World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(RESEARCH ARTICLE)

Check for updates

The importance of encryption awareness, adoption barriers and encryption by default practices

Imafidor Victoria *, Shokefun Ebunoluwa and Valentin Maria

Department of Mathematics and Computer Science, Southwest Minnesota State University, Marshall, Minnesota, United States of America.

World Journal of Advanced Engineering Technology and Sciences, 2026, 19(03), 320-328

Publication history: Received on 18 May 2026; revised on 27 June 2026; accepted on 29 June 2026

Article DOI: https://doi.org/10.30574/wjaets.2026.19.3.0339

Abstract

Encryption is widely recognized as one of the most effective methods for protecting sensitive digital information from unauthorized access, data breaches, and device theft. Despite its importance, adoption among everyday technology users remains limited. This study examined encryption awareness, confidence in file encryption, barriers to encryption adoption, and attitudes toward encryption by default practices among young adult technology users. A quantitative survey methodology was employed using an online questionnaire distributed through both physical and digital recruitment channels. A total of 108 participants aged 18 years and older completed the survey. The findings indicate that many participants reported limited confidence in their ability to encrypt files when necessary. Lack of knowledge, uncertainty regarding encryption procedures, and perceived complexity were identified as common barriers preventing adoption. Survey responses also revealed that many participants would be more likely to utilize encryption if clearer instructions and educational resources were available. Support for encryption by default was high among respondents, suggesting a preference for security measures that do not require significant user intervention.

The results align with previous research demonstrating that usability challenges and limited cybersecurity knowledge continue to hinder the adoption of encryption technologies. The findings suggest that relying on users to manually implement encryption may not provide adequate protection for sensitive information. Integrating encryption by default into devices and applications offers a practical approach for improving security while reducing the burden placed on individual users. Increased cybersecurity education and simplified security tools may also contribute to greater adoption and more effective protection of personal data.

Keywords: Encryption Awareness; Cybersecurity Education; Data Protection; Encryption By Default; Usability Barriers

1. Introduction

Data security has become one of the most pressing concerns in the digital age, yet one of the most overlooked by everyday users. As personal devices store increasingly sensitive information, from financial records and private communications to health data and professional documents, the need for robust data protection mechanisms has never been more urgent. Encryption stands as one of the most reliable and well-documented tools available for protecting digital information, yet its broad adoption among general users remains alarmingly low. Understanding why this gap exists, and what can be done to close it, is central to advancing cybersecurity at the individual and institutional level.

Personal devices such as smartphones, laptops, and tablets are now primary vehicles for storing and transmitting sensitive data. These devices are vulnerable to a range of threats including unauthorized access, data breaches, theft,

* Corresponding author: Imafidor Victoria.

and malware. File encryption addresses many of these risks by converting readable data into an unreadable format that can only be accessed with the appropriate key or credential. When properly implemented, encryption provides a critical layer of defense that limits the damage caused by physical device loss or digital compromise. Despite this, encryption remains underutilized by the public, suggesting that technical availability alone is not sufficient to drive adoption. Research consistently points to a disconnect between users' desire for privacy and their actual security behaviors[1][2]. Many individuals acknowledge the importance of protecting their data but report low confidence in their ability to use encryption tools effectively. Usability barriers, limited cybersecurity education, and a general lack of awareness about encryption options contribute to this disconnect. When users do not understand how encryption works or how to apply it, they are unlikely to seek it out, even when the tools are readily accessible. This creates a systemic vulnerability that affects not only individual users but also the broader digital ecosystem they participate in.

These patterns raise important questions about where responsibility for data protection should lie. If users lack the knowledge, confidence, or motivation to encrypt their own files, a compelling argument emerges for shifting that responsibility to device manufacturers and software developers through encryption by default practices. Default encryption would ensure that data protection is applied automatically, removing the burden from individual users and establishing a higher baseline of security across devices and platforms. This study examines encryption awareness, adoption barriers, and attitudes toward default encryption practices among young adult technology users. Specifically, the research evaluates participant confidence in their ability to encrypt files, identifies factors that discourage encryption adoption, and assesses support for automatic encryption implementation on personal devices. The findings of this study suggest that low encryption adoption is driven primarily by usability challenges and limited awareness, and that implementing encryption by default represents a practical and necessary step toward improving data protection for everyday users.

