Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-4 | April - 2025 | Page 280-287

Cybersecurity Awareness

[1]Sahil Bandhe, [2]Rajan Kumar, [3]Naveen Gupta, [4]Himanshu Patel, [5]Mr. Kamlesh Kumar Yadav

[1,2]Students of BCA 6th Semester

[3,4]Students of BCS 6th Semester

[5]Assistant Professor

[1,2,3,4,5]Kalinga University, Naya Raipur (C.G)

[1]Sahilbandhe581@gmail.com, [2]rajankumarmth503@gmail.com, [3]nivyoscar87701@gmail.com,

[4]himanshupatel5212@gmail.com, [5]kamlesh.yadav@kalingauniversity.ac.in

Abstract

In the digital age, cybersecurity has emerged as a foundational pillar for both personal safety and national security. As technology continues to evolve rapidly, so do the methods and tactics of cybercriminals, posing increasing threats to individuals, organizations, and governments alike. However, despite significant investments in cybersecurity infrastructure and technologies, human error remains one of the most critical vulnerabilities exploited in cyberattacks. This research paper investigates the pivotal role of cybersecurity awareness in mitigating digital threats and building a more resilient digital society. The study explores the current landscape of cybersecurity awareness among various user groups—including students, working professionals, and general internet users—by conducting comprehensive surveys and analyzing behavioral patterns related to online safety. By leveraging behavioral theories such as the Protection Motivation Theory and the Technology Acceptance Model, this paper identifies common knowledge gaps, risky behaviors, and misconceptions that often lead to data breaches and system compromises.

Keywords: Cybersecurity Awareness, Digital Threats, Online Safety Behavior, Information Security Education, Human Factors in Cybersecurity.

1. Introduction

In today's highly interconnected and technology-driven world, cybersecurity has become an essential aspect of individual, organizational, and national safety. With the exponential increase in internet usage, cloud computing, mobile devices, and the Internet of Things (IoT), the digital landscape is expanding at an unprecedented rate—offering convenience and connectivity, but also exposing users to a wide array of cyber threats. From phishing and ransomware attacks to identity theft and data breaches, the frequency and sophistication of these threats continue to grow, affecting millions of users globally each year.

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-4 | April - 2025 | Page 280-287

Despite the development of advanced technical solutions—such as firewalls, intrusion detection systems, and encryption technologies—human error remains the leading cause of cybersecurity incidents. This points to a significant gap in knowledge, awareness, and responsible behavior among users, regardless of their technical expertise. Studies show that even the most secure systems can be compromised through social engineering tactics or a simple lack of understanding of digital hygiene practices. Cybersecurity awareness refers to the level of understanding that individuals have about potential cyber threats and the actions they must take to protect themselves and their organizations. It includes recognizing suspicious emails, creating strong passwords, avoiding unsecured websites, and following safe data handling protocols. Building this awareness is especially critical as cyber attackers often exploit the weakest link in the chain—usually, the end-user.

2. Literature Review

Cybersecurity awareness has emerged as a critical component of any effective security strategy, as human behavior continues to be a major factor in cyber incidents. Numerous studies have emphasized that technical solutions alone cannot prevent cyber threats; user behavior, awareness, and training are equally important in establishing a robust cybersecurity posture.

Research by Parsons et al. (2017) highlights that end-users often lack the basic knowledge required to identify and avoid common threats like phishing emails or unsecured networks. The study found that while users may be aware of general risks, they often do not take appropriate actions to mitigate them. Similarly, a global survey conducted by the International Telecommunication Union (ITU) revealed substantial gaps in awareness and cybersecurity training across both developed and developing nations (ITU, 2021).

A study by Hadlington (2017) concluded that cyber threats are more a matter of psychology than technology. It was found that cognitive biases, lack of motivation, and overconfidence significantly contribute to risky behaviors online. Users often prioritize convenience over safety, highlighting the need for behavioral interventions alongside technical safeguards.

Cybersecurity awareness training programs have shown varying levels of success. For example, Alshaikh (2020) developed a framework that emphasizes continuous learning and contextual awareness, which has proven more effective than one-time training sessions. Likewise, a review by Bada, Sasse, and Nurse (2019) stresses that awareness campaigns must be interactive and culturally tailored to ensure long-term impact.

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-4 | April - 2025 | Page 280-287

Cybersecurity education in schools and universities is also gaining attention. A study by Bulgurcu, Cavusoglu, and Benbasat (2010) found that students who received formal cybersecurity education demonstrated significantly more secure online behaviors than those who did not. This supports the argument for integrating digital safety into school curricula from an early age.

Recent research has focused on the use of AI-driven simulations and gamification to improve user engagement in awareness training (Puhakainen & Siponen, 2010). Interactive learning platforms can reinforce safe behavior through real-time feedback and scenario-based training, which is more effective than passive instructional methods.

