

СЕКЦІЯ 31.

КОМП'ЮТЕРНА ІНЖЕНЕРІЯ, КІБЕРБЕЗПЕКА ТА СИСТЕМНІ ТЕХНОЛОГІЇ

Zhuk Yevheniia Yuriivna, Higher Education Student, Faculty of Cybersecurity
Kharkiv National University of Radio Electronics; Ukraine

Scientific supervisor: Bukovska Inna Yuriivna, Senior Lecturer, Department of
Foreign Languages
Kharkiv National University of Radio Electronics; Ukraine

THE HUMAN FACTOR IN CYBERSECURITY: ENHANCING USER AWARENESS AND DIGITAL HIGIENE

In the context of rapid digitalization and the widespread adoption of online learning, cybersecurity has become a critical issue for higher education institutions. While technical security measures provide foundational protection for information systems, their overall success heavily depends on users and the choices they make in daily digital scenarios. Password management, handling sensitive data, software installation, and adherence to security policies directly impact the level of protection. For this reason, cybersecurity in higher education must address both technical controls and how students apply security practices in their daily routines.

A key challenge is the discrepancy between knowing a security rule and actually complying with it. Users often understand what is expected of them, yet act differently in real-life situations. This frequently happens when security requirements are difficult to grasp, take too much time, or interfere with routine tasks. Continuous exposure to such demands can trigger “security fatigue”, where users grow tired of protective procedures and start viewing them as obstacles. As a result, some recommendations are ignored and certain security steps are avoided. Therefore, cybersecurity education should prioritize practices that are clear, manageable, and suitable for everyday use, rather than relying solely on passing on theoretical information [2].

The daily practices of university students highlight the relevance of this issue. A survey of 141 students aged 17-21 at the Bath Spa University Academic Centre RAK included participants from Creative Computing, Business and Management, and Psychology. The findings revealed that 38.46% of respondents reused passwords across different accounts, while 44% shared their passwords with others. Additionally, 77% stored passwords directly on their devices – such as in emails, documents, contacts, or notes. Furthermore, 51% of students failed to recognize the importance of reviewing user agreements before accepting them during software installation [3].

Clear differences were also noted between student groups. More than 80% of respondents studying Business and Management or Psychology reported saving passwords on their devices, compared to 71% of Creative Computing students. Password sharing was reported by 32% of Creative Computing students, 52% of Business and Management students, and 59% of Psychology students. At the same time, 90% of all participants expressed an interest in learning more about cybersecurity. These results confirm that an interest in cybersecurity does not automatically translate into secure daily habits. This makes the practical focus and content of cybersecurity education especially important for students from diverse academic backgrounds [3].

The relationship between cybersecurity knowledge and awareness was also analyzed among university students in Dhaka, Bangladesh. The study gathered 430 initial responses, of which 19 were excluded, leaving 411 valid questionnaires. Researchers evaluated cybersecurity knowledge, password security, self-perceived skills, cybersecurity attitude, and cybersecurity awareness using Partial Least Squares Structural Equation Modeling (PLS-SEM) via SmartPLS 3.3.9 [1].

Cybersecurity knowledge demonstrated a statistically significant positive direct effect on cybersecurity awareness (coefficient 0.137). Password security was likewise positively linked with awareness (coefficient 0.223). However, self-perception of skills showed a very different outcome. Its direct effect was weak and statistically insignificant (coefficient 0.038). Consequently, students who feel confident about their cyber skills cannot be assumed to possess higher security awareness. The paper discusses inaccurate self-assessment and a false sense of security, referencing the Dunning-Kruger effect as part of its theoretical background. Nevertheless, the study's empirical results do not indicate that the Dunning-Kruger effect occurred among the participants [1].

Cybersecurity attitude played a key mediating role in the proposed model. The indirect effect between cybersecurity knowledge and awareness through cybersecurity attitude was $\beta = 0.114$ ($p = 0.033$). The corresponding indirect effects for password security and self-perceived skills were $\beta = 0.214$ ($p < 0.001$) and $\beta = 0.194$ ($p = 0.002$), respectively. Overall, the model accounted for 72.3% of the variance in cybersecurity awareness ($R^2 = 0.723$) [1]. This indicates that cybersecurity awareness is connected not only to knowledge and practical habits, but also to user attitudes toward cybersecurity.

The findings of these reviewed studies highlight a major limitation of approaches based strictly on information transfer. Students can be aware of cybersecurity risks while continuing to use unsafe password practices. Similarly, users may know the correct procedure but bypass it when it feels inconvenient or complicated. Cybersecurity education must therefore combine theoretical concepts with practical, real-world tasks that can be easily applied in everyday digital environments [2; 3].

For higher education institutions, cybersecurity training can be integrated directly into scenarios students encounter every day. Password hygiene, credential protection, and decisions made during software installation represent areas where theoretical knowledge can be applied immediately. At the same time, security guidelines should stay simple and easy to follow. Excessively complex requirements reduce user compliance, which diminishes the practical value of security education [2].

A practical method to enhance cybersecurity awareness is incorporating security training directly into students regular academic routines. Short learning modules, realistic

scenarios, and hands-on tasks help students identify common risks and understand how security rules apply to daily situations. This approach can feature exercises on password management, identifying suspicious emails, protecting personal data, and making safer decisions on online platforms. Regular repetition also helps convert isolated security rules into consistent digital habits. This is essential, as awareness alone does not guarantee safe behavior – especially when security steps feel complex or burdensome [2; 3].

Therefore, the human element of cybersecurity must be addressed alongside technical defenses. The available evidence demonstrates that knowledge, password practices, user attitudes, self-perception, and policy usability all influence cybersecurity awareness. Adopting a more practical approach to cybersecurity education will help students move from simply knowing safety rules to applying them consistently in their digital lives.

References

1. Ahamed, B., Polas, M. R. H., Kabir, A. I., Sohel-Uz-Zaman, A. S. M., Fahad, A. A., Chowdhury, S., & Rani Dey, M. (2024). Empowering Students for Cybersecurity Awareness Management in the Emerging Digital Era: The Role of Cybersecurity Attitude in the 4.0 Industrial Revolution Era. *SAGE Open*, 14(1). <https://doi.org/10.1177/21582440241228920>
2. Bada, Maria & Sasse, Angela & Nurse, Jason. (2015). Cyber Security Awareness Campaigns: Why do they fail to change behaviour?. 118-131. <https://doi.org/10.48550/arXiv.1901.02672>
3. Subhani, A., Alam Khan, I., & Ahmad, U. (2023). Importance of Conducting Cyber Security Awareness Sessions among Undergraduate Students. *Journal of Advanced Research in Social Sciences and Humanities*, 8(2). <https://doi.org/10.26500/jarssh-08-2023-0202>