2. Literature Review

File encryption technologies are fundamental tools used to protect sensitive information from unauthorized access. Encryption transforms readable data into ciphertext that can only be accessed using an authorized cryptographic key. According to Scarfone et al. [3], storage encryption technologies can be implemented through full-disk encryption, volume encryption, and file-level encryption, each providing different levels of protection for data stored on end-user devices. These technologies help protect information from device theft, unauthorized access, and data breaches, making encryption a critical component of modern cybersecurity. Organizations increasingly rely on encryption technologies to safeguard confidential information stored on computers, portable devices, removable media, and enterprise backup systems. Fritsche and Rodgers [4] evaluated multiple encryption solutions as part of a university-wide initiative to secure sensitive information and found that successful encryption implementation depends not only on the strength of encryption algorithms but also on factors such as platform compatibility, authentication methods, usability, and key management capabilities. Their evaluation of various whole-disk, file-level, and virtual-disk encryption solutions demonstrated that organizations must balance security requirements with ease of use to ensure effective deployment.

The literature suggests that while modern encryption technologies provide strong protection for digital information, their effectiveness depends on both technical implementation and user accessibility. As digital devices continue to store increasing amounts of sensitive personal and organizational data, encryption remains one of the most important tools for maintaining confidentiality and reducing the risk of unauthorized access. Consumer cybersecurity behavior is often influenced by users' perceptions, awareness, and understanding of available security technologies. Although many individuals express concerns about privacy and data protection, research suggests that users frequently misunderstand the tools designed to secure their information. This disconnect can reduce the effectiveness of cybersecurity measures and contribute to poor security practices.

Dechand et al. [5] examined user perceptions of end-to-end encryption following WhatsApp's implementation of default encrypted messaging. The researchers found that although most participants had heard of encryption, only a small number understood its purpose or implications. Many users overestimated the capabilities of attackers while underestimating the effectiveness of modern encryption technologies. Participants commonly believed that skilled attackers, governments, or hackers could easily bypass encryption protections, resulting in low levels of trust in encryption systems.The study also revealed a significant lack of awareness regarding encryption. Despite WhatsApp's deployment of end-to-end encryption and notifications informing users that their communications were protected, many participants remained unaware that encryption was being used. Others reported noticing security notifications but either ignored them or misunderstood their significance. These findings indicate that simply providing security technologies does not guarantee that users will understand or trust them.The results highlight a persistent gap between cybersecurity protections and user awareness. Even when encryption is automatically implemented, many users fail to recognize its presence or understand its benefits. This lack of awareness may contribute to poor security decision-

making and supports the need for both improved cybersecurity education and security by default approaches that protect users regardless of their technical knowledge.

Although encryption provides an effective method for protecting sensitive information, usability challenges continue to limit its effectiveness among everyday users. Security technologies can only provide protection when users are able to locate, understand, and correctly use the available security features. When encryption systems are difficult to navigate or require specialized technical knowledge, users may avoid them altogether. Furnell [6] argues that one of the most significant obstacles to effective cybersecurity is the usability of security features within end-user applications. The study found that users frequently encounter difficulties finding security options, understanding their purpose, and applying them correctly. Even when security functionality is available, users often fail to benefit from it because they lack the knowledge required to configure and operate the features effectively. Furnell further notes that many security tools require users to understand complex concepts such as encryption algorithms, cryptographic keys, and digital signatures, creating additional barriers for nontechnical users. The research also highlights the role of interface design in influencing security behavior. Security options are often presented using technical terminology, fragmented menus, and complicated configuration settings that discourage user engagement. As a result, users may ignore available security protections or make uninformed decisions regarding security settings. Furnell [6] suggests that security features should be easy to locate, simple to configure, supported by clear documentation, and designed to minimize the technical burden placed on users.

