Battling the Silent Invaders: The Alarming Impact of Computer Viruses on Student Laptops and Effective Protection Strategies

Melca Abogado*
Southern Leyte State University -Tomas Oppus , Southern Leyte, Philippines
E-mail: abogadomica1298@gmail.com

Efren I. Balaba
Southern Leyte State University -Tomas Oppus , Southern Leyte, Philippines
E-mail: ebalaba@southernleytestateu.edu.ph
*Corresponding Author

Received: *06/06/2025* ***Revised :*** *23/06/2025* ***Accepted:*** *26/06/2025*

Abstract

The aim of the present study is to examine the impact of computer viruses on student computers or laptops and to explore the preventive measures students adopt to protect their devices. In the digital era, students increasingly rely on electronic devices for learning, communication, and entertainment. However, this dependence exposes them to various cyber threats, including malware infections, cyber-attacks, data breaches, and digital terrorism. The findings indicate that although a majority of students are aware of the risks posed by malware, only a minority actively engage in protective practices, such as regularly updating software or using strong and secure passwords. Alarmingly, 33% of the surveyed students reported experiencing malware infections. Furthermore, the study reveals a high level of interest in cybersecurity education, with 93% of participants expressing a desire to learn more about digital safety and data protection. These findings highlight the urgent need for targeted awareness campaigns and the integration of cybersecurity education into student curricula.

Keywords: Cybersecurity, Computer Viruses, Malware Infections

Introduction

The study "Battling the Silent Invaders: The Alarming Impact of Computer Viruses on Student Laptops and Effective Protection Strategies" explores the growing threat that computer viruses pose to student laptops. With students increasingly relying on laptops for academic tasks, research, and communication, the risk of malware infections has become a significant concern. Malware infections can lead to security breaches, data loss, and system vulnerabilities, making it critical for students to adopt strong cybersecurity practices. Earlier studies, such as Am I Secured: A Computer Virus Awareness among BSIT Students, have emphasized the need for better cybersecurity awareness among students to safeguard their devices.

While advancements in cybersecurity have been made, students' laptops stay highly susceptible to infections due to unsafe browsing habits, phishing frauds, and outdated software. Research like Effect of Virus on Computer Systems: A Survey of Student's Perception, Journal of Computer Science, and Its Application, AJOL highlights that most students lack awareness of the risks, leaving their devices vulnerable. Moreover, even schools with comprehensive security systems struggle with cyber-attacks, as shown in the

study "Cyber Viruses Infect Schools Across Nation", which underscores the need for more student- specific solutions. This study aims to address gaps in the current understanding of how students specifically manage virus infections. The research will investigate common infection sources, such as weak passwords, outdated antivirus software, and risky online behaviors. A key focus will be on evaluating students' awareness of cybersecurity best practices and their responses to infections. Despite research on general malware defense strategies, few studies delve into the unique challenges students face, such as limited access to premium security software and reliance on public networks.

Research Questions

1.What are students' current cybersecurity practices and habits related to malware prevention?

2.How effective are students' responses to malware infections on their laptops?

3.What is the level of awareness among students about virus threats and preventive measures?

Based on the findings, this study will propose a set of practical guidelines to help students improve their cybersecurity awareness. These guidelines will aim to reduce the risk of infection and equip students with the knowledge and tools needed to protect their laptops from evolving cyber threats. The results of this study could serve as the foundation for developing cybersecurity training programs tailored specifically to students, making it easier for them to implement effective protection strategies.

Framework

This study examines how malware infiltrates systems, the factors influencing students' security behaviors, and the effectiveness of protective measures. The framework integrates key cybersecurity principles and theories to explain how students assess risks and adopt protective strategies. The aim is to understand the psychological and behavioral factors that shape students' cybersecurity practices and guide the recommendations of the study.

1.Protection Motivation Theory (PMT)

Protection Motivation Theory (PMT) suggests that individuals evaluate threats based on their perceived severity (how dangerous a virus is) and perceived vulnerability (how likely they are to be infected). According to PMT, students' motivation to protect their laptops depends on how seriously they perceive malware threats and their vulnerability to these threats.

