email communication and on-campus distribution. Before completing the questionnaire, participants were provided with information describing the purpose of the study, voluntary participation, and confidentiality assurances. Respondents completed the survey independently at their convenience.

Data Analysis

Quantitative data were analyzed using descriptive statistical techniques. Mean scores were computed to summarize respondents' perceptions across the ten usability heuristic dimensions. Frequency distributions were examined alongside mean scores to provide additional insight into response patterns and variability. Mean values were interpreted using the following scale: 1.00–1.80 = Very Low, 1.81–2.60 = Low, 2.61–3.40 = Moderate, 3.41–4.20 = High, and 4.21–5.00 = Very High. Higher mean scores indicate more positive usability evaluations, while lower scores indicate potential usability concerns. The descriptive approach allowed direct interpretation of usability strengths and limitations based on Nielsen's heuristic framework.

Results and Discussion

This section presents the results of the heuristic-based usability evaluation of IT security technologies used by university personnel. The analysis was guided by Jakob Nielsen's Ten Usability Heuristics in order to examine how users interact with institutional security control systems and to identify usability strengths and limitations.

Table 1 presents the mean scores for the ten usability heuristic dimensions. The results indicate that the evaluated IT security technologies obtained an overall mean usability score of 3.80, corresponding to a high level of usability according to the interpretation scale. This suggests that the security control systems are generally usable and acceptable to end-users, although several dimensions show room for improvement.

Table 1.

Usability Evaluation Based on Nielsen's Heuristics

HEURISTIC	DESCRIPTION	MEAN SCORE	INTERPRETATION
Visibility of System Status	The system/app always keeps the users informed. It provides clear and concise feedback about what is happening and displays relevant information that helps users understand their actions and the system's processes.	3.90	High
Match between System and the Real World	The system/app speaks the users' language using words, phrases, and concepts familiar to the user, rather than internal jargon. This helps users feel comfortable and confident using the system, making learning how to use it easier.	3.84	High
User Control and Freedom	The system/app clearly marked "emergency exit" to leave the unwanted action without going through an extended process and without getting stuck and frustrated.	3.68	High
Consistency and Standards	The system/app is designed consistently and follows established conventions, guidelines, and standards. This helps users learn how to use the system more quickly and easily, reducing the risk of errors.	3.88	High
Error Prevention	The system/app helps users avoid mistakes by implementing intuitive error-handling mechanisms. Error messages are clear and concise, and provide enough information to understand what went wrong and how to correct it.	3.72	High
Recognition rather than Recall	The system/app is designed to make it easy for users to find the information they need without having to remember many things by presenting information in a way that is easily recognizable, such as using clear and visible labels and instructions.	3.71	High
Flexibility and Efficiency of Use	The system/app provides different levels of functionality and support for different levels of experience that can be used by a broader range of people, and can be more effective for everyone.	3.78	High
Aesthetic and Minimalist Design	The system/app is designed to be visually appealing and easy to use. This means using a simple visual design focused on essential information and functionality. Obstructive elements are eliminated to avoid clutter and distraction.	3.85	High
Help Users Recognize, Diagnose, and Recover from Errors	The system/app displays plain language that is easy to understand and provides enough information for users to identify and correct the problem. Additionally, it provides users with ways to recover from errors without losing work or experiencing significant disruptions.	3.84	High
Help and Documentation	The system/app provides users the help they need to use effectively by providing relevant and easily accessible help resources.	3.85	High
	Overall Mean	**3.80**	**High**

Scale: 1.00–1.80 Very Low, 1.81–2.60 Low, 2.61–3.40 Moderate, 3.41–4.20 High, 4.21–5.00 Very High.

Among the heuristic dimensions, Visibility of System Status obtained the highest mean score (M = 3.90), followed by Consistency and Standards (M = 3.88) and Aesthetic and Minimalist Design (M = 3.85). These findings indicate that users generally perceive the systems as clear, predictable, and visually understandable. In contrast, User Control and Freedom received the lowest mean score (M = 3.68), followed by Recognition Rather than

Recall (M = 3.71) and Error Prevention (M = 3.72). These results suggest that limitations remain in user autonomy, memory support, and error management.

The pattern of results indicates that the evaluated security technologies perform better in interface clarity and system feedback than in supporting flexible and error-resistant interaction. This finding suggests that while users can generally understand system operations, they may experience difficulty when recovering from errors or performing complex tasks. Such limitations may reduce efficiency and may encourage workarounds that weaken security practices.