These findings demonstrate that usability is a critical factor influencing encryption adoption. Even when users recognize the importance of protecting their information, poorly designed security interfaces can prevent effective use of encryption technologies. Improving usability through simplified interfaces, clearer guidance, and more intuitive security controls may help increase encryption adoption and strengthen overall cybersecurity practices. LaFleur and Chen [7] investigated why email encryption remains underutilized despite its importance in protecting sensitive information. Through a survey of email users from various professional backgrounds, the researchers found that the primary barriers to adoption were poor usability and limited user knowledge. Participants frequently reported that encryption programs were difficult and frustrating to use, while many lacked an understanding of how encryption works or what information should be protected. The study also revealed that users often transmitted sensitive information through email without encryption and were generally dissatisfied with existing encryption tools. The authors concluded that improving user education and increasing the usability of encryption technologies are essential for increasing adoption. These findings suggest that relying solely on users to voluntarily implement encryption may be ineffective when awareness and technical understanding remain limited, supporting the need for more automated approaches to data protection.

Cybersecurity literacy plays a critical role in determining whether individuals adopt protective technologies and follow recommended security practices. Cybersecurity literacy refers to a user's ability to understand security risks, recognize threats, and effectively utilize available security tools to protect sensitive information. Despite growing awareness of cyber threats, research suggests that many users continue to engage in behaviors that increase their vulnerability to cyberattacks. Moustafa et al. [8] argue that human behavior remains one of the greatest vulnerabilities in cybersecurity. Citing previous research, the authors note that human errors are responsible for a substantial proportion of cyber and network attacks. Common security mistakes include password sharing, reusing passwords across multiple accounts, clicking suspicious links, opening attachments from untrusted sources, failing to update software, and oversharing information online. These behaviors often occur because users prioritize convenience and accessibility over security protections. The authors further found that many individuals underestimate the likelihood of experiencing cybersecurity incidents and frequently fail to recognize potential threats. Studies reviewed by Moustafa et al. [8] demonstrated that significant numbers of users fall victim to phishing attacks, disclose sensitive information, and delay important security updates. These findings suggest that limited cybersecurity awareness and poor security decision-making contribute significantly to user vulnerability. The relationship between cybersecurity literacy and encryption adoption is particularly important because encryption requires users to understand both the risks associated with unprotected data and the benefits of available security technologies. Users with limited cybersecurity knowledge may be unaware of encryption tools or uncertain about how to use them effectively. Consequently, low cybersecurity literacy can become a barrier to encryption adoption. These findings support the need for improved cybersecurity education while also reinforcing the importance of encryption-by-default approaches that provide protection regardless of users' technical knowledge or security awareness.

3. Materials and Methods

This study employed a quantitative survey research methodology to examine encryption awareness, encryption adoption barriers, user confidence in file encryption, and attitudes toward encryption by default practices among young

adult technology users. The research focused on evaluating participant confidence in their ability to encrypt files, identifying factors that discourage encryption adoption, assessing whether educational resources could increase encryption usage, and examining support for automatic encryption implementation on personal devices. Quantitative survey methodology was selected because it provided a structured approach for collecting measurable participant attitudes, perceptions, and self reported cybersecurity behaviors related to data protection and digital privacy. Descriptive statistical analysis was utilized to identify trends and patterns associated with encryption awareness, adoption barriers, and support for default encryption practices.

Participants were recruited using both physical and digital distribution methods over a three month data collection period. Eligibility requirements specified that all participants must be at least 18 years of age prior to participation. Consent confirmation was included at the beginning of the survey instrument to ensure voluntary participation and adherence to ethical research standards. Recruitment efforts included distributing survey flyers throughout educational and public environments such as classrooms, student centers, cafeterias, campus buildings, conferences, student organizations, and community bulletin boards. Both standard poster sized flyers and smaller portable handout versions were utilized to increase participant accessibility and engagement. Digital survey links were additionally shared through electronic communications, social media platforms, peer networks, and group messaging channels to broaden participant reach and improve response diversity. Participation remained entirely voluntary throughout the study. No monetary compensation, academic incentives, or coercive recruitment methods were used. Participants were informed that all responses would remain anonymous and that no personally identifiable information would be collected during the study. Maintaining respondent anonymity was intended to encourage honest responses regarding cybersecurity knowledge, encryption usage, and digital privacy practices. At the conclusion of the data collection period, 108 complete survey responses were retained for analysis. Following completion of data collection, the survey instrument was unpublished from Google Forms and closed to additional submissions to preserve dataset integrity.

