Borneo International Journal eISSN 2636-9826; Vol.8 (4); 2025; 8-17
Published by *Majmuah Enterprise*
www.majmuah.com

An Assessment of User Awareness on Cybersecurity Best Practices on Social Media Platforms

MUHAMMAD EIZZAT ABDUL RAZZAK, MOHAMMAD FADLI ZOLKIPLI

School of Computing, College of Arts and Science, Universiti Utara Malaysia (UUM), 06010 Sintok, Kedah, MALAYSIA
Email: m_eizzat_abdul@ahsgs.uum.edu.my, m.fadli.zolkipli@uum.edu.my

Received: November 19, 2025
Accepted: November 25, 2025
Online Published: December 01, 2025

Abstract

Social media platforms are increasingly vulnerable to sophisticated cyberattacks such as phishing, malware, identity theft, data scraping, and social engineering. These risks stem from technical flaws and risky user behaviors, including poor password management, over-disclosure of personal information, and habitual disregard for security measures. Additionally, psychological factors like security fatigue, privacy resignation, and habituation to security warnings contribute to these challenges, elevating the perceived cost of secure behavior over the risks of data breaches. This assessment explores these vulnerabilities while advocating for a multifaceted approach to enhance cybersecurity awareness on social media. Such an approach includes educational initiatives, technical interventions, and the cultivation of user responsibility to promote secure practices and strengthen trust across these platforms.

Keywords: Cybersecurity; Social Media; User Awareness; Security Threats; Data Privacy; Risk Management

1. Introduction

In social media, user awareness of security threats and data privacy is undeniably important in addressing cybersecurity posture. Many cybersecurity incidents have pointed to the fact that human being is weakest link in the defense against cyber threats (Kannelønning & Katsikas, 2023). Awareness serves as the first level of defense for information systems and networks (Ben Salamah et al., 2023). By exploring the challenges and opportunities of cybersecurity in this domain, this research aims to identify and summarize key insights and develop guidance for reducing social media security and technological risks. Specifically, this review focuses on identifying factors affecting users' cyber awareness on social media platforms, alongside platform's security-related features and determining the impact of best practices awareness on users' cyber behaviour.

2. Methodology

The research methodology for this SLR involves defining data sources and search queries based on established practices used in related systematic reviews.

2.1. Data Sources

Relevant literature searches in the field of cybersecurity awareness and social media frequently target the following academic databases:

- Scopus and Google Scholar.
- IEEE Xplore and the ACM Digital Library.
- Science Direct via eRESOURCES@LINTAS UUM.

2.2. Keywords

To gather comprehensive literature relevant to user awareness, best practices, and social media security, the search queries would combine Boolean operators (AND, OR) with a selection of primary and related keywords:

- Primary Keywords: *'cybersecurity'* OR *'cyber security'*, *'social media'*, *'user awareness'*, *'security threats'*, *'data privacy'*, and *'risk management'*.

- Related Keywords: *'social media best practices'*, *'social media security'*, *'social guideline'*, *'social media risks'*, and *'information security awareness'*.

2.3. Inclusion and Exclusion Criteria

The selection of relevant articles would be guided by the following inclusion and exclusion criteria, ensuring adherence to academic standards.

Table 1: Inclusion and Exclusion Criteria

Inclusion Criteria	Exclusion Criteria
Peer-reviewed articles with full access rights.	Articles asking for payments for the access.
Published within a specified timeframe, such as 2020–2025 (to focus on recent trends).	Articles published outside the intended time frame.
Language is English.	Articles written in other languages.
Full text availability.	Articles with no full-text availability.
Must include relevant keywords and pertain to cybersecurity awareness or behaviour of a user on social media.	Non-empirical studies.
Articles that address cybersecurity behaviour and discuss a theoretical model (if seeking theoretical depth).	Studies describing behaviour but not specifically cybersecurity.

2.4. Data Extraction

Data extracted from the literature focus on observable user behaviours, identified knowledge deficits, and the measured success of awareness programs.

3. User Behaviours and Knowledge Gaps on Cybersecurity Best Practices

3.1. Discrepancy in Behaviour

There is apparent inconsistency between privacy concerns and practise of privacy by social media users, displaying contradictory behaviour famously known as the privacy paradox (Herath et al., 2022). The privacy paradox reflects how immediate social rewards often outweigh abstract or distant security risks. Users gain recognition, connection, and validation through sharing and engagement, while the harms of poor privacy practices feel uncertain or unlikely. Users often prioritize social interaction over security issues and reveal a lot of information about themselves due to their desire to build their own identities, leading them to neglect privacy settings or security measures (Cengiz et al., 2022). Platform design reinforces this imbalance through default-open settings, frictionless sharing, and prompts that highlight social benefits rather than security costs. Knowing the security policies and guidelines may not necessarily equates to acting and complying with them. One example is the respondents in research by Alkhazi et al. indicates many enterprise users believe in the importance of security measures, however due to time contrains, they themself do not adhere to simple practices such as timely change of passwords or review privacy settings (Alkhazi et al., 2022). This supports the idea of present bias, by prioritizing immediate needs and convenience over abstract risks.