Overall, the results support the view that usability represents an important component of effective information security implementation. Systems that provide clear feedback and consistent interaction patterns are more likely to support correct user behavior, while limitations in control and error prevention may reduce effective system use.

Visibility of System Status

The heuristic Visibility of System Status obtained the highest mean score (M = 3.90), indicating that respondents generally perceived the security control systems as providing adequate feedback regarding system operations. Clear status indicators and notifications helped users understand ongoing processes and system responses, thereby supporting user confidence and awareness. However, several respondents noted occasional delays in feedback during longer processes, suggesting the need for improved real-time system communication. Consistent with Nielsen's principles, timely feedback reduces uncertainty and promotes trust in system operation.

Match between System and the Real World

The heuristic Match Between System and the Real World obtained a mean score of 3.84, indicating generally positive alignment between system terminology and user expectations. Respondents reported that commands and labels were usually understandable, although technical terminology occasionally created confusion among non-technical users. This finding suggests that while the systems are generally accessible, further improvements in terminology and icon design may enhance intuitive interaction and reduce learning requirements.

User Control and Freedom

The heuristic User Control and Freedom obtained the lowest mean score (M = 3.68), indicating relatively weaker performance compared with other usability dimensions. Respondents reported difficulties in undoing actions and recovering from errors, suggesting limitations in system flexibility. Although basic navigation options were available, users experienced restricted control when correcting mistakes or reversing unintended actions.

Limited user control may increase frustration and reduce efficiency, particularly during complex security tasks.

Consistency and Standards

The heuristic Consistency and Standards obtained a mean score of 3.88, indicating that respondents generally perceived the systems as predictable and uniform in design. Consistent terminology and interface layouts helped users learn system operations more easily and reduced cognitive effort. However, minor inconsistencies in labeling and interface patterns were reported, suggesting that further standardization could improve usability.

Error Prevention

The heuristic Error Prevention obtained a mean score of 3.72, indicating moderate effectiveness in helping users avoid mistakes. Respondents reported that warnings and validation features were generally present, although some safeguards were not sufficiently visible. The results suggest that existing preventive mechanisms support users to some extent but could be strengthened through clearer warnings and more intuitive system guidance.

Recognition Rather than Recall

The heuristic Recognition Rather than Recall obtained a mean score of 3.71, indicating moderate support for memory-independent interaction. Respondents reported that menus and visual cues generally supported navigation, although some tasks still required remembering procedures or commands. Increasing the visibility of options and improving interface cues may reduce cognitive load and improve task efficiency.

Flexibility and Efficiency of Use

The heuristic Flexibility and Efficiency of Use obtained a mean score of 3.78, indicating moderate system adaptability. Respondents reported that the systems were generally usable for routine tasks, although advanced users perceived limited opportunities for customization and efficiency improvements. Improved shortcut options and configurable features may enhance usability for experienced users.

Aesthetic and Minimalist Design

The heuristic Aesthetic and Minimalist Design obtained a mean score of 3.85, indicating positive perceptions of visual clarity and layout simplicity. Respondents generally described the interface as uncluttered and easy to follow. However, some respondents indicated that excessive simplification occasionally made certain functions difficult to locate. Balanced visual design may therefore improve both clarity and accessibility.

Help Users Recognize, Diagnose, and Recover from Errors

This heuristic obtained a mean score of 3.84, indicating generally positive perceptions of error messages and recovery support. Respondents reported that error messages were usually understandable, although some lacked sufficient detail to guide corrective action. Improved diagnostic messages and clearer recovery instructions may strengthen user confidence.

Help and Documentation

The heuristic Help and Documentation obtained a mean score of 3.85, indicating moderate satisfaction with available support materials. Respondents reported that help menus and documentation were generally accessible but sometimes too generic or outdated. Context-sensitive help features may improve usability and reduce dependence on external assistance.

Strengths and Weaknesses of Security Technologies

While Table 1 presents the quantitative usability scores across Nielsen's heuristic dimensions, Table 2 summarizes the key usability strengths and weaknesses identified in the evaluated IT security technologies and their implications for effective security practices. The results indicate that the strongest usability characteristics were associated with visibility of system status, consistency of interface design, and aesthetic clarity, suggesting that users generally understood system operations and navigation. These characteristics support user confidence and reduce uncertainty when performing security-related tasks.