The results of this study reveal that while most students are aware of malware risks, most do not implement adequate protective measures, such as software updates or stronger passwords. This aligns with PMT's idea that while students recognize the severity of threats, their sense of vulnerability or their belief in their ability to avoid infection may not be high enough to drive preventive actions.

2.Risk Compensation Theory (RCT)

Risk Compensation Theory suggests that individuals may take riskier actions when they feel protected by security measures, such as antivirus software or firewalls. Students may feel secure with antivirus tools and engage in unsafe online behaviors, such as visiting

questionable websites or downloading files from unreliable sources. The study finds that most students with antivirus software still experience infections. Students may take greater risks online when they feel "protected". This behavior aligns with RCT, which predicts that protective measures may lead to overconfidence that results in more risky behaviors, ultimately leaving students vulnerable to malware attacks.

3.Human Factor Theory of Cybersecurity

The Human Factor Theory of Cybersecurity emphasizes that human errors, such as weak passwords or unsafe browsing, play a significant role in cybersecurity vulnerabilities. Students may not follow basic security practices like updating software, using complex password, or avoiding risky link.

The study shows that a considerable number of students overlook essential digital safety measures, such as keeping software up-to-date and using robust passwords. This behavior highlights the importance of addressing human factors in improving cybersecurity. Training students to understand the risks of such behaviors could reduce their exposure to malware.

4.Social Cognitive Theory (SCT)

Social Cognitive Theory posits that behavior is influenced by external factors, such as peer behavior, educational programs, and institutional policies. In the context of this study, SCT explains how students' cybersecurity awareness and behaviors may be shaped by external influences, such as the availability of cybersecurity training or guidance from peers. A significant 93% of students in the study expressed interest in learning more about securing their devices, indicating that external educational factors can influence students' behaviors. This aligns with SCT, which suggests that increasing students' exposure to cybersecurity education could enhance their motivation to adopt protective measures.

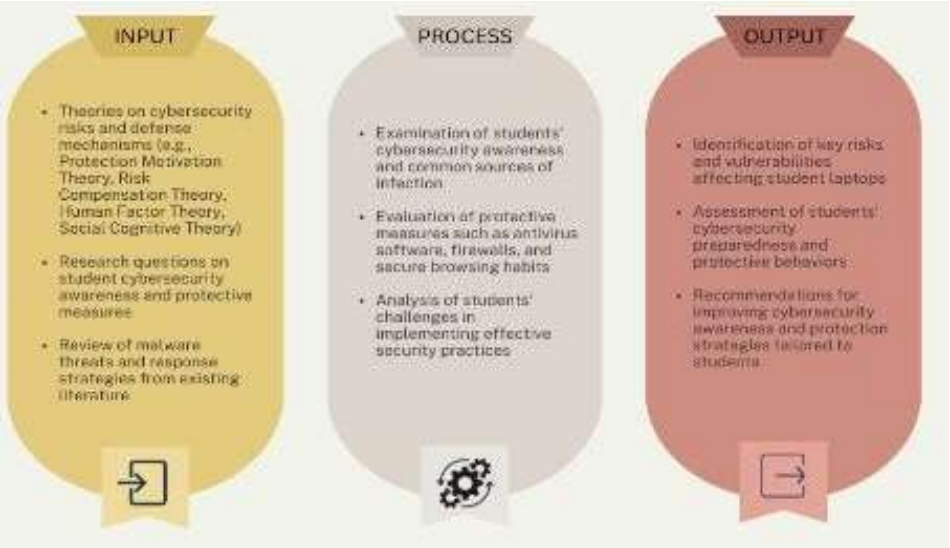

Figure 1. Conceptual Framework

Design and Methods

This study adopts a quantitative research design to investigate the impact of computer viruses on student laptops. The primary aim is to assess students' cybersecurity awareness,

common sources of malware infections, and their response strategies using statistical data. The quantitative approach ensures that the analysis is aim, relying on measurable data to find trends, patterns, and potential gaps in cybersecurity behaviors among students. The study will target students from various academic institutions who often use laptops for academic purposes. Structured survey questionnaires will be distributed to gather numerical data on students' security habits, virus infections, and cybersecurity practices. This design will help find gaps in students' cybersecurity knowledge and inform recommendations for improving digital safety across educational settings.