Cognitive biases also play a role, where optimism bias, present bias, and social proof encourage users to assume that negative events won't happen to them, or that common practices must be safe, assuming risks are more likely to happen to others (Frauenstein et al., 2023). Individuals tends to have an optimistic bias on security risk perception of themselves; overestimating the likelihood of cyber compliance and underestimating the likelihood of cybersecurity incident (Almansoori et al., 2023). This discrepancy appears as inconsistent use of privacy controls, acceptance of broad app permissions, and routine posting of information that can be sensitive. Users may understand that data can be misused, yet fail to review settings, limit audiences, or question third-party integrations (Cengiz et al., 2022). In social media tools, many interfaces are complex or fragmented, thereby expose user's data to more public access than intended. There is a necessity for user-friendly privacy tools (Ghosh et al., 2025). Over time, habits form around convenience and visibility, relying on exterior cues and simple decision rules to save time and effort on social media. This *'convenience gap'* overlooks suspicious characteristics, making it harder to reverse course even after learning about risks, thereby creating the gap between stated security concerns and actual behaviours (Frauenstein et al., 2023).

3.2. Self-Disclosure and Vulnerability

High usage of social media correlates with a high level of self-disclosure behaviour (Herath et al., 2022). Social media users frequently share excessive personal details (e.g. phone numbers, locations) and often fail to check privacy settings beforehand. This self-disclosure is driven by platform affordances, and social dynamics that reward visibility, authenticity, and rapid interaction (Cengiz et al., 2022). Over exposure of personal data may happen through:

- Features such as stories, live updates, and geotagging encourage regular posting and real-time sharing.
- Identity-based communities and comparison culture can increase the pressure to share more details to maintain status or belonging.
- Emotional states - excitement, stress, fear of missing out - makes personal details feel harmless, weakens caution in the moment, and reducing the motivation to review privacy boundaries.

The risk increases the moment user are complacent in diligently managing their social media accounts' privacy settings, thus providing cybercriminals with the ammunition needed to craft social engineering and phishing attacks (Mouncey & Ciobotaru, 2025). Scammers launch targeted phishing schemes leveraging these emotional states – for example the anxiety present in users who have fear of missing out (FOMO) of a reward or deal (Mouncey & Ciobotaru, 2025). For attackers, these disclosures create a rich pool of open-source intelligence (Nowakowski, 2025). Birthdates, workplaces, routines, family ties, and travel plans can be combined to tailor spear-phishing messages, impersonation attempts, and pretexting scenarios that feel highly credible (Herath et al., 2022). These snippets of information are perfect ammunition for social engineering, and increases the success rate of well-crafted spear phishing on social media.

3.3. Limited Knowledge and Awareness

Most users are unaware of the specific risks and vulnerabilities associated with social media platforms unless they have personally experienced a cyber incident (Herath et al., 2022). Experience with a breach or scam often triggers learning; the study by Mamade and Dabala found that a staff member's cybersecurity awareness was significantly enhanced by a real cyber-attack on the individual (Mamade & Dabala, 2021). Even among educated populations, many possess minimal cybersecurity knowledge, particularly regarding sophisticated protections like firewalls or updating anti-virus software (Abdulla et al., 2023). For instance, highly educated individuals may still miss the need to be at certain cybersecurity awareness levels, due to manual habits or infrequent computer use. A central issue is that users are often considered the most vulnerable element in the security chain (Mulahuwaish et al., 2025). Complicated terminology and information security issues concepts requires effort to be fully understood and may require advanced technical knowledge. Terms like phishing, two-factor authentication, end-to-end encryption, and permissions are often misunderstood or conflated (Kannelønning & Katsikas, 2023). Users may not recognize that small oversights - delayed software updates, weak authentication, permissive application access – is compound into significant risk of vulnerability exposures (Pattnaik et al., 2023).

Education level does not always translate into cybersecurity competence. One study conducted by Reid16 found that self-identified experts had less cyber hygiene knowledge than self-identified non-experts (Zwilling et al., 2020). Busy schedules and infrequent personal computer use can lead to long privacy update gaps and unreviewed privacy controls. Some users assume platforms or institutions will handle security automatically, reducing personal vigilance (Mulahuwaish et al., 2025).

