

IMPLEMENTING VIRTUAL HYGIENE AMONG THE POPULATION: AWARENESS OF INVISIBLE DIGITAL THREATS AND PASSWORD SAFETY

Yusupova Shaxzoda

Affiliation: Tashkent University of Information Technologies

Department: Computer Engineering

Year: 2025

Abstract: In the digital era, personal online behavior determines the security and privacy of individuals and society. This paper examines the concept of virtual hygiene — a modern approach to maintaining digital safety through responsible online actions. It focuses on common user mistakes such as password sharing, poor data protection, and the lack of awareness of invisible digital threats. The research explores how ICT-based education programs can improve digital literacy and protect citizens from online risks. Findings suggest that implementing “virtual hygiene” principles in educational systems and public campaigns can significantly reduce cyber vulnerability.

Keywords: Virtual hygiene, ICT education, Cyber awareness, Password safety, Digital literacy, Cyber threats.

1. Introduction

With the rapid development of Information and Communication Technologies (ICT), people’s lives have become more connected and digitized. However, while physical hygiene is a well-understood concept in every household, virtual hygiene remains underrecognized. Millions of users share personal data without realizing the potential risks hidden behind invisible cyber threats such as phishing, malware, and social engineering.

In developing countries, especially, users often lack fundamental digital hygiene skills such as using strong passwords, updating software, and recognizing suspicious links. Therefore, this research emphasizes the need to integrate virtual hygiene awareness into ICT education and public policy.

2. Literature Review

Previous studies have demonstrated that human behavior is one of the weakest links in cybersecurity. According to Alotaibi (2023), over 60% of cyber incidents occur due to poor digital hygiene practices such as password reuse or oversharing information online.

Other researchers (Kumar & Lee, 2022) highlight that invisible threats — such as data tracking, spyware, and background app permissions — remain unnoticed by the average user.

The Organization for Economic Cooperation and Development (OECD, 2024) reports that digital literacy programs focusing on cyber hygiene reduce national cybercrime risks by up to 40%. However, such programs are still rare in many developing nations, including Uzbekistan.

3. Methodology

A quantitative survey was conducted among 200 participants aged 18–45 from Tashkent city. The survey included 15 questions focusing on three key areas:

1. Password management (complexity, reuse, and sharing habits)
2. Awareness of invisible threats (social engineering, phishing, and tracking)
3. General digital behavior (use of two-factor authentication, software updates, etc.)

The collected data were analyzed using descriptive statistics to identify the most frequent unsafe behaviors among respondents.

4. Results and Discussion

The survey revealed that 63% of respondents reused the same password across multiple platforms, while 48% admitted sharing their passwords with friends or family. Additionally, 52% were unaware that mobile applications can access personal data in the background.

These findings indicate a lack of understanding about invisible digital threats. Respondents showed higher concern for visible risks (like hacking) but underestimated indirect dangers (like location tracking and data mining).

To improve this situation, ICT-based awareness campaigns should be launched through schools, universities, and social media platforms. Interactive tools — such as digital hygiene mobile applications and online safety quizzes — can engage users more effectively than traditional lectures. Gamified learning has proven to increase user retention and behavior change in previous studies.

5. Conclusion

The study concludes that virtual hygiene is a vital aspect of modern cybersecurity awareness. As ICT continues to evolve, users must adopt safe digital habits just as they practice physical hygiene in daily life.

The government, educational institutions, and ICT ministries should collaborate to design training programs, integrate digital safety into school curricula, and organize national awareness campaigns.

By promoting a culture of virtual hygiene, societies can significantly reduce online risks and build a safer digital future for all.

References:

1. Alotaibi, A. (2023). Cyber Hygiene Practices in Modern ICT Environments. *Journal of Digital Security*.
2. Kumar, S., & Lee, J. (2022). Invisible Threats: Understanding the Psychology of Cyber Risk. *International Journal of Cyber Studies*.



3. OECD. (2024). Digital Literacy and Cyber Awareness in Developing Nations. OECD Digital Economy Papers.
4. Rahman, N. (2023). ICT-based Education for Cyber Safety. Asian Journal of Information Systems.
5. Smith, D. (2022). From Physical to Virtual Hygiene: A New Perspective on Digital Citizenship. Global ICT Review.