Primary data collection was conducted using Google Forms as the survey administration platform. The survey instrument incorporated demographic questions, multiple choice items, Likert scale measurements, and cybersecurity perception questions designed to evaluate participant understanding and use of encryption technologies. Responses were collected electronically and automatically compiled through the survey platform for subsequent analysis.

The survey specifically examined:

- participant confidence in their ability to encrypt files when necessary;
- barriers preventing the adoption and use of file encryption technologies;
- willingness to adopt encryption practices if clearer instructions and educational resources were available; and
- participant attitudes regarding whether encryption should be enabled by default on personal devices.

The final participant population consisted primarily of younger adult technology users with high levels of digital engagement. Most participants were between the ages of 18 to 24 years (72.2%), followed by participants between the ages of 25 to 34 years (18.5%). Smaller participant groups represented older demographic categories. The participant population was heavily student dominated, with students representing 82.4% of all respondents. Educational backgrounds varied from high school education through doctoral level attainment. This demographic composition provided an appropriate sample for examining encryption awareness, usability barriers, and attitudes toward default security protections among users who frequently interact with online applications, cloud storage services, and personal computing devices. Survey responses were analyzed using descriptive statistical techniques. Frequency distributions, percentages, and response patterns were calculated for each survey question to identify trends related to encryption awareness and adoption. Results were presented through graphical visualizations illustrating participant confidence in file encryption abilities, perceived barriers to encryption use, willingness to utilize encryption when provided with clearer instructions, and support for default encryption implementation on personal devices. These analyses were used to evaluate whether usability challenges and knowledge limitations influence encryption adoption and whether participants support automated security measures designed to improve data protection.

Table 1 Demographic characteristics of participants (N = 108)

Category	n	%
18–24	78	72.2
25–34	20	18.5
35–44	5	4.6
45–54	1	0.9
55–64	2	1.9
≥65	2	1.9
Student	89	82.4
Full-time employed	11	10.2
Part-time employed	3	2.8
Self-employed	3	2.8
Unemployed	2	1.9
High school or equivalent	25	23.1
Some college	34	31.5
Associate degree	5	4.6
Bachelor's degree	31	28.7
Master's degree	10	9.3
Doctoral degree	3	2.8

4. Results and Discussion

Participant confidence in file encryption abilities was evaluated using a five-point Likert scale, as shown in Figure 1. The responses indicate that confidence levels varied considerably among participants, with many respondents reporting only moderate confidence in their ability to encrypt files when necessary. These findings suggest that although younger technology users interact with digital devices on a daily basis, many do not possess the practical skills required to implement file encryption independently.

