A STUDY OF CYBERSECURITY BEHAVIOUR AMONG UNDERGRADUATES OF RAJARATA UNIVERSITY OF SRI LANKA

A.W.D.K. Weerakoon[1, *] and K.M.P.G.A.J. Bandara[2]

[1,2] *Department of Information Systems, Faculty of Management Studies, Rajarata University of Sri Lanka, Mihintale, Sri Lanka*

[*]Corresponding author (email: dushankavindaweerakoon@gmail.com)

INTRODUCTION

Information technology has advanced significantly in recent decades, paralleling the surge in internet use by individuals and organizations. As individuals immerse themselves more in the digital world and share information, especially through social networks, which have become an indispensable part of many people's lives, their privacy is jeopardized due to the ubiquitous use of the internet and electronic devices. While ordinary users often perceive the internet as safe, believing they are immune to threats and are not in attackers' crosshairs, the reality is that cybersecurity is under threat daily. Security threats have become intertwined with technological advancements and the proliferation of internet technologies. People are generally exposed to threats when they engage with information technology in their daily routines. Whether knowingly or unknowingly, they are susceptible to security breaches (Aldossary & Zeki, 2016). Today, the internet is teeming with cybercriminals, including hackers, crackers, pranksters, and cyber terrorists. These actors employ a myriad of methods to commit cyberattacks, such as Denial-of-Service attacks (DoS), hacking, phishing, ransomware, viruses, cyberstalking, and more. Many individuals fall prey due to a lack of awareness about cyber threats and strategies to counteract cybercrimes (Aldossary & Zeki, 2016). This study delves into the current state of cybersecurity behavior among undergraduates in Sri Lanka, shedding light on the challenges they encounter and potential measures to bolster their cybersecurity habits. An exhaustive analysis of various factors influencing cybersecurity behavior among undergraduates is provided, spanning education level, awareness, cultural norms, and government policies. The study also offers suggestions for elevating cybersecurity behavior among Sri Lankan undergraduates. The results unveil a positive correlation between the independent and dependent variables. This insight indicates that one's self-perception of cybersecurity competencies and their grasp of cybersecurity can sway their behavior in this realm. However, there are instances where undergraduates' cybersecurity knowledge and their confidence in their skills are at odds. While undergraduates possess considerable knowledge and exhibit confidence in their cybersecurity abilities, they often don't apply this knowledge and these skills effectively.

METHODOLOGY

This is explanatory research that evaluates the factors affecting cybersecurity behavior. It assesses the effect of self-perception of cybersecurity skills, cybersecurity attitude, and cybersecurity knowledge on the cybersecurity behavior of undergraduates at Rajarata University of Sri Lanka.

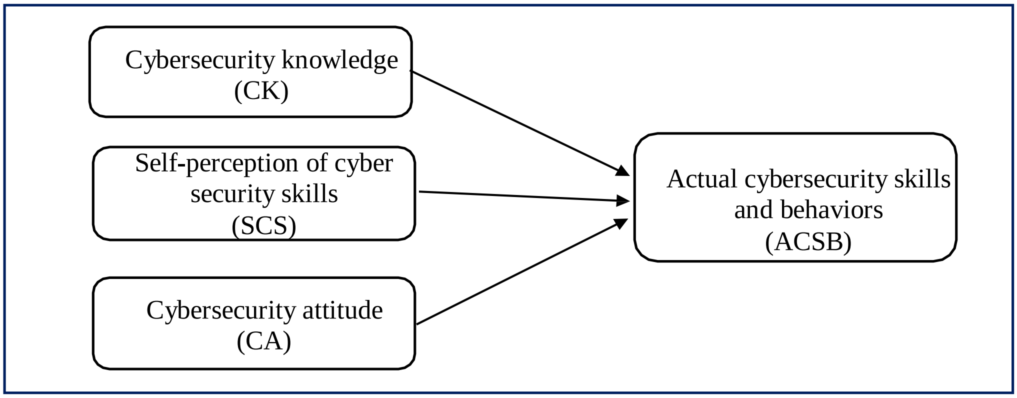
A quantitative method is applied for this study, and essentially, three hypotheses are used to test the nature of the impact between three independent variables and one dependent variable. The survey method is chosen as the strategy for this study, as it is commonly used in deductive research. Since this research aims to investigate the cybersecurity behavior of undergraduates at Rajarata University of Sri Lanka, and data are collected from each individual, treating each student's response as individual data, the unit of analysis is at the individual level.