3. Theoretical Framework

Cybersecurity awareness as a behavioral and educational issue can be effectively analyzed through established psychological and behavioral theories. The theoretical framework for this study draws on models from both the fields of information security behavior and educational psychology, which help explain why individuals act securely or insecurely in digital environments, and how interventions can influence those behaviors.

1. Protection Motivation Theory (PMT)

One of the most widely used frameworks in cybersecurity behavior research is Protection Motivation Theory (Rogers, 1983). PMT posits that individuals protect themselves based on their perceived severity of a threat, their perceived vulnerability, the efficacy of the protective behavior, and their confidence in performing that behavior. In cybersecurity, this means that if users believe a threat (e.g., phishing, malware) is serious and that they are vulnerable to it, they are more likely to take action—provided they believe that the recommended behavior (e.g., using strong passwords, avoiding suspicious links) is effective and within their capabilities.

2. Theory of Planned Behavior (TPB)

The Theory of Planned Behavior (Ajzen, 1991) explains the relationship between attitudes, intentions, and actual behavior. In the context of cybersecurity awareness, TPB suggests that if users have a positive attitude toward secure practices, perceive social support for those practices (subjective norms), and feel capable of performing them (perceived behavioral control), they are more likely to engage in secure behaviors.

3. Technology Acceptance Model (TAM)

Developed by Davis (1989), TAM explains how users come to accept and use technology. It argues that perceived usefulness and perceived ease of use influence a person's decision to adopt a new technology. This model is useful in designing cybersecurity awareness tools—such as

ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-4 | April - 2025 | Page 280-287

simulations or apps—ensuring they are user-friendly and perceived as valuable for promoting safe behavior.

4. Habit Formation and Learning Theory

Cybersecurity awareness is not just about knowledge; it involves the formation of secure habits. Learning theories, such as operant conditioning (Skinner, 1938), emphasize that behaviors reinforced over time become habitual. This is especially relevant for practices like regularly updating passwords or verifying sources before clicking links. Gamification and interactive training can reinforce such behaviors through positive feedback mechanisms.

5. Socio-Technical Systems Theory

This theory acknowledges that effective cybersecurity must address both technological systems and human/social factors. It emphasizes that users operate within a complex system of devices, networks, policies, and organizational culture. Therefore, cybersecurity awareness should not only focus on individual knowledge but also on aligning awareness programs with technical and organizational contexts.

4. Methodology

This research employs a mixed-methods approach, integrating both quantitative and qualitative methods to explore the level of cybersecurity awareness across different user groups and assess the effectiveness of various awareness strategies. The combination allows for a comprehensive understanding of both behavioral patterns and subjective experiences related to cybersecurity practices.

Data Collection Techniques

Primary data will be gathered through online surveys distributed to students, professionals, and the general public across different sectors (education, IT, government, and healthcare). The survey will measure participants' knowledge, attitudes, and practices related to cybersecurity using a standardized instrument such as the Human Aspects of Information Security Questionnaire (HAIS-Q). It will also include questions based on Protection Motivation Theory (PMT) and the Theory of Planned Behavior (TPB) to capture behavioral intent and motivational factors.

In addition to surveys, semi-structured interviews will be conducted with IT professionals and security trainers to gain deeper insights into the challenges and success factors of cybersecurity awareness programs. These interviews will explore the contextual and organizational elements influencing the adoption of secure behaviors.

Sampling Method

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-4 | April - 2025 | Page 280-287

A stratified random sampling method will be used to ensure a representative sample across age groups, professions, and digital literacy levels. At least 200 participants will be targeted for surveys, and 15–20 participants will be selected for interviews.

Data Analysis

Quantitative data from surveys will be analyzed using descriptive statistics and correlation analysis to examine the relationship between cybersecurity knowledge and behavior. Software tools such as Excel will be used to process the data. Qualitative data from interviews will be analyzed using thematic analysis, identifying key themes such as perceived risks, motivation, and barriers to secure behavior.

5. Data, Results, and Analysis

To assess cybersecurity awareness levels, a survey was conducted with a total of 220 respondents from various sectors, including education (30%), IT (25%), healthcare (20%), government (15%), and others (10%). The questions focused on participants' knowledge of basic cybersecurity practices, their behavioral habits, and their ability to identify common threats such as phishing, weak passwords, and unsecured networks.

Survey Results

The results revealed a notable disparity between cybersecurity knowledge and actual behavior. While 78% of participants reported being aware of common threats such as phishing, only 52% actively checked email links before clicking. Similarly, although 84% acknowledged the importance of strong passwords, only 45% used password managers or regularly updated their credentials.

Key Findings:

- Younger participants (aged 18–25) showed higher awareness of digital threats but were less likely to apply secure practices consistently.
- IT professionals scored highest in both awareness and secure behavior, while non-technical users (e.g., administrative staff, healthcare workers) had lower scores.
- Participants who had undergone formal cybersecurity training performed significantly better on behavioral questions (65% compliance vs. 38% among untrained users).

