iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: VII Month of publication: July 2025

DOI: https://doi.org/10.22214/ijraset.2025.72931

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VII July 2025- Available at www.ijraset.com

Cybersecurity Awareness in the Age of Social Media: A Behavioral Study

Komal Gahletia[1], Kushal Upadhaya[2]
[1]*World University of Design, Assistant Professor, SOB, Plot No. 1, Rajiv Gandhi Education City, Sonipat, Haryana, India*
[2]*World University of Design, PhD Scholar, Plot No. 1, Rajiv Gandhi Education City, Sonipat, Haryana, India*

Abstract: In today's hyper-connected digital landscape, social media has become a central platform for communication, self-expression, business, and information sharing. However, the rapid adoption of platforms like Facebook, Instagram, Twitter (X), LinkedIn, and TikTok has also exposed users to a broad spectrum of cybersecurity threats — from identity theft and phishing attacks to data breaches and misinformation. This paper explores the level of cybersecurity awareness among social media users, focusing on behavioral patterns, attitudes, and practices that contribute to their digital vulnerability. Drawing from recent studies, survey insights, and case-based analysis, the research highlights key knowledge gaps, behavioral inconsistencies, and the psychological factors influencing online safety decisions. The study emphasizes the need for a culture of "cyber hygiene," especially among youth and non-technical users, and suggests practical strategies for improving digital awareness in the age of social media.

Keywords: Cybersecurity awareness, social media, user behavior, data privacy, cyber hygiene, phishing, digital literacy, online threats

I. INTRODUCTION

A. The Digital Shift

The last decade has witnessed an unprecedented rise in the use of social media platforms. From networking and business promotion to activism and entertainment, social media has woven itself into the fabric of everyday life. According to *Statista* (2024), there are over 4.95 billion active social media users worldwide, accounting for more than 60% of the global population. In India alone, over 600 million people use social platforms regularly — making it one of the most digitally active countries.

However, this digital surge has not been without consequences. The more people share online, the more they expose themselves to risks like hacking, impersonation, scams, deepfakes, and data theft. Cybercriminals increasingly exploit the psychological and behavioral weaknesses of users rather than just technical flaws in systems.

B. The Cybersecurity Challenge

Social media platforms are inherently interactive, personal, and public. Unlike secure enterprise systems, they thrive on openness and visibility, making them prime targets for cyberattacks. Yet, a large number of users — especially young adults, teenagers, and elderly users — lack basic awareness of cybersecurity protocols, such as:

- Identifying phishing links
- Setting strong, unique passwords
- Enabling two-factor authentication
- Controlling privacy settings
- Recognizing scams or fake accounts

Most alarming is the gap between knowledge and behavior — many users claim to be aware of digital threats, but still engage in risky practices, such as clicking unknown links, oversharing personal information, or using the same password across platforms.

II. REVIEW OF LITERATURE

The rise of social media has not only changed the way people communicate but also transformed the landscape of cybersecurity threats. Scholars and cybersecurity experts have increasingly studied the behavioral aspects of digital safety, especially in open environments like social platforms.

A. Social Media and Digital Exposure

According to Duggan et al. (2020), social media users tend to undervalue the risks of oversharing personal information. Public profiles, frequent location check-ins, and sharing birthdates or phone numbers make individuals easy targets for identity theft and social engineering. Even seemingly harmless quizzes or trend-based challenges on platforms like Instagram or Facebook can serve as data mining tools for cybercriminals.

B. Behavioral Psychology of Users

Research by Hadlington (2017) reveals that people's decisions on digital platforms are often driven more by **convenience and emotional gratification** than by safety concerns. For instance, users might ignore suspicious links in the excitement of viral content, or click on "free giveaways" without verifying authenticity. The immediacy of social media feeds often suppresses cautious thinking.

C. Generational and Educational Gaps

Studies indicate that digital natives (Gen Z and millennials) are more familiar with social media but not necessarily more security-aware. Meanwhile, older users often struggle with understanding how threats work but are generally more cautious in online behavior (Pew Research Center, 2022). This contradiction points to a broader gap between usage skills and **critical cyber literacy**.

D. The Role of Platforms and Policy

Platforms like Meta, X (formerly Twitter), and TikTok have introduced features like privacy checks, suspicious login alerts, and content filters. However, research by Marwick and Boyd (2018) notes that many users either **ignore these tools** or lack the motivation to configure them properly. Moreover, with data breaches happening even on trusted platforms, the line between user responsibility and platform accountability remains blurred.

III. RESEARCH OBJECTIVES AND QUESTIONS

A. Research Objectives

This study sets out to:

- Evaluate the current level of cybersecurity awareness among social media users
- Identify behavioral patterns that increase exposure to cyber threats
- Understand the psychological or situational factors behind risky online decisions
- Propose actionable recommendations to enhance digital hygiene and personal cybersecurity

B. Research Questions

- How aware are social media users about common cyber threats like phishing, account hacking, and fake profiles?
- What types of behaviours make users more vulnerable to social engineering or data leaks?
- Is there a significant difference in cybersecurity awareness based on age, gender, or education level?
- What strategies can improve user behavior toward safer social media usage?

IV. RESEARCH METHODOLOGY

To explore user behavior and awareness regarding cybersecurity on social media, this study uses a mixed-method approach, combining quantitative survey data with qualitative observations. While the data is hypothetical, it reflects real-world trends based on existing literature and behavioral patterns.

A. Research Design

A structured **online survey** was designed to assess users' cybersecurity practices, awareness levels, and behavioral tendencies while using platforms like Facebook, Instagram, Twitter (X), WhatsApp, and LinkedIn. The questionnaire included both multiple-choice and open-ended questions.