A structured questionnaire is used to collect primary data. Accordingly, this study is based on primary data gathered from 370 Rajarata University undergraduates, and the stratified sampling method was employed to collect data.

Additionally, data were gathered from previous research studies, documents, papers, magazines, reports, and online published content.

Figure 3

Conceptual Framework of the study


Cybersecurity knowledge (CK)
Self-perception of cyber security skills (SCS)
Cybersecurity attitude (CA)
Actual cybersecurity skills and behaviors (ACSB)

The following hypothesis was developed for the study.

H1: There is a significant positive relationship between undergraduates' cybersecurity knowledge and their actual cybersecurity behavior at Rajarata University of Sri Lanka.

H2: There is a significant positive relationship between undergraduates' self-perception of cybersecurity skills and their actual cybersecurity behavior at Rajarata University of Sri Lanka.

H3: There is a significant positive relationship between undergraduates' cybersecurity attitudes and their actual cybersecurity behavior at Rajarata University of Sri Lanka.

RESULTS AND DISCUSSION

In this study, a descriptive analysis was conducted to identify the basic nature of the research variables. The Mean, Standard Deviation, and Skewness of the dependent and independent variables were calculated. The results are shown in the table below.

According to the table above, all the independent variables (Cybersecurity attitude, Self-perception of cybersecurity skills, Actual cybersecurity knowledge) and the dependent variable (Actual cybersecurity behavior) are generally distributed, as their Skewness values are close to 0.

The correlation table shows the relationship between each variable and other variables, including the dependent variable. Consequently, the correlation matrix can assist the researcher in determining the relationships among variables. The table above elucidates this. The correlation coefficient ranges between -1 and +1. A value of -1 represents a completely negative relationship, while +1 indicates a completely positive relationship between variables.

Table 1
Relationship between cyber security knowledge and Actual cyber security behavior

	ACSB	CK	SCS	CA
ACSB	1			
CK	0.183**	1		
SCS	0.183**	0.076	1	
CA	0.064	0.025	0.115	1

N = 370, **P<0.01

According to Table 1, the Pearson correlation value for undergraduates' cybersecurity knowledge to actual cybersecurity behavior was 18.3%, indicating a weak positive relationship between the variables mentioned above. The significance value in the table above is 0.000 (P<0.01), indicating that both variables are significant at the 0.01 level. Consequently, there was a statistically weak but positive relationship between the self-perception of cybersecurity skills and actual cybersecurity behavior.

It is accepted that a significance value of less than 0.05 is required for the correlation to be considered significant.

According to Table 1, the Pearson correlation value for undergraduates' self-perception of cybersecurity skills to actual cybersecurity behavior was 18.3%, indicating a weak positive relationship between the aforementioned variables. The significance value in the table is 0.000 (P<0.01), indicating that both variables are significant at the 0.01 level.

Consequently, there was a statistically weak but positive relationship between the self-perception of cybersecurity skills and actual cybersecurity behavior.

It is accepted that a significance value of less than 0.05 is required for the correlation to be considered significant.

According to Table 1, the Pearson correlation value between undergraduates' cyber security attitudes and actual cyber security behavior was 6.4%. The significance value in the table is 0.222 (P>0.01). As a result, statistically, there was no relationship between cyber security attitude and actual cyber security behavior. It is generally accepted that a significance value of less than 0.05 is required for the correlation to be considered significant.