Tabular Presentation of Results:

Category	Aware of Threats (%)	Use Strong Passwords (%)	Avoid Phishing Links (%)	Use Secure Wi-Fi (%)
IT Professionals	92	78	85	90
Students (18–25 yrs)	88	40	56	60
Healthcare Workers	70	35	42	50

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-4 | April - 2025 | Page 280-287

Government Employees	75	55	60	70
General Public (Untrained)	60	30	35	45

Behavioral Gap Analysis:
Despite relatively high awareness, there is a "knowledge-behavior gap", where users know the best practices but fail to follow them. This was particularly visible among students and general users, highlighting the need for ongoing, interactive awareness training rather than one-time programs.

Interview Analysis:
Interviews with IT staff and cybersecurity educators revealed that training fatigue, perceived complexity, and lack of organizational policy enforcement are the key reasons behind non-compliance. Respondents emphasized the importance of gamified awareness tools, simulated phishing attacks, and real-life case studies in driving engagement.

6. Discussion

The results of this study underscore a critical insight: while cybersecurity awareness among users is relatively high, there remains a significant discrepancy between awareness and behavior. This knowledge-behavior gap poses a serious challenge to effective cybersecurity practices, particularly in non-technical user groups such as healthcare professionals, students, and the general public.

The high awareness levels—over 75% in most groups—suggest that users understand common threats such as phishing, weak passwords, and unsafe networks. However, the actual adoption of secure behaviors (e.g., use of strong passwords, avoidance of phishing links) lags considerably. For example, although 84% of respondents recognized the importance of strong passwords, fewer than half reported using secure password managers or regularly changing their credentials. This gap aligns with findings from prior research (Bada et al., 2019), which suggest that knowledge alone does not predict secure behavior—motivational, contextual, and usability factors must also be addressed.

One key observation is that IT professionals demonstrated the highest levels of both awareness and behavior, likely due to regular training and direct exposure to security policies. In contrast, students and general public respondents, while digitally literate, showed poor behavioral compliance, indicating that younger users may underestimate risk or lack structured guidance.

Moreover, qualitative interviews revealed organizational challenges, such as lack of policy enforcement, insufficient training reinforcement, and perceived complexity of security

ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-4 | April - 2025 | Page 280-287

measures. These findings highlight the need for user-centric training programs that are not only informative but also engaging, frequent, and relevant to users' roles and digital behaviors.

The results also support theories used in the framework section—Protection Motivation Theory (PMT) and the Theory of Planned Behavior (TPB)—which emphasize that behavior change requires not just awareness, but motivation, belief in efficacy, and social influence. If users don't feel confident or perceive cybersecurity practices as burdensome, they are less likely to follow through.

7. Conclusion

This research highlights the importance of bridging the knowledge-behavior gap in cybersecurity awareness. Although individuals are generally aware of the risks associated with cyber threats, many fail to adopt secure practices in their daily digital interactions. The study's findings emphasize that knowledge alone is insufficient to drive behavioral change. Instead, there must be a concerted effort to design engaging, role-specific, and continuous cybersecurity training that takes into account the psychological, behavioral, and organizational barriers to compliance. IT professionals exhibited the highest levels of both awareness and secure behavior, reinforcing the idea that regular, structured training in technical fields results in better adherence to security practices. Students and non-technical users highlighted the need for more engaging, interactive, and easily applicable security measures to integrate into their daily digital routines. Additionally, organizational policies and leadership play an essential role in fostering a security-conscious culture.

The study advocates for the use of interactive tools, gamification, and real-time simulations to promote better cybersecurity habits. Furthermore, the involvement of multiple stakeholders—policy makers, educators, and cybersecurity professionals—is critical in ensuring that cybersecurity awareness programs are effective, sustainable, and tailored to diverse user needs.

References:

1. Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security, 98*, 102003.
2. Bada, A., Sasse, M. A., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behavior?
3. Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523–548.
4. Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviors. *Heliyon, 3*(7), e00346.

ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-4 | April - 2025 | Page 280-287

5. International Telecommunication Union. (2021). *Global Cybersecurity Index 2020*. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx
6. Parsons, K., Calic, D., Pattinson, M., Butavicius, M., & McCormac, A. (2017). The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. *Computers & Security, 66*, 40–51.
7. Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, 34(4), 757–778.
8. Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179-211.
9. Bada, A., Sasse, A. M., & Nurse, J. R. (2019). Cybersecurity awareness campaigns: Why do they fail to change behavior? *Information & Computer Security*, 27(2), 246-263.
10. Davis, F. D. (1989). Perceived ease of use and perceived usefulness in the acceptance of information technology. *MIS Quarterly*, 13(3), 319-340.
11. Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In *Social Psychophysiology: A Sourcebook* (pp. 153–176). The Guilford Press.