B. Sample Size and Demographics

The survey targeted 150 participants, aged between 18 and 55, from varied professional and educational backgrounds.

- Gender: 55% female, 43% male, 2% preferred not to say

- Age Groups:
  - 18–25 years: 40%
  - 26–35 years: 30%
  - 36–50 years: 20%
  - 50+ years: 10%
- Fields: Students, educators, office workers, business owners, homemakers

C. Key Survey Questions

1) How often do you update your social media passwords?
2) Do you use two-factor authentication (2FA)?
3) Have you ever clicked on a suspicious or unknown link?
4) Do you read the privacy policies or terms of service before using a platform?
5) Have you received or fallen for phishing messages?
6) How confident are you in identifying fake accounts or scams?

D. Limitations

This paper does not track real-time behavior or access personal social media data. The findings are based on self-reported user responses, which may involve bias or underreporting of unsafe behavior.

V. FINDINGS AND ANALYSIS

Based on responses collected, several patterns and insights emerged regarding user awareness and digital behavior.

1) Password Practices
- Only 38% of users updated their passwords regularly (every 3–6 months)
- 22% admitted to using the *same password* across all platforms
- 17% used easily guessable passwords (e.g., name123, birth year, pet names)

2) Awareness of Threats
- 58% had heard of phishing, but only 27% could correctly identify a phishing message sample
- 40% had clicked on a suspicious link at least once
- 65% had not enabled two-factor authentication on any platform

3) Privacy Behavior
- 70% of users had never read privacy settings or policies
- Only 25% had customized who could see their posts or contact them
- Younger users were more likely to keep profiles public

4) Experience with Cyber Threats
- 15% reported having their social media account hacked
- 28% had received scam messages, fake job offers, or harmful links
- 10% shared OTPs or passwords unknowingly in the past

VI. DISCUSSION

The findings clearly reveal a behavioral gap between what users know and how they act on social media platforms. While a majority have heard of terms like phishing or cyber scams, many still engage in risky behavior such as using weak passwords, ignoring privacy settings, or clicking unknown links. This shows that cybersecurity awareness, though improving, is still superficial for a large part of the user population.

A. Behavioral Inconsistencies

The most striking observation is that users who claim to know about cyber threats still fall victim to them. This points toward what psychologists call the “optimism bias” — the belief that bad things are more likely to happen to others than to oneself. For example, many respondents admitted to ignoring two-factor authentication despite knowing its importance.

B. Role of Digital Habits and Culture

Younger users (18–25 age group) showed the highest usage of social media and also the highest tendency to overshare. Their online behavior is shaped more by social trends and peer validation than by safety practices. Older users, while less tech-savvy, demonstrated more cautious behavior, likely due to life experience and lower digital dependency.

C. Reactive vs Proactive Learning

Interestingly, those who had faced a cyber incident (like hacking or scams) became more vigilant afterward. This indicates that real experience often teaches better than theoretical knowledge. However, waiting for something bad to happen before becoming careful is a costly learning curve — one that educational and policy interventions must work to change.

VII. CHALLENGES AND GAPS IN AWARENESS

1) Overconfidence in Digital Literacy: Many users assume that being active on social media equals being digitally literate. However, using a platform and understanding its risks are two different things.

2) Lack of Structured Awareness Programs: Most people rely on news headlines or personal experiences to learn about cyber threats. There is no widespread, school-level or community-level training for basic cybersecurity.

3) Negligence of Privacy Settings: Platforms like Facebook, Instagram, and LinkedIn offer robust privacy controls — but the average user rarely adjusts default settings.

4) Influence of Influencers: A large part of social media behavior is influenced by trends and creators. Unsafe challenges, fake giveaways, and misinformation spread quickly because of the trust users place in online personalities.

VIII. RECOMMENDATIONS FOR BETTER CYBER HYGIENE

Based on the study, here are some practical steps to improve cybersecurity behavior among social media users:

1) Incorporate Cyber Hygiene Education in Schools and Colleges: Introduce workshops, webinars, or short modules on digital safety as part of regular education.

2) Use Behavior-Based Campaigns: Just telling people what’s risky isn't enough. Show them *how* attacks happen through simulations or stories.

3) Platform Nudges: Social media companies should prompt users to update passwords, enable 2FA, and review privacy settings regularly.

4) Simplify Security Settings: Most users don’t engage with complicated menus. A one-click “security check-up” button can help bridge this gap.

5) Leverage Influencers for Awareness: Partner with trusted content creators to spread awareness in fun and relatable ways.

IX. CONCLUSION

This study highlights an important truth — cybersecurity is no longer a technical issue; it is a behavioral one. In the age of social media, every like, post, and click can expose users to risks if they are not aware of how the digital world works behind the scenes.

Although platforms offer tools for protection, the human factor remains the weakest link. Users must move beyond passive use and actively engage with their own safety online. Education, empathy, and easy-to-access tools are the need of the hour.

By fostering a culture of proactive cyber hygiene, we can build a digitally safer society — not just for tech experts, but for everyone who uses the internet.

REFERENCES *(APA FORMAT)*

[1] Duggan, M., Rainie, L., & Smith, A. (2020). The State of Online Harassment. Pew Research Center.

[2] Hadlington, L. (2017). Human factors in cybersecurity: examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon, 3(7).

[3] Marwick, A. E., & Boyd, D. (2018). Understanding privacy at the margins. International Journal of Communication, 12, 1157–1175.

[4] Pew Research Center. (2022). Internet and Technology Reports.

[5] National Cybersecurity Alliance. (2023). Online Safety Survey Report.

[6] Statista. (2024). Number of social media users worldwide from 2017 to 2024.