In contrast, several heuristic dimensions showed moderate limitations. User control and freedom, error prevention, and recognition rather than recall received comparatively lower scores, indicating that users experienced difficulties in correcting mistakes, preventing errors, and performing tasks without relying on memory. These limitations suggest that users may encounter obstacles during more complex interactions with security systems.

The results also indicate moderate limitations in flexibility and efficiency of use, particularly for experienced users who require faster and more customizable workflows. Limited flexibility may reduce productivity and may encourage users to bypass formal security procedures in order to complete tasks more efficiently.

Table 2.

Usability Heuristics in IT Security Technologies: Strengths, Weaknesses, and Implications

Usability Heuristic	Strengths	Weaknesses	Usability Implications
Visibility of System Status	Precise feedback mechanisms, status indicators, progress updates.	Some delays in real-time feedback; occasional lack of detailed explanations.	Enhances user confidence, but delayed/incomplete feedback may cause uncertainty and hinder trust.

Usability Heuristic	Strengths	Weaknesses	Usability Implications
Match Between System and the Real World	Uses familiar terminology and aligns with user expectations.	Non-IT staff do not easily understand specific technical jargon.	Promotes ease of learning; misalignment risks user confusion and errors in security compliance.
User Control and Freedom	Undo/recovery options are present; basic navigation is intuitive.	Limited flexibility for advanced users; restricted autonomy in some workflows.	This increases the sense of agency, but lacking freedom may frustrate users and reduce engagement.
Consistency and Standards	Interface design and terminology are mostly uniform across modules.	Minor inconsistencies in icons, labels, and workflows.	Supports predictability and reduces the learning curve, but inconsistencies raise cognitive load and error rates.
Error Prevention	Includes warnings, clear instructions, and validation checks.	Some preventive features are underutilized or overlooked.	Reduces frequency of errors, but gaps in design may still allow costly security mistakes.
Recognition Rather Than Recall	Menu-driven options and visual cues aid navigation.	Some tasks still require memorization of steps or commands.	Improves efficiency by reducing memory burden, but recall dependency increases errors and slows adoption.
Flexibility and Efficiency of Use	Supports both novice and experienced users; some shortcuts are available.	Limited customization options; advanced users feel constrained.	Boosts productivity for novices, but insufficient flexibility reduces satisfaction for expert users.
Aesthetic and Minimalist Design	Interface uncluttered; visual hierarchy well applied.	Some modules lack modern, engaging design features.	Enhances focus and comprehension, but the absence of aesthetic appeal may lower user satisfaction.
Help Users Recognize, Diagnose, and Recover from Errors	Provides error messages and step-by-step recovery guides.	Messages are sometimes vague or overly technical.	Assists users in troubleshooting, but unclear guidance can delay recovery and reduce confidence.
Help and Documentation	Includes manuals, tooltips, and online help resources.	Some documentation is outdated or too generic.	Supports independent learning and problem-solving, but poor documentation reduces reliability and user trust.

Finally, although help and documentation and error recovery mechanisms were generally available, respondents reported that support materials were sometimes overly technical or insufficiently detailed. Improving contextual guidance and recovery instructions may strengthen user confidence and reduce dependence on external technical support.

Overall, the findings indicate that while the evaluated IT security technologies demonstrate generally positive usability, several usability limitations remain that may influence effective system use. These results suggest that usability challenges are not merely interface issues but factors that may directly affect user compliance and organizational security practices.

Overall Usability Implications

The results indicate that IT security technologies at Bicol University demonstrate generally positive usability, with an overall mean score of 3.80, corresponding to a high usability level. Strong performance in system visibility, interface consistency, and visual design suggests that users can generally understand and navigate security applications effectively. However, moderate limitations in user control, flexibility, and error prevention indicate that usability improvements are still necessary. These limitations may reduce efficiency and increase the likelihood of user errors, particularly during complex tasks.

The findings highlight that usability plays a critical role in the effectiveness of information security technologies. Systems that are easier to understand and operate are more likely to support correct user behavior and consistent compliance with security procedures. Conversely, usability limitations may encourage inefficient practices or workarounds that weaken institutional security. For higher education institutions, these results emphasize the importance of incorporating usability considerations into the selection, design, and implementation of information security technologies. Regular usability evaluation may help institutions ensure that security systems remain aligned with user needs and organizational requirements.