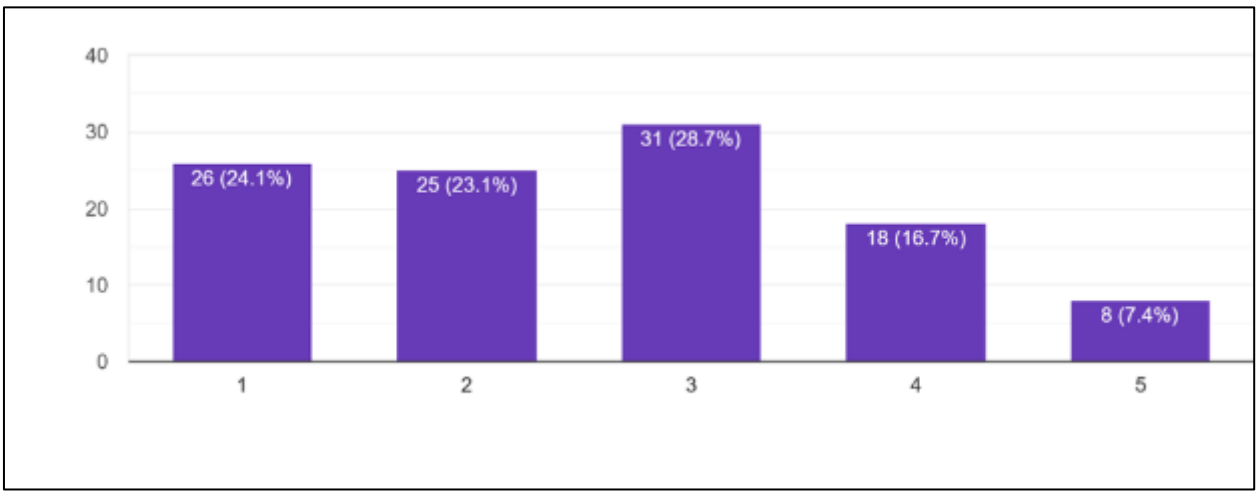

Figure 1 Confidence in File Encryption Ability (How confident are you in your ability to encrypt files)

The findings are consistent with prior research demonstrating that users frequently struggle with encryption technologies. Abu-Salma et al. [1] reported that "the vast majority of participants did not understand the essential concept of end-to-end encryption" (Abu-Salma et al., [1]). Ruoti et al. [9] concluded that modern encryption tools remain unusable for the masses despite years of technological advancement (Ruoti et al., [9]). The persistence of these challenges suggests that making encryption available does not guarantee that users will understand or utilize it effectively.

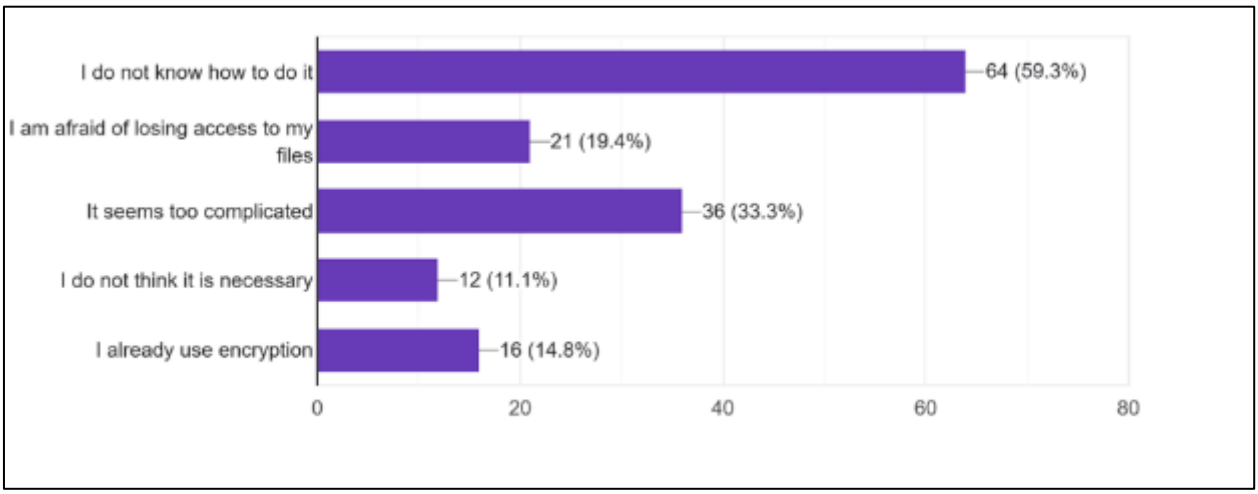

Figure 2 Barriers to File Encryption Adoption

The barriers identified by participants closely align with findings reported throughout the cybersecurity literature. Reuter et al. [10] found that users frequently experience confusion when interacting with encryption systems and often struggle with key management processes (Reuter et al., [10]). Ramokapane et al. [11] reported that many smartphone users do not fully understand privacy and security settings available on their devices (Ramokapane et al., [11]). Frik et al. [12] found that users often remain unaware of available security controls and rarely review their device security settings after initial setup (Frik et al., [12]). These studies suggest that encryption adoption is influenced by both technical availability and user comprehension. When security systems require substantial effort, technical knowledge, or additional configuration steps, adoption rates decline. Alsaleh et al. [13] reported that users frequently prioritize convenience over security and may disable security features when they interfere with everyday activities (Alsaleh et al., [13]). This behavior creates a challenge for cybersecurity professionals seeking to improve user protection through voluntary adoption alone.