3.4. Password Practices

In as survey conducted by Abulla et al, it is common for internet users to use their personal data to register on social accounts. Moreover they were commonly using the similar password for different social media accounts, increasing their vulnerability (Abdulla et al., 2023). Password reuse and reliance on personal information reflect a trade-off between convenience and security under cognitive constraints. Users struggle to remember many unique credentials and therefore choose familiar patterns -names, dates, or interests - that are easy to recall but also easy to guess. Social media content itself often reveals these patterns, making cracking a password easy for a hacker who possesses the right software tools and a few personal data, gained from someone's social media (Herath et al., 2022). Reuse further amplifies risk; when one platform is breached, attackers can perform credential stuffing across other services to gain control broadly and rapidly (Shah et al., 2023).

The implementation of robust authentication methods is required to prevent the risk of identity theft and secure password practices. Another good exercise is to regularly update passwords, or deploy multi-factor authentication, which can significantly reduce the risk of identity theft and account hijacking (Mulahuwaish et al., 2025). The use of password managers are now vital tools that both store and generate secure passwords and make it easy to update passwords frequently to add an extra layer of security (Ghosh et al., 2025).

4. Effectiveness of Awareness Programs

4.1. Impact of Awareness

Studies by Herath et al. suggest that higher cybersecurity awareness directly contributes to lesser cases of reported online risky behaviours. Conversely, lack of knowledge on appropriate cybersecurity actions can also lead to inappropriate cyber behaviour (Herath et al., 2022). The Knowledge, Attitude, and Behaviour (KAB) concept model used in a different study puts forward the idea that higher knowledge of security policies and procedures leads to an improvement in cyber hygiene, which ultimately enhances security-related behaviour (Alkhazi et al., 2022). Conversely, low understanding concerning appropriate cybersecurity actions can lead to inappropriate cyber behaviour. Cybersecurity incidents are often caused by human mistakes or inadequate knowledge; compliant behaviour is at stake when employees neither have the knowledge nor been given sufficient information about the organization's security policies (Almansoori et al., 2023). In other words, a higher digital and cyber-security literacy correlate with better safety and risk analysis on social media (Mouncey & Ciobotaru, 2025).

4.2. Training Effectiveness

Cybersecurity training needs to be clear and easily understood to enhance its effectiveness, considering that most important mechanisms against attacks are user vigilance and awareness. An effective awareness training should be:

- Platform-specific, rather than generic social media phishing training (Mouncey & Ciobotaru, 2025).
- Focus on literacy levels of individuals, not overgeneralize based on demographics (Mouncey & Ciobotaru, 2025).
- Continuous refined for social cybersecurity, ensuring they are intuitively comprehensible (Mulahuwaish et al., 2025).

4.3. Limitations of Traditional Methods

Traditional awareness campaigns can increase short-term knowledge, but may be temporary, with messages quickly forgotten. This lack of long-term effectiveness is exacerbated when the training methods used such as static documents or unidirectional lectures does not engage participants effectively, causing knowledge retention problems and hindering the development of practical skills (Eliza, 2025). Furthermore, studies focusing on organizational settings found that security policies are often ignored even when known, due to factors such as time pressure or differing motivations (Abdillah et al., 2024). Security measures often inherently reduce the usability and functionality of systems, hence employees may deliberately choose noncompliant behaviour if security is viewed as a hindrance to achieving their work objectives or ensuring social interaction. Some trainings and campaigns have been observed as unsuccessful in changing behaviour, demonstrating a substantial gap between what users know and what they actually do (Herath et al., 2022). This difficulty in behavioural modification implies that merely educating employees does not equate to compliance, as individuals may deliberately choose to not comply even when policies and guidelines are known (Alkhazi et al., 2022).

5. Thematic Analysis

5.1. Human Error

The concept that humans are the weakest link remains a core theme across the literatures, suggesting this viewpoint is practically common knowledge. The popularity and effectiveness of social engineered attacks stems from the attacker's ability to exploit human behavioural vulnerabilities, often in connection with software design that fails to account for these natural human tendencies (Nowakowski, 2025). Even organizations that invest heavily in strong security technologies continue to suffer incidents, demonstrating that effective security is a combination of people, processes, and technology (Alkhazi et al., 2022). The risks posed by social media are amplified not solely by technological vulnerability, but by the user's thoughtless actions, negligent behaviour, or intentional disregard for security protocols (Herath et al., 2022) (Ben Salamah et al., 2023). Users frequently exhibit insecure behaviours, such as skipping

important software updates, unwillingness to adopt to Multi-Factor Authentication (MFA) or password managers, or neglecting security issues to ensure social interaction (Pattnaik et al., 2023). Even when users are aware of security policies, some may ignore compliance out of preference, due to factors like time pressure, inadequate knowledge, or different motivations (Abdillah et al., 2024). Moreover, frequent and habitual engagement on social media can lead to user-induced vulnerabilities; behaviors like sharing and clicking hyperlinks performed with insufficient cognition, making users vulnerable to phishing (Frauenstein et al., 2023).