The pattern of usability scores suggests that security technologies are generally effective in providing system feedback and maintaining interface consistency, but less effective in supporting flexible and error-resistant interaction. This pattern indicates that institutional security systems may prioritize technical monitoring and control functions over user-centered interaction design. Similar findings have been reported in usability studies of security systems, where technically robust solutions often present usability challenges for end-users. These results highlight the importance of balancing technical security requirements with usability considerations in institutional environments.

These findings reinforce the importance of integrating usability evaluation into cybersecurity system design, particularly in organizational environments where users with diverse technical backgrounds interact with complex security technologies.

Conclusion, Limitations, and Future Research

This study evaluated the usability of IT security technologies used by university personnel using Jakob Nielsen's usability heuristics as an analytical framework. The findings indicate that the evaluated security control systems demonstrated a generally positive usability profile, with an overall mean usability score of 3.80, corresponding to a high level of usability. The results suggest that university personnel were generally able to understand and interact effectively with institutional security applications.

Among the heuristic dimensions, the highest usability ratings were observed in visibility of system status, consistency and standards, and aesthetic and minimalist design,

indicating that the systems provided clear feedback and predictable interaction patterns. These characteristics support user confidence and reduce uncertainty during security-related tasks. In contrast, relatively lower ratings were observed in user control and freedom, recognition rather than recall, and error prevention, suggesting that limitations remain in user autonomy, error management, and memory support. These usability constraints may affect efficiency and increase the likelihood of user errors during complex interactions with security systems.

The findings reinforce the view that effective information security depends not only on technical safeguards but also on the usability of security technologies. Systems that are easier to understand and operate are more likely to support correct user behavior and consistent compliance with security procedures. Conversely, usability limitations may reduce efficiency and encourage workarounds that weaken institutional security practices. The study therefore supports a socio-technical perspective in which users are viewed not as sources of vulnerability but as essential participants in maintaining organizational security.

Several limitations should be considered when interpreting the findings of this study. First, the study was conducted within a single higher education institution, which may limit the generalizability of the results to institutions with different technological infrastructures or user populations. Second, the study relied on self-reported perceptions of usability collected through a survey questionnaire. Although perception-based measures are appropriate for usability evaluation, they may not fully reflect actual user behavior when interacting with security technologies. Third, the study focused specifically on usability characteristics and did not assess the technical effectiveness or security performance of the evaluated systems.

Future research may extend this work by conducting comparative studies across multiple institutions to determine whether the usability patterns identified in this study are consistent across higher education environments. Behavioral and observational usability methods, such as task-based usability testing or simulated security scenarios, may provide deeper insights into user interaction with security technologies. Longitudinal studies may also examine how usability perceptions evolve as users gain experience or receive training. In addition, future studies may explore psychological and human–computer interaction perspectives to better explain how usability influences secure behavior in organizational contexts. Intervention-based research evaluating improvements in interface design, error messages, and user support systems may further strengthen the practical application of usability principles in information security.

REFERENCES

Bush, M., & Mashatan, A. (2025). Bringing security home: The Need for a human-centric approach to securing smart homes. In *The Security of Self: A Human-Centric Approach to Cybersecurity*.

Center for Internet Security. (2026). *Why employee cybersecurity awareness training is important*. https://www.cisecurity.org/insights/blog/why-employee-cybersecurity-awareness-training-is-important

Farahbod, K., Shayo, C., & Varzandeh, J. (2020). Cybersecurity indices and cybercrime annual loss and economic impacts. *Journal of Business and Behavioral Sciences*, *32*(1), 63–71.

IBM. (2025). *IBM X-Force 2025 Threat Intelligence Index*. https://www.ibm.com/thought-leadership/institute-business-value/report/2025-threat-intelligence-index

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security*, *106*, 102267.

Lee, W. J., & Hwang, I. (2021). Sustainable information security behavior management: An empirical approach for the causes of employees' voice behavior. *Sustainability*, *13*(11), 6077.

Morgan, S. (2020). *Cybercrime to cost the world $10.5 trillion annually by 2025*. Cybercrime Magazine. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Nielsen, J. (1994). Enhancing the explanatory power of usability heuristics. In B. Adelson, S. Dumais & J. Olson (Eds.), *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '94)* (pp. 152–158). Association for Computing Machinery. https://doi.org/10.1145/191666.191729

Parenty, T. J. & Domet, J. J. (2019). *A Leader's Guide to Cybersecurity: Why boards need to lead—and how to do*. Harvard Business Review Press.

Triplett, W. J. (2022). Addressing human factors in cybersecurity leadership. *Journal of Cybersecurity and Privacy*, *2*(3), 573–58.