Research Methods

To collect primary data, survey questionnaires will be distributed among students. These questionnaires will include questions about students' cybersecurity practices, experiences with malware infections, and awareness of cybersecurity best practices. Secondary data will also be analyzed by reviewing past research studies and related literature to compare trends and findings related to malware infections on student laptops. For data analysis, quantitative methods will be applied, including frequency distributions and percentage-based evaluations. Measures of central tendency (mean, median, and mode) will also be used where proper to analyze the collected data and find trends in students' cybersecurity behaviors. This study will adhere to ethical guidelines to ensure the protection of participants' privacy and keep the confidentiality of the data collected. All personal information will be anonymized, and informed consent will be obtained from all participants before they engage in the survey. The research will ensure no harm is caused to participants, and their participation will be entirely voluntary.

Results and Discussion

This chapter presents the findings of the study based on data collected from students about the impact of computer viruses on their laptops and their cybersecurity practices. The results are entirely based on quantitative data using statistical tools, including frequency distribution, percentages, and where applicable, measures of central tendency (mean, median, and mode). The discussion interprets these findings considering the study's aims and existing literature.

Results

Demographics and Laptop Usage

Table 1 provides an overview of the demographic characteristics of the respondents, including their age, academic year, and frequency of laptop usage. Most respondents (48.15%) are in the 21-23 age group, with 74.07% being third-year students. In terms of laptop usage, 44.44% use their laptops daily, while the rest use them less often. This high rate of regular exposure to digital environments underscores the importance of understanding cybersecurity behaviors and practices among students.

Table 1: Demographic Information and Laptop Usage

Category	Subcategory	Count	Percentage (%)
Age Group	18-20 years old	12	44.44%
	21-23 years old	13	48.15%
	Above 23 years old	2	7.41%
Academic Year	First Year	4	14.81%
	Second Year	3	11.11%
	Third Year	20	74.07%
Laptop Usage	Daily	12	44.44%
	Few times a week	8	29.63%
	Occasionally	4	14.81%
	Rarely	2	7.41%

Cybersecurity Awareness and Practices

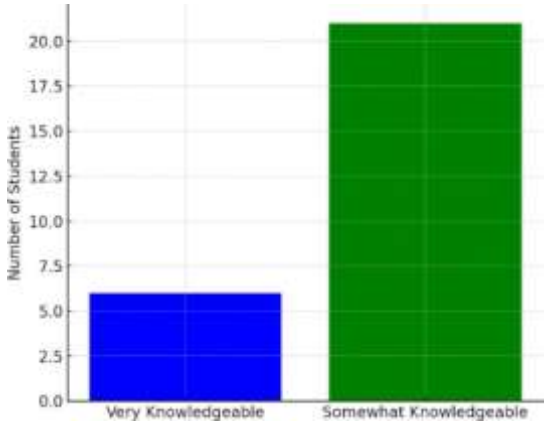

Figure 2. Cybersecurity Awareness Levels

Figure 2 illustrates the self-reported cybersecurity awareness levels of the students. The results show that 6 students (22.22%) consider themselves deeply knowledgeable about cybersecurity, while 21 students (77.78%) describe their knowledge as somewhat adequate. This suggests that although most students have a moderate understanding of cybersecurity, there is a notable gap in their awareness of advanced security measures, which leaves them vulnerable to cyber threats.