5.2. Motivation and Risk Perception

Research exploring cybersecurity behaviour often employs behavioural theories, particularly the Protection Motivation Theory (PMT), as the most frequent theoretical model utilized (Almansoori et al., 2023). This prominence is rooted in PMT's ability to explain how people respond to fear appeals and their subsequent motivation to protect themselves (Akib et al., 2025). According to this framework, an individual's decision to engage in protective actions is primarily influenced by two cognitive evaluations: threat assessment, and coping appraisal. By understanding these factors, protective behaviours can be adopted to tailor to individual differences, as these decisions are intrinsically built on how an individual perceives and evaluates risk. The core thematic focus of PMT is concentrated on psychological factors related to threat appraisal, specifically the concepts of perceived severity and perceived vulnerability - the psychological factors that drive individuals to adopt protective measures (Almansoori et al., 2023). When individuals perceive a threat as severe and believe they are highly susceptible to it, they are strongly motivated to adopt protective behaviors aimed at mitigating that threat. This makes PMT a crucial tool for designing effective countermeasures, as the theory's structure explicitly identifies the psychological elements necessary to enhance a positive attitude and translate awareness into protective conduct (Frauenstein et al., 2023).

5.3. Threat Landscape

Social media is recognized as a tireless amplifier of cyber threats, facilitating various attacks such as phishing, malware, identity theft, and social engineering. Social media sites have been found to be ten times more effective at delivering malware and stealing information than previously popular methods like email (Abdillah et al., 2024). Social media serves as a *'goldmine of information'* for attackers, with users readily sharing intimate details such as birth dates, locations, and employers, or voluntarily revealing more personal information than intended (Nowakowski, 2025). The sheer volume of data shared and the subsequent ability of cybercriminals to craft sophisticated and tailored scams, emphasize the vulnerability arising from the platform's open and high-sharing nature (Herath et al., 2022). Phishing is a prominent threat often distributed via social media platforms, which exploit the tendency of a normal person to act on trust, even when it's easy to falsify them online. Modern threat actors have amplified this vulnerability by utilizing Artificial Intelligence (AI) to craft customized attacks. AI-enabled tools are used to launch targeted attacks, including AI-powered phishing and deepfake videos, making scams highly convincing and tailored to specific audiences (Ghosh et al., 2025). This sophisticated automation makes identifying and resisting these difficult-to-detect threats a critical challenge for users.

6. Factors Influencing User Awareness and Behaviour

6.1. Best Practise Knowledge

Cyber knowledge is frequently recognized as a dominant factor that positively correlates with increased cyber security awareness (Kovacevic et al., 2020). This relationship is a fundamental premise of the Knowledge-Attitude-Behaviour (KAB) model discussed in section 4.1 earlier, which suggests that acquiring more knowledge about security policies and procedures leads to advancement in attitude towards risk, thereby enhancing overall security-related behaviour. Empirical evidence supports this link, confirming that an individual's degree of information security knowledge has a positive association with information security awareness, and those with greater knowledge of the cyber world are typically associated with higher awareness of cyber-attacks (Chua et al., 2021). This highlights the critical role of structured educational programs, as learning about cybersecurity through formal education or specialized training is positively connected to improving an individual's cyber-attack awareness. This heightened cyber awareness is a crucial intermediate factor that directly influences subsequent protective behaviour, as research by Akib et al. demonstrates that cyber security awareness partially mediates the connection between knowledge and cyber protection (Akib et al., 2025). This means that individuals who possess better cyber knowledge become more sensitive to potential cyber hazards, which then prompts them to exhibit more protective behaviours. Studies show that higher awareness correlates with a lower number of reported online risky behaviours, impacting user behaviour when protecting against information security risks (Herath et al., 2022). Ultimately, it is the level of awareness that dictates a user's efforts to

reduce the chances of a cyber-attack, allowing them to apply appropriate measures to prevent threats and reducing the number of potential attacks.