To examine whether educational interventions could improve encryption adoption, participants were asked whether they would be more likely to encrypt files if clearer instructions were available. The results are presented in Figure 3.

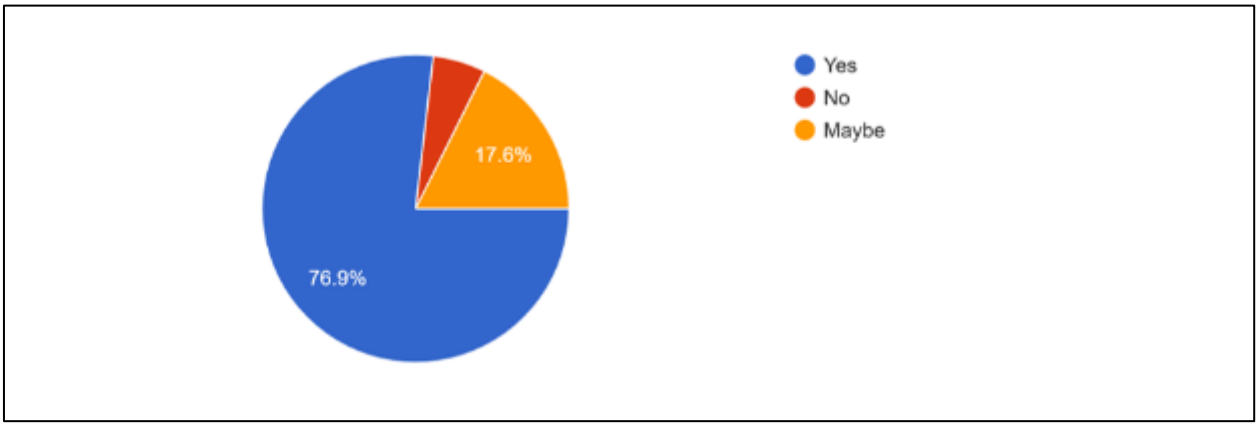

Figure 3 Willingness to Use Encryption if Clearer Instructions Were Available

Most participants indicated that they would be more likely to utilize encryption if clearer guidance and educational resources were provided. This finding suggests that a lack of cybersecurity knowledge represents a significant barrier

to adoption. Participants appear willing to engage in protective security behaviors but may lack the practical knowledge required to do so effectively. The literature supports this interpretation. Numerous studies have demonstrated that users express concern about privacy and data security while failing to implement available protective measures. Oltmann found that many individuals value privacy and data protection but often lack the knowledge or motivation required to utilize encryption technologies (Oltmann, [2]). Abu-Salma et al. [1] observed that misunderstanding of encryption concepts directly influences adoption decisions (Abu-Salma et al., [1]). Cybersecurity education remains important, but educational interventions should be viewed as complementary rather than standalone solutions. Stransky et al. [14] found that visual explanations and indicators of encryption status had only limited effects on user behavior (Stransky et al., [14]). Their findings suggest that even when users receive additional information about encryption, many continue to struggle with implementation. Education can improve awareness, but awareness alone does not guarantee adoption.

Participant responses regarding encryption by default practices provide evidence supporting structural solutions. As illustrated in Figure 4, a large proportion of respondents agreed that encryption should be enabled by default on personal devices.

