International Journal of Information System & Innovation Technology 2(2) (2023) 13-18

IJISIT

http://ejournal.enlightenlearner.com

User-Centric Security Education and Awareness for Web Users

Tandhy Simanjuntak, Boston University, USA
Correspondence: E-mail: tandhysimanjuntak@gmail.com

Article Info

Article history:

Received November 15, 2023
Revised December 15, 2023
Accepted December 20, 2023

Keywords:

Web,
Cyber,
Security,
Users

ABSTRACT

As people rely more heavily on web-based services, everyday online activities increasingly involve exposure to cybersecurity risks such as phishing, malware, identity theft, weak password practices, and social engineering attacks. Although technical security tools continue to improve, many incidents still occur because users do not always recognize threats or know how to respond safely. This study examines the importance of user-centric security education and awareness in strengthening the online safety practices of web users. A qualitative literature-based approach was used to review common web security threats, user-related vulnerabilities, and awareness strategies that can reduce risky online behavior. The discussion shows that cybersecurity education is more effective when it is practical, continuous, interactive, and adjusted to user characteristics such as digital literacy, age, and professional context. The study concludes that user-centered awareness programs should become an essential part of cybersecurity strategies because informed users can serve as an important first line of defense against online threats.

1. INTRODUCTION

Web technologies have become deeply embedded in everyday life. People use online platforms to communicate, work, shop, learn, access financial services, and manage personal information. This growing dependence on digital services has created many benefits, but it has also increased users' exposure to cybersecurity threats. Phishing emails, malicious links, fake websites, malware, identity theft, and credential theft are now common risks faced by web users [1], [2].

For many years, cybersecurity has often been treated mainly as a technical problem. Organizations invest in firewalls, antivirus software, encryption, authentication systems, and monitoring tools to protect digital assets. These technologies are important, but they cannot fully prevent security incidents when users make unsafe decisions online. A single click on a deceptive link or the use of a weak password can compromise an otherwise well-protected system [3].

This situation shows that human behavior is a central part of cybersecurity. Users are not only potential victims of cyberattacks but also active participants in maintaining digital safety. When users understand

cyber risks and develop secure habits, they can help reduce the likelihood of security incidents. In contrast, users with limited awareness may unintentionally expose themselves or their organizations to serious risks.

Among the various threats faced by web users, social engineering is especially difficult to manage. Unlike attacks that rely mainly on technical weaknesses, social engineering targets human judgment. Attackers may use urgency, fear, curiosity, trust, or authority to persuade users to reveal confidential information, download harmful files, or visit fraudulent websites. This type of attack remains effective because it adapts to human emotions and daily communication patterns [4].

Security education and awareness programs are therefore necessary to improve users' ability to recognize threats and respond appropriately. However, not all awareness programs are equally effective. Some programs are delivered only once, focus mainly on rules, or use generic materials that do not reflect users' real online experiences. Such approaches may increase knowledge temporarily but may not lead to lasting behavioral change.

A user-centric approach offers a more practical direction. Instead of treating all users as having the same needs, user-centric security education considers differences in digital literacy, age, work context, prior experience, and online behavior. Training becomes more meaningful when users can connect the material with the situations they actually face, such as suspicious emails, unsafe websites, password reuse, or privacy risks on social media [5].

Based on this background, this study discusses user-centric security education and awareness for web users. The purpose of the study is to examine how awareness programs can improve online safety practices and reduce user vulnerability to cyber threats. This paper focuses on common web security threats, the role of user behavior, the importance of practical awareness strategies, and recommendations for improving cybersecurity education.

2. METHODS

This study uses a qualitative literature review approach. This method was selected because the research focuses on understanding existing concepts, findings, and practices related to cybersecurity awareness, user behavior, and social engineering prevention.

2.1 Research Design

The study was designed as a conceptual and literature-based analysis. The discussion was developed by reviewing academic publications, cybersecurity references, and awareness-related studies that explain how users respond to cyber threats and how education can improve secure behavior.

2.2 Data Sources

The data sources used in this study include academic books, journal articles, cybersecurity studies, and publications related to web security, information security behavior, phishing prevention, and user awareness. These sources were selected because they provide relevant explanations of both technical and human aspects of cybersecurity.

2.3 Research Procedure

The research procedure was conducted in four stages. First, common threats faced by web users were identified from the literature. Second, user-related vulnerabilities were examined, particularly those connected to password habits, phishing susceptibility, careless information sharing, and lack of

awareness. Third, existing security education strategies were reviewed to understand which approaches are more likely to support behavioral improvement. Finally, the findings were synthesized into recommendations for user-centric cybersecurity awareness programs.

2.4 Analysis Technique

The literature was analyzed thematically. Several themes were used to organize the discussion, including web security threats, human factors in cybersecurity, social engineering, user awareness, demographic differences, and organizational security culture. Through this thematic analysis, the study identifies how education and awareness can contribute to safer online behavior.

3. RESULTS AND DISCUSSION

3.1 Common Security Threats Faced by Web Users

The review shows that web users face a wide range of security threats. Phishing is one of the most frequent threats because it uses deceptive messages to trick users into giving away sensitive information such as usernames, passwords, or banking details. Malware is also a major concern, especially when users download files from untrusted sources or click links that lead to infected websites.

Password-related risks remain common. Many users continue to reuse passwords across multiple services or choose passwords that are easy to guess. This behavior increases the impact of a single credential leak because attackers may use the same credentials to access several accounts. Identity theft and online scams also remain serious risks, especially when users share personal information without checking whether a website or message is legitimate.

Social engineering is particularly dangerous because it does not always look like a technical attack. It may appear as a normal email from a trusted institution, a message from a colleague, or an urgent request from a service provider. This makes user awareness essential. If users are not trained to pause, verify, and question suspicious requests, they may unknowingly assist attackers.