6.2. Educational Background

Research consistently suggests that a higher education level leads to higher information security awareness and subsequently helps to reduce risky user behaviour (Herath et al., 2022). Empirical studies confirm that social education level influences cybersecurity awareness and subsequent protective behaviour, noting that an individual's background plays a vital role in addressing cyber security risks (Hijji & Alam, 2022). When users improve their awareness, this is reflected in better security behaviour, which indicates that educational efforts generally succeed in improving cyber security outcomes. This variability underscores the critical need for specialized cyber security awareness training programs, particularly focusing on the specific knowledge gaps inherent in non-technical departments. Employees with technological backgrounds tend to be more familiar with cyber threats than others, while the general population often finds complex information security issues difficult to fully comprehend due to the requirement for advanced technical knowledge (Kannelønning & Katsikas, 2023). Therefore, effective programs must move away from generic, *'one-size-fits-all'* approaches, which are known to fail, and instead tailor the training depth based on the roles and responsibilities of the employees (Zhang et al., 2021). Highly technical training methods, such as Capture the Flag (CTF), are more suitable for those with technology educational backgrounds and unsuitable for non-technical participants (Eliza, 2025). This gap necessitates that cybersecurity education must be able to address the needs of people across all educational backgrounds, rather than solely those in technical departments.

6.3. Demographic Variables

Findings regarding the influence of age on cyber security outcomes are notably inconsistent in the general literature. On one hand, some studies found that older adults achieved higher Information Security Awareness (ISA) scores than young adults, and a linear relationship has been pointed out where ISA improves with increased age (Zwilling et al., 2020). Conversely, despite younger individuals often possessing higher social media digital literacy, they are frequently characterized as being in the high-risk category for victimization, particularly those between 18 and 30 years old (Herath et al., 2022). Thus, the elevated vulnerability is largely attributed to high usage of the internet especially social media and networks, which exposes them disproportionately to threats like social media phishing, regardless of age. Similarly, the influence of gender on cyber awareness is conflicting across different studies. Some sources identified a small significant difference where females had higher ISA scores than males (Herath et al., 2022). However, contrasting research suggests that males have more cyber hygiene knowledge. In a comparative study by Zwilling et al., males were found to possess more awareness of cyber-attacks compared to females (Zwilling et al., 2020). These gender differences in self-reported knowledge and awareness sometimes correlate with women reporting slightly lower computer skills and less prior experience with computer security, suggesting that variations in self-evaluation (such as potential overconfidence among men or under confidence among women) might contribute to these disparate research findings (Kovacevic et al., 2020).

7. Gaps in Literature

Significant gaps remain in the literature concerning user awareness of cybersecurity best practices on social media, particularly when moving beyond general internet security.

7.1 Social Media Specificity

Eyber security training is found to be effective only when it is specific to the reality of the learner, suggesting that a generic social media anti-phishing training may be less effective than training tailored to particular platforms, like Facebook or Instagram (Mouncey & Ciobotaru, 2025). Many organizations rely on existing training frameworks that are often generic, cumbersome to implement, and fail to adequately address human factors, overlooking the nuances of security within the highly interactive social media environment (Ben Salamah et al., 2023). Researchers attempting to assess security awareness often find that previous work focused narrowly on just one element of information security, such as phishing or mobile device security, instead of providing a holistic view of risks across diverse platforms (Alkhazi et al., 2022). This indicates a need for studies that delve into platform-specific security risks and features related to different social networking sites, to improve mitigation strategies for unwary users.

7.2 Platform's Vulnerability Assessment

There is lack of sufficient studies that definitively disclose the impact of social media users' secure behaviour on their vulnerability level within the platform. Although cyber behaviour generally influences the vulnerability level a user

faces, there is inadequate evidence to prove this direct link specifically for secured behaviour on social media platforms (Herath et al., 2022). This gap hinders the ability to quantify the effectiveness of secure practices, such as employing complex, unique passwords or multi-factor authentication, in reducing the chances of becoming a victim of threats like identity theft or malware spread through social media. Understanding this relationship is crucial because users frequently expose themselves to risk through actions like over-sharing personal details or using third-party apps, making the assessment of how secure behaviours counters these specific vulnerabilities.

7.3 Recommended Practices from User's Perspective

Another limitation identified in systematic reviews is the missing studies related to recommended cybersecurity practices for social media users as articulated from the users' point of view. Policy makers and security professionals frequently propose mitigation strategies that are rarely derived from empirical investigation into user perspectives. For example, some students claim to use a 'best practices' approach, but the meaning of this term is subjective, often rooted merely in knowledge gleaned from the internet, friends, or colleagues (Herath et al., 2022). Identifying recommended practices from the users' perspective is necessary to develop training and policies that are practical, usable, and effectively address the inherent risks users faces.