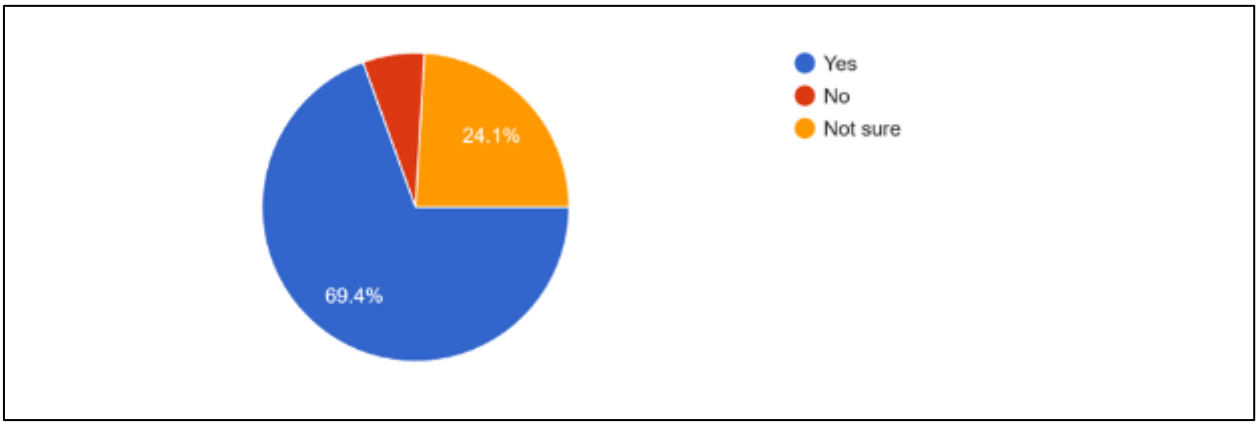

Figure 4 Support for Encryption by Default

Support for default encryption reflects recognition that security should not depend entirely on user expertise. Participants acknowledged the importance of protecting personal information while reporting barriers that prevent them from implementing encryption independently. These findings suggest that users prefer security solutions that operate automatically and require minimal technical intervention. The concept of encryption by default is increasingly supported by both industry practice and academic research. Apple's Data Protection framework automatically encrypts user data on supported devices, while Google's Android operating system incorporates file based encryption as a standard security feature (Apple, [15]; Google, [16]). These approaches recognize that many users will never manually configure advanced security settings regardless of their awareness of cybersecurity risks. Research findings from the present study provide support for this approach. Participants reported limited confidence in their encryption abilities, identified knowledge and usability barriers as major obstacles, and expressed support for automatic encryption implementation. These findings suggest that placing responsibility for encryption solely on end users may be ineffective.

The results also highlight an important cybersecurity policy consideration. Personal devices now store financial information, health records, educational data, authentication credentials, and private communications. The consequences of unencrypted data exposure continue to increase as digital technologies become more integrated into daily life. Regulatory frameworks and cybersecurity best practices increasingly emphasize proactive data protection measures rather than reactive responses after data breaches occur. Implementing encryption by default aligns with these principles by providing protection regardless of individual user expertise. The findings of this study demonstrate that low encryption adoption is driven primarily by usability challenges, limited technical knowledge, and insufficient cybersecurity education. The results indicate that users value privacy and security but frequently lack the ability or confidence necessary to implement encryption independently. Encryption by default represents a practical strategy for improving data protection while reducing the burden placed on individual users. The evidence presented in both the survey findings and existing literature suggests that automatic encryption implementation offers a more reliable and scalable solution than relying solely on voluntary user adoption.

5. Conclusion

The findings of this study reinforce a straightforward but important conclusion: most users are not encrypting their data, not because they do not care about privacy, but because the tools available to them are complex, poorly understood, and difficult to access. Across the survey responses, participants consistently reported low confidence in their ability to encrypt files and identified usability barriers and lack of knowledge as the primary reasons they do not currently use encryption. At the same time, the vast majority indicated they would be more likely to use encryption if clearer instructions were provided and expressed support for encryption being enabled by default on their personal devices. These results paint a clear picture of a population that values data protection but lacks the practical means to act on that value. The gap between awareness and implementation is not a new problem in cybersecurity, but it is one that carries serious consequences. As personal devices become more deeply integrated into daily life and continue to store increasingly sensitive data, the cost of inadequate protection grows alongside them. Relying on individual users to voluntarily adopt encryption, without adequate education, intuitive tools, or structured guidance, places an unrealistic burden on the very people that security practices are meant to protect. The evidence from this study suggests that this model is not working and that a structural change in how encryption is delivered is needed.