3.2 The Role of User Awareness in Cybersecurity

The findings suggest that user awareness can significantly reduce cybersecurity risks. Users who understand common attack patterns are more likely to recognize suspicious links, avoid unsafe downloads, use stronger passwords, and report possible incidents. Awareness helps users move from passive technology users to active participants in digital protection.

However, awareness alone does not always lead to secure behavior. Some users may understand the risks but still ignore security practices because of convenience, time pressure, or overconfidence. For example, a user may know that password reuse is unsafe but continue doing it because it is easier to remember one password. This gap between knowledge and behavior shows that security education must go beyond simply providing information.

Effective cybersecurity education should therefore focus on practical habits. Users need repeated exposure to realistic examples, opportunities to practice decision-making, and reminders that support secure behavior over time. In this sense, awareness should be treated as a continuous process rather than a one-time activity.

3.3 Effectiveness of User-Centric Security Education

User-centric security education is more effective when the learning content is connected to users' daily digital activities. For instance, employees may benefit from phishing simulations that resemble workplace emails, while students may need guidance on protecting academic accounts, social media profiles, and personal devices.

Interactive methods also appear more useful than purely lecture-based approaches. Simulations, short quizzes, case studies, role-play scenarios, and practical demonstrations can help users understand how cyberattacks occur in real situations. These methods encourage users to think critically and practice safer responses rather than merely memorizing security rules.

Another important aspect is continuity. A single awareness session may temporarily increase knowledge, but users can forget the information if it is not reinforced. Regular training, reminders, and updated examples are needed because cyber threats continue to change. A user-centric program should therefore be flexible enough to adapt to new risks and user needs.

3.4 Influence of Demographic and Contextual Factors

The effectiveness of security education may differ among user groups. Age, educational background, digital literacy, professional role, and frequency of Internet use can influence how users understand and respond to cybersecurity messages. Users with strong digital skills may prefer more advanced explanations, while users with limited experience may need simple language, clear examples, and step-by-step guidance.

This variation suggests that cybersecurity awareness should not rely on a one-size-fits-all model. Training materials should be adjusted to the audience. For example, employees handling sensitive organizational data may require more detailed guidance on data protection and phishing response, while general web users may need practical advice on password management, privacy settings, and safe browsing.

Context also matters. A user's behavior at work may be different from behavior at home. In the workplace, policies and monitoring may influence security behavior. At home, users may rely more on personal judgment. Therefore, awareness programs should help users develop secure habits that can be applied across different digital environments.

3.5 Organizational Culture and Security Behavior

In organizational settings, user behavior is strongly shaped by culture. If cybersecurity is treated only as an IT department responsibility, users may not feel personally responsible for protecting information. On the other hand, when leaders and managers consistently promote cybersecurity, users are more likely to take security practices seriously.

A strong security culture includes clear policies, regular communication, accessible reporting channels, and supportive responses when users report suspicious activities. Users should not feel afraid to report mistakes or possible threats. Instead, reporting should be encouraged as part of responsible digital behavior.

Security education works best when it is supported by this kind of culture. Training can provide knowledge, but culture reinforces behavior. When awareness, policies, and leadership support work together, users are more likely to develop secure routines.

3.6 Recommendations for Security Awareness Programs

Based on the discussion, several recommendations can be proposed. First, cybersecurity awareness training should be conducted regularly, not only during onboarding or after incidents. Second, training should use practical examples that reflect real threats faced by users. Third, materials should be adjusted to the needs and abilities of different user groups. Fourth, organizations should support awareness programs with clear policies and simple reporting mechanisms. Finally, the effectiveness of awareness programs should be evaluated periodically to determine whether they improve not only knowledge but also behavior.

These recommendations show that user-centric security education is not merely about delivering information. It is about helping users build habits, confidence, and responsibility in digital environments.

4. CONCLUSION

This study emphasizes that cybersecurity is not only a matter of technology but also a matter of human behavior. Web users face many threats, including phishing, malware, password attacks, identity theft, scams, and social engineering. While technical security tools remain important, they cannot fully protect users who are unaware of risks or unsure how to respond to suspicious activities.

The discussion shows that user-centric security education can improve online safety practices by making cybersecurity knowledge more practical, relevant, and easier to apply. Training is more effective when it is continuous, interactive, and adapted to user characteristics such as digital literacy, age, and professional context. In organizations, awareness programs should also be supported by a strong security culture that encourages responsible behavior and threat reporting.

Future research may conduct empirical studies using surveys, experiments, or training evaluations to measure how user-centric awareness programs influence actual behavior over time. Such studies would provide stronger evidence for designing cybersecurity education that is both practical and sustainable.

5. ACKNOWLEDGMENT

The author would like to thank the academic and cybersecurity research community whose work has contributed to the development of this study.

6. REFERENCES

[1] M. E. Whitman and H. J. Mattord, *Principles of Information Security*, 7th ed. Boston, MA, USA: Cengage, 2021.

[2] W. Stallings, *Effective Cybersecurity: A Guide to Using Best Practices and Standards*. Boston, MA, USA: Addison-Wesley, 2019.

[3] S. Furnell and M. Bishop, "Human aspects of information security and assurance," *Computers & Security*, vol. 67, pp. 1–2, 2017.

[4] A. Algarni, Y. Xu, and T. Chan, "The role of security awareness in combating phishing attacks," *Information & Computer Security*, vol. 30, no. 2, pp. 212–228, 2022.

[5] M. Parsons et al., "The human aspects of information security questionnaire," *Computers & Security*, vol. 42, pp. 165–176, 2014.