Perceived Risk of Virus Infection

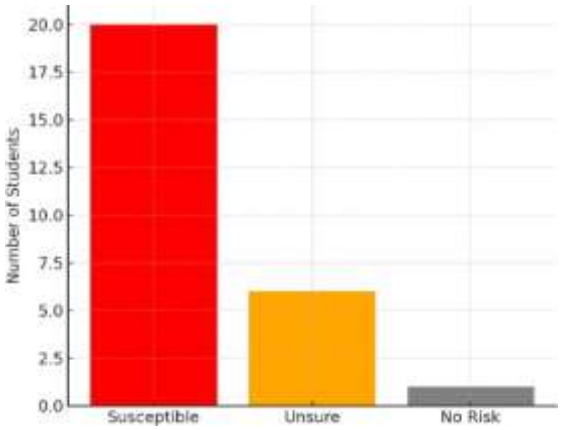

Figure 3. Perceived Risk of Virus Infection

Figure 3 reflects the perceived risk of virus infection among students. The data shows that 20 students (74.07%) believe they are susceptible to malware or virus attacks. A smaller group, 6 students (22.22%), are unsure about their vulnerability, while only 1 student (3.70%) feels immune. Students recognize the threat but are unclear about the risk level and how infections spread, showing gaps in understanding.

Software Update Frequency

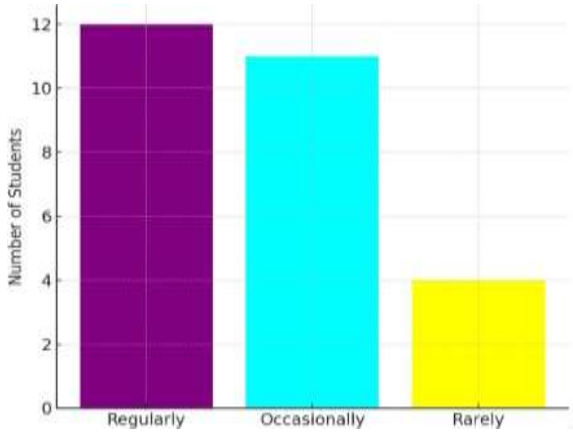

Figure 4. Software Update Frequency

Figure 4 shows the frequency of software updates among the students. The data reveals that 12 students (44.44%) regularly update their software, 11 students (40.74%) update occasionally, and 4 students (14.81%) rarely update their systems. This gap in update frequency highlights a key vulnerability, as not keeping software up to date can leave devices exposed to malware and virus attacks, which thrive on outdated software and security loopholes.

Password Practices

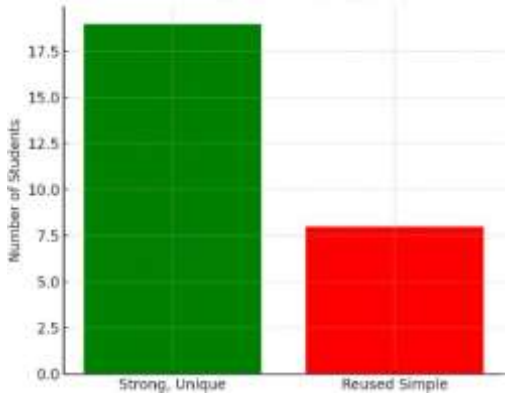

Figure 5. Password Practices

Figure 5 shows students' password security habits. While 19 students (70.37%) report using strong and unique passwords, 8 students (29.63%) admit to reusing simple passwords across multiple platforms. This inconsistency in password management is concerning, as weak or reused passwords are one of the most common entry points for cyber attackers and viruses.

Experience with Malware Infections

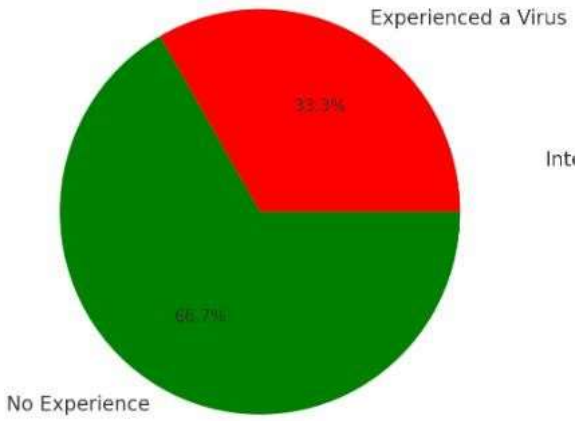

Figure 6. Experience with Malware Infections

Figure 6 reveals that 9 students (33%) have met malware or virus infections, while 18 students (67%) have not. This statistic directly highlights the alarming impact of computer viruses on students' devices, showing that a sizable part of the student population has already experienced the disruption and damage that malware infections can cause.