Encryption by default offers the most direct path to addressing this gap. When encryption is built into devices and applications as a standard feature rather than an optional one, users benefit from data protection regardless of their technical knowledge or security awareness. This approach shifts responsibility from the user to the manufacturer and developer, where the technical capacity to implement encryption already exists. Many technology companies have already adopted automatic encryption and stronger built in security protections, while regulatory frameworks continue to evolve in ways that increasingly favor stronger data protection standards. This study's findings support the case for accelerating that shift and making default encryption a baseline expectation rather than a premium feature. Cybersecurity education also remains an important component of any long term solution. While default encryption reduces the barrier to protection, an informed user base is better equipped to make decisions about their data, recognize threats, and engage meaningfully with the security tools available to them. Integrating practical encryption education into academic curricula, workplace training programs, and public facing digital literacy initiatives would complement technical improvements by building the foundational knowledge users currently lack. protecting user data should not depend on whether a user happens to know what encryption is or how to use it. Security by default, supported by accessible education and clear communication, represents the most equitable and effective approach to ensuring that data protection is available to everyone, not just those with the technical background to pursue it independently.

Limitations

Several limitations should be considered when interpreting the findings of this study. First, the participant population was heavily student dominated, with individuals between the ages of 18 to 24 representing most respondents. As a result, the findings may not fully represent broader demographic populations with different educational backgrounds, technology usage behaviors, or digital literacy levels.

Compliance with ethical standards

Acknowledgments

The authors would like to thank all survey participants who contributed to this study.

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Abu-Salma R, Sasse MA, Bonneau J, Danilova A, Naiakshina A and Smith M. (2017). Obstacles to the adoption of secure communication tools. 2017 IEEE Symposium on Security and Privacy, 137-153.

[2] Oltmann SM. (2023). Outcomes and affordances: Examining why people use encryption. International Journal of Communication, 17.

[3] Scarfone K, Souppaya M and Sexton M. (2007). Guide to storage encryption technologies for end user devices. NIST Special Publication 800-111.

[4] Fritsche GD and Rodgers SK. (2007). Encryption technologies: Testing and identifying campus needs. Proceedings of the 35th Annual ACM SIGUCCS Fall Conference, 109-112.

[5] Dechand S, Naiakshina A, Danilova A and Smith M. (2019). In encryption we don't trust: The effect of end-to-end encryption to the masses on user perception. 2019 IEEE European Symposium on Security and Privacy (EuroS&P), 401-415.

[6] Furnell S. (2005). Why users cannot use security. Computers and Security, 24(4), 274-279.

[7] LaFleur KS and Chen L. (2014). Email encryption: Discovering reasons behind its lack of acceptance. Proceedings of the International Conference on Security and Management (SAM), 1-7.

[8] Moustafa AA, Bello A and Maurushat A. (2021). The role of user behaviour in improving cyber security management. Frontiers in Psychology, 12, 561011.

[9] Ruoti S, Andersen J, Zappala D and Seamons K. (2015). Why Johnny still, still can't encrypt: Evaluating the usability of a modern PGP client. ArXiv Preprint arXiv:1510.08555.

[10] Reuter A, Abdelmaksoud A, Boudaoud K and Winckler M. (2021). Usability of end-to-end encryption in e-mail communication. Frontiers in Big Data, 4, 568284.

[11] Ramokapane KM, Rashid A and Such JM. (2019). A study on the usability of smartphone manufacturer provided privacy settings. Proceedings on Privacy Enhancing Technologies, 2019(4), 211-232.

[12] Frik A, Kim J, Sanchez A and Egelman S. (2022). Users' expectations about and use of smartphone privacy and security settings. Proceedings of the CHI Conference on Human Factors in Computing Systems.

[13] Alsaleh M, Alarifi A, Al-Salman AM, Alshreef M and Alfaris A. (2017). Smartphone users: Understanding how security mechanisms are perceived and new persuasive methods. PLOS ONE, 12(3), e0173284.

[14] Stransky C, Wermke D, Huaman N, Acar Y, Fahl S and Mazurek ML. (2021). On the limited impact of visualizing encryption. Seventeenth Symposium on Usable Privacy and Security. USENIX Association.

[15] Apple Inc. (2024). Encryption and data protection overview. Apple Platform Security.

[16] Google. (2024). Android encryption. Android Open Source Project.