7.4 Methodological Focus

Research into cybersecurity behaviour, including within social media contexts, predominantly relies on quantitative research methods, primarily utilizing questionnaire surveys for data collection (Almansoori et al., 2023). This over-reliance on self-reported, subjective data collection methods is noted as a weakness, as it can lead to biased responses and struggles to reliably measure true compliance. Furthermore, in the niche area of social cybersecurity, studies focusing exclusively on forecasting and prediction of cyberattacks are lacking, with most current analyses focusing only on attack detection (Mazhar et al., 2023). Future research is encouraged to employ objective measurements, utilize mixed methods approaches to mitigate bias, and adopt more advanced analytical techniques such as machine learning algorithms, to process the large-scale data generated by social media activity for predictive capabilities.

7.5 Emerging Threats

The research landscape also struggles to keep pace with the rapid emergence and evolution of sophisticated threats amplified by modern technology. There is a need for ongoing investigation to address the evolution of the social media landscape as attackers continuously leverage on new platform features and communication channels (Mulahuwaish et al., 2025). Attackers also are increasingly employing generative AI tools to automate and customize attacks, creating convincing deep fakes and targeted phishing campaigns that exploit human psychology, making it harder to distinguish fact from fiction. This requires researchers to develop adaptive modelling frameworks and focus on proactive threat prediction and dynamic defence strategies, moving beyond detection alone.

8. Implications for Practice

Based on the synthesis of key findings, several practical recommendations can be made for enhancing user awareness on cybersecurity best practices. The recommendations are split into two, on one side targeting users themselves and on the other side focusing on platform owners and policy makers.

8.1. Targeting Individual Social Media Users

- **Cultivate Digital Scepticism:** Individual users must cultivate digital scepticism to effectively combat sophisticated threats like phishing and social engineering, which frequently exploit the human tendency to act on trust. Digital scepticism requires continuous education on social engineering tactics and phishing scams. For example, with help of AI, it's easy to forge online fake profiles to impersonate known individuals or businesses. Users need to be very cautious when receiving messages or links from an unknown source and must verify the authenticity of the message before clicking or providing sensitive details (Ghosh et al., 2025). Educational campaigns and training programs that improve digital literacy and critical evaluation skills are crucial for countering misinformation and enabling users to recognize deceptive content, ensuring they do not become the weakest link in falling for scams (Monachelis et al., 2025).

- **Manage Data Disclosure:** Social media users must consciously manage their data disclosure by being very cautious of what they share online. Reckless disclosure of Personally Identifiable Information (PII) often results in identity theft, harassment, or stalking (Ghosh et al., 2025). The most powerful privacy protection strategy falls into the users' own hands regarding what they publish and to whom. To enforce this, users must verify and regularly

change their privacy settings to ensure only trusted individuals view their data, particularly since default settings often compromise privacy (Kohanová et al., 2025). Users should avoid exposing sensitive data, such as identification numbers or passwords, in any public or semi-public posts.

- **Adopt Holistic Cyber Hygiene:** To adopt a holistic cyber hygiene, users should implement a comprehensive suite of protective measures integrated into their regular digital habits, promoting wiser and smarter usage behaviour (Abdillah et al., 2024). This includes consistently implementing and regularly updating anti-malware software on all devices, as well as ensuring regular software updates are performed for operating systems and applications to neutralize vulnerabilities. Additionally, cyber hygiene involves the proactive behaviour of regularly monitoring accounts for abnormal access activity or unauthorized changes, and incorporating these secure practices into continuous digital literacy efforts (Jian & Kamsin, 2021).

8.2. Targeting Organizations and Policymakers

- **Implement Adaptive Training Frameworks:** Effective training must be customized to organizations and circumstances, taking into account factors like business needs, budgets, and cultures (Mulahuwaish et al., 2025). It is recommended for organizations to implement adaptive training frameworks such as the *Adaptive Cybersecurity Training Framework for Social Media Risks (ACSTF-SMR)*. This framework was specifically developed to tailor education based on employee roles and responsibilities, where existing frameworks were often perceived as too generic or cumbersome to implement (Ben Salamah et al., 2023). This is done by assessing the employee's level of awareness (knowledge, behaviour, and attitude) and identifying their background, including preferred training methods, job roles, age, and education.

- **Focus on Behavioural Change:** To achieve effective security outcomes, training programs must fundamentally focus on behavioural change, moving past mere information dissemination. In the security awareness definition by *NIST Special Publication 800-16* mentioned that ‘awareness’ itself is explicitly stated to be not training. Programs should be designed to encourage compliance and demonstrably improve cyber hygiene practices (Eliza, 2025). Effective training courses should be crafted as problem-centred initiatives that utilize realistic case studies, tailored to the specific threats and the employee's level of awareness (Zwilling et al., 2020). Furthermore, programs that are designed to be enjoyable and engaging are crucial, as this increases the likelihood that employees will stay committed, and subsequently engage in self-development activities, which also helps minimize security fatigue (Alkhazi et al., 2022). Comparative studies of intervention strategies by Alkhazi et al. also revealed that text-based and game-based training formats significantly outperformed other methods, like lectures alone, in achieving superior behavioural change outcomes.

