

Cybersecurity Hygiene and Preventive Practices among University Students at Rajarata University of Sri Lanka

D.P.D.A.K. Madhuwantha¹ and D.P.D. Dayananda^{2,*}

*Department of Information Systems, Faculty of Management Studies,
Rajarata University of Sri Lanka, Mihintale, Sri Lanka^{1,2}*

*Corresponding author: piyumidinushini@gmail.com

Abstract

The rapid digitisation of higher education has heightened the importance of cybersecurity hygiene among university students, particularly in developing countries such as Sri Lanka. At Rajarata University, students' frequent use of digital platforms for academic and personal purposes exposes them to increased risks due to poor awareness, inconsistent preventive practices, and limited technological access. Despite this vulnerability, little research has examined the socio-cultural and behavioural dimensions of cybersecurity practices in Sri Lankan universities. Addressing this gap, the present study investigates the factors influencing cybersecurity hygiene and preventive behaviours among undergraduates. Grounded in the Theory of Planned Behaviour (TPB), Protection Motivation Theory (PMT), Technology Acceptance Model (TAM), Health Belief Model (HBM), and Cultural Theory of Risk, the study evaluates the influence of cybersecurity awareness and knowledge, cultural and behavioural attitudes, technological access, and cybersecurity risk perception on students' practices. A quantitative explanatory research design was employed, and data were collected from 367 undergraduates across all six faculties using a structured online questionnaire. Validity and reliability were ensured through pilot testing, and data were analysed using SPSS with descriptive statistics, correlation, and regression analysis. The results show that all four independent variables significantly affect students' cybersecurity hygiene, with cultural and behavioural attitudes exerting the strongest impact. While students demonstrate basic awareness of cyber threats, major gaps remain in procedural knowledge and consistent practices such as password management, phishing recognition, system updates, and safe data handling, which are further exacerbated by limited access to secure technologies and cultural norms discouraging proactive behaviours. The study concludes by recommending targeted cybersecurity education programmes, and institutional policies tailored to the Sri Lankan university context.

Keywords: cultural attitudes, cybersecurity hygiene, preventive practices, risk perception, technological access