As previously mentioned, a five-point Likert scale has been used in this study, with a mean value of 3. Based on this, the following decision rules can be formulated:

According to the table, the mean value for Cyber security attitude is 3.9903, and it is negatively skewed (-1.827). This indicates that respondents have a favorable cyber security attitude. The mean value for the self-perception of cyber security behavior is 3.9292 and it is negatively skewed (-2.192). This suggests that respondents have a positive self-perception of cyber security behavior. Furthermore, the mean value for cyber security knowledge is 3.9292, with a skewness value of -2.192, indicating that respondents possess good cyber security knowledge.

Moreover, the mean value for actual cyber security behavior is 2.3130, which is relatively low, suggesting that respondents may not exhibit strong actual cyber security behaviors.

CONCLUSION AND IMPLICATIONS

The study provides an in-depth analysis of various factors that influence cybersecurity behavior among undergraduates, including education level, awareness, cultural norms, and government policies. The paper offers recommendations for enhancing undergraduate cybersecurity behavior in Sri Lanka. The results revealed a positive relationship between independent and dependent variables. This finding suggests that the self-perception of cybersecurity skills and cybersecurity knowledge can influence cybersecurity behavior. However, undergraduates' cybersecurity knowledge and self-perception of cybersecurity skills sometimes contradict each other. Undergraduates possess significant knowledge and are confident about their cybersecurity skills; however, they do not always put their knowledge and skills into practice. Moreover, there was a positive, albeit weak, relationship between the self-perception of cybersecurity skills and actual cybersecurity behavior. Self-perception of the ability to manage positive and negative affect is associated with high efficacy in managing one's educational development and resisting temptations to engage in anti-social activities such as computer misuse. Statistically, there was a weak but positive relationship between the self-perception of cybersecurity skills and actual cybersecurity behavior.

In the context of this research, students are advised to prioritize the enhancement of their cybersecurity practices. It is of utmost importance that they establish robust, unique passwords, activate two-factor authentication whenever available, and consistently update their software to address known vulnerabilities. Students should exercise vigilance in recognizing and avoiding phishing attempts, secure their Wi-Fi networks, and use encrypted communication methods for sensitive discussions. Additionally, they must consistently practice sound digital hygiene, which includes limiting the sharing of personal information, downloading content cautiously, and staying informed about the evolving landscape of cybersecurity threats. By adhering to these recommendations, students can actively contribute to safeguarding their digital identities and information, fostering a more secure online environment.

Researchers recommend several policy measures to enhance cybersecurity behavior among undergraduates. Firstly, policymakers should advocate for the integration of cybersecurity education within university curricula. This would encourage educational institutions to develop cybersecurity courses or modules that cover essential concepts and practical skills, ensuring that students navigate the digital landscape securely. Secondly, allocating funding for cybersecurity resources within universities is crucial. These resources can include cybersecurity training programs, workshops, and readily accessible materials. Adequate financial support is essential to equip students with the tools and knowledge they need to develop strong cybersecurity habits

Keywords: Cybersecurity attitude, cybersecurity knowledge, cybersecurity skills and behaviors, security threats

REFERENCES

Aldossary, A. A., & Zeki, A. M. (2016). Web user’ knowledge and their behavior towards security threats and vulnerabilities. Proceedings - 2015 4th International Conference on Advanced Computer Science Applications and Technologies, ACSAT 2015, 256–260. https://doi.org/10.1109/ACSAT.2015.51

Ani, U. D., He, H., & Tiwari, A. (2019). Human factor security: Evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology,* 21(1), 2–35. https://doi.org/10.1108/JSIT-02-2018-0028

Ahmed, I. N. I. (2018). Information security awareness amongst students in IIUM. http://210.48.222.250/bitstream/handle/123456789/5416/1/t11100384890IbrahimNasreldin_SEC_24.pdf

Slusky, L., & Partow-Navid, P. (2012). Students information security practices and awareness. *Journal of Information Privacy and Security*, 8(4), 3–26. https://doi.org/10.1080/15536548.2012.10845664

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems,* 62(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269