- **Leverage Social Media for Education:** Policymakers, academic institutions, and governments should actively leverage on social media to disseminate cybersecurity awareness material regularly, capitalizing on the platforms’ efficiency as communication mediums. Since social media is progressively superseding traditional media, the most effective approach is to utilize the same communication media that users engage with regularly (Chua et al., 2021). Similarly, government and organizations can efficiently utilize these platforms to disseminate data and issue timely alerts about specific threats and good practices via social media posts (Ben Salamah et al., 2023).

- **Address Cultural and Regional Gaps:** Policymakers must address cultural and regional gaps by developing effective security awareness programs that account for the diverse socio-technical systems and cultural differences that influence human online behaviour globally (Shah et al., 2023). To ensure program success, policy must champion culturally sensitive training and awareness programs that are available in local languages, addressing the barrier posed by many existing IT security programs being available only in English. This regionally and culturally tailored approach helps states enhance cyber safety, governance, and trust among their citizens.

9. Conclusions

This assessment highlights the critical need for enhanced user awareness of cybersecurity threats on social media platforms. The prevalence of cyberattacks like phishing, identity theft, and data exploitation serves as a reminder of both the technical vulnerabilities these platforms face and the significant role of risky user behaviors. The review confirms that while social media offers vast opportunities, its increasing usage presents significant cybersecurity risks, primarily exacerbated by human factors. Addressing these challenges requires a tailored and multifaceted approach that combines technological solutions, user education, and psychological interventions to mitigate risks. Significant research gaps persist, particularly the lack of studies validating the direct links between awareness and secure behaviours specifically on social media platforms, and the need for more culturally and individually tailored research.

By fostering better password hygiene, reducing over-disclosure of personal information, and combatting security fatigue, individuals and organizations can work collaboratively to improve online safety, strengthen governance, and build trust among digital citizens.

Acknowledgments

The authors would like to thank all members of the School of Computing who are involved in this study. This study was carried out as part of the Cybersecurity and Social Media Project. This work was supported by Universiti Utara Malaysia. Special appreciation is extended to academic mentors and colleagues for their valuable feedback and guidance throughout the research process. The author is also thankful for the availability of open-access research and documentation, which played a critical role in shaping the analysis presented in this paper.

References

Abdillah, A., Widianingsih, I., Buchari, R. A., & Nurasa, H. (2024). Big data security & individual (psychological) resilience: A review of social media risks and lessons learned from Indonesia. Array, 21, 100336. https://doi.org/10.1016/j.array.2024.100336

Abdulla, R. M., Faraj, H. A., Abdullah, C. O., Amin, A. H., & Rashid, T. A. (2023). Analysis of social engineering awareness among students and lecturers. IEEE Access, 11, 101098–101111. https://doi.org/10.1109/access.2023.3311708

Akib, A. A. P. M., Candiwan, C., & Ramadhani, D. P. (2025). Cybersecurity compliance and other factors influencing employee protective behavior: A case study of bank X in Indonesia. International Journal of Safety and Security Engineering, 15(06), 1229–1241. https://doi.org/10.18280/ijsse.150613

Alkhazi, B., Alshaikh, M., Alkhezi, S., & Labbaci, H. (2022). Assessment of the impact of information security awareness training methods on knowledge, attitude, and behavior. IEEE Access, 10, 132132–132143. https://doi.org/10.1109/access.2022.3230286

Almansoori, A., Al-Emran, M., & Shaalan, K. (2023). Exploring the frontiers of cybersecurity behavior: A systematic review of studies and theories. Applied Sciences, 13(9), 5700. https://doi.org/10.3390/app13095700

Ben Salamah, F., Palomino, M. A., Craven, M. J., Papadaki, M., & Furnell, S. (2023). An adaptive cybersecurity training framework for the education of social media users at work. Applied Sciences, 13(17), 9595. https://doi.org/10.3390/app13179595

Cengiz, A. B., Kalem, G., & Boluk, P. S. (2022). The effect of social media user behaviors on security and privacy threats. IEEE Access, 10, 57674–57684. https://doi.org/10.1109/access.2022.3177652

Chua, H. N., Teh, J. S., & Herbland, A. (2021). Identifying the effect of data breach publicity on information security awareness using hierarchical regression. IEEE Access, 9, 121759–121770. https://doi.org/10.1109/access.2021.3107426

Eliza, F. (2025). Effectiveness of cybersecurity awareness program based on mobile learning to improve cyber hygiene. International Journal of Information and Education Technology, 15(2), 220–229. https://doi.org/10.18178/ijiet.2025.15.2.2235

Frauenstein, E. D., Flowerday, S., Mishi, S., & Warkentin, M. (2023). Unraveling the behavioral influence of social media on phishing susceptibility: A Personality-Habit-Information Processing model. Information & Management, 60(7), 103858. https://doi.org/10.1016/j.im.2023.103858

Ghosh, S., Gulati, A., Bera, A., Singh, S., . A., & Bhatia, M. (2025, May). Cybersecurity and social media: Privacy concerns in the digital age. SSRN Electronic Journal. International Conference on Innovative Computing & Communication (ICICC), New Delhi. https://doi.org/10.2139/ssrn.5237743

Herath, T. B. G., Khanna, P., & Ahmed, M. (2022). Cybersecurity practices for social media users: A systematic literature review. Journal of Cybersecurity and Privacy, 2(1), 1–18. https://doi.org/10.3390/jcp2010001

Hijji, M., & Alam, G. (2022). Cybersecurity awareness and training (CAT) framework for remote working employees. Sensors, 22(22), 8663. https://doi.org/10.3390/s22228663

Jian, N. J., & Kamsin, I. F. B. (2021). Cybersecurity awareness among the youngs in Malaysia by gamification. Atlantis Highlights in Computer Sciences. 3rd International Conference on Integrated Intelligent Computing Communication & Security (ICIIC 2021), Bangalore. https://doi.org/10.2991/ahis.k.210913.061

Kannelønning, K., & Katsikas, S. K. (2023). A systematic literature review of how cybersecurity-related behavior has been assessed. Information & Computer Security, 31(4), 463–477. https://doi.org/10.1108/ics-08-2022-0139

Kovacevic, A., Putnik, N., & Toskovic, O. (2020). Factors related to cyber security behavior. IEEE Access, 8, 125140–125148. https://doi.org/10.1109/access.2020.3007867

Mamade, B. K., & Dabala, D. M. (2021). Exploring the correlation between cyber security awareness, protection measures and the state of victimhood: The case study of Ambo University's academic staffs. Journal of Cyber Security and Mobility, 10(4), 699–724. https://doi.org/10.13052/jcsm2245-1439.1044

Mazhar, T., Irfan, H. M., Khan, S., Haq, I., Ullah, I., Iqbal, M., & Hamam, H. (2023). Analysis of Cyber Security Attacks and Its Solutions for the Smart grid Using Machine Learning and Blockchain Methods. Future Internet, 15(2), 83. https://doi.org/10.3390/fi15020083

Monachelis, P., Maitland, E., Iordanou, K., Patrikakis, C. Z., Yalaz, E., & Papadopoulos, P. (2025). Social media as a lens for understanding public trust in science. 2025 IEEE 49th Annual Computers, Software, and Applications Conference (COMPSAC), 203–211. https://doi.org/10.1109/compsac65507.2025.00034

Mouncey, E., & Ciobotaru, S. (2025). Phishing scams on social media: An evaluation of cyber awareness education on impact and effectiveness. Journal of Economic Criminology, 7, 100125. https://doi.org/10.1016/j.jeconc.2025.100125

Mulahuwaish, A., Qolomany, B., Gyorick, K., Abdo, J. B., Aledhari, M., Qadir, J., Carley, K., & Al-Fuqaha, A. (2025). A survey of social cybersecurity: Techniques for attack detection, evaluations, challenges, and future prospects. Computers in Human Behavior Reports, 18, 100668. https://doi.org/10.1016/j.chbr.2025.100668

Nowakowski, W. (2025). Social engineering analysis framework: A comprehensive playbook for human hacking. IEEE Access, 13, 18827–18849. https://doi.org/10.1109/access.2025.3532999

Pattnaik, N., Li, S., & Nurse, J. R. C. (2023). Perspectives of non-expert users on cyber security and privacy: An analysis of online discussions on twitter. Computers & Security, 125, 103008. https://doi.org/10.1016/j.cose.2022.103008

Shah, M. U., Iqbal, F., Rehman, U., & Hung, P. C. K. (2023). A comparative assessment of human factors in cybersecurity: Implications for cyber governance. IEEE Access, 11, 87970–87984. https://doi.org/10.1109/access.2023.3296580

Zhang, Z. (Justin), He, W., Li, W., & Abdous, M. (2021). Cybersecurity awareness training programs: A cost–benefit analysis framework. Industrial Management & Data Systems, 121(3), 613–636. https://doi.org/10.1108/imds-08-2020-0462

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber security awareness, knowledge and behavior: A comparative study. Journal of Computer Information Systems, 62(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269