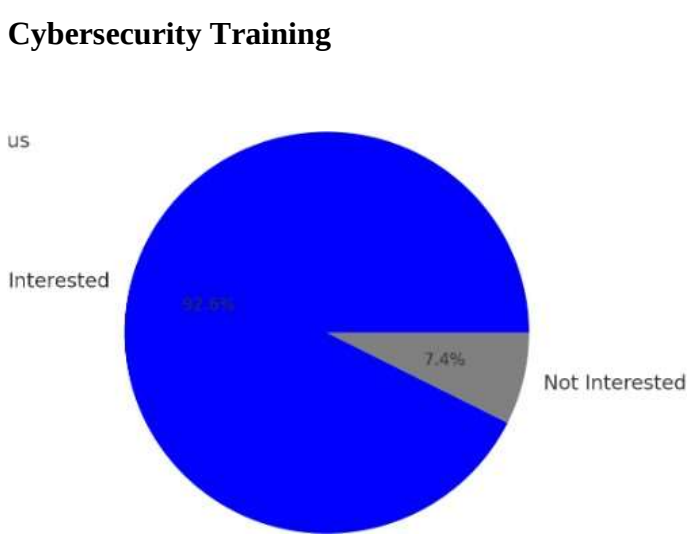

Figure 7. Interest in Cybersecurity Training

Figure 7 presents the students' interest in receiving cybersecurity training. A substantial 93% of students (25 out of 27) expressed interest in learning more about cybersecurity, while only 7% (2 students) were not interested. This finding strongly suggests a desire for better education and training to improve students' ability to protect themselves from computer viruses and other cybersecurity threats.

Discussion

The findings of this study underscore the alarming impact of computer viruses on student laptops. The fact that 33% of students have already experienced malware infections shows the tangible consequences of these threats. Additionally, 74.07% of students perceive themselves as susceptible to virus infections, reinforcing the significance of the problem.

However, despite the recognition of risk, cybersecurity practices among students stay inconsistent. While most students show moderate awareness, there is a lack of implementation of protective measures. For example, while 70.37% of students report using strong passwords, nearly 30% still reuse simple passwords across multiple platforms, exposing themselves to unnecessary risks. Furthermore, the fact that 55.55% of students do not regularly update their software shows a critical gap in their defense against cyber threats.

The strong interest in cybersecurity training (93%) suggests that students are eager to learn and improve their practices. This aligns with earlier studies, such as one by Alharbi and Rania (2020), who found that cybersecurity improves students' knowledge and initiative-taking behaviors toward protecting their devices from cyber threats.

Recommended Effective Protection Strategies

To combat the increasing threat of computer viruses, students must adopt more consistent and effective protection strategies:

1.Regular Software Updates – Students should prioritize keeping their systems up to date, as timely updates are crucial in preventing malware infections.

2.Password Management – It is essential to emphasize the use of strong, unique passwords for every account, and tools like password managers can be introduced to help students manage their credentials securely.

3.Cybersecurity Training – Institutions should integrate cybersecurity education into their curriculum, offering workshops or online training sessions to enhance students' understanding of potential risks and how to mitigate them. This could include practical, direct sessions for students to learn how to secure their devices and personal data.

Conclusion

In conclusion, this study has illuminated the significant impact that computer viruses have on student laptops and the critical gaps in students' cybersecurity practices. The findings reveal that one-third of students have already experienced malware infections, and most either neglect software updates or reuse weak passwords—leaving them vulnerable to cyber threats. Despite moderate levels of cybersecurity awareness, implementing safe digital habits remains inconsistent.

A key insight from the study is the overwhelming interest—93% of respondents—in cybersecurity education. This indicates a strong desire for improvement and highlights an opportunity for educational institutions to incorporate comprehensive cybersecurity training into their curriculum. Such programs should not only present theoretical knowledge but also include hands-on activities that equip students with practical skills to defend against evolving threats.

While this research contributes valuable insights, it is not without limitations. The study focused on a limited student population and relied on self-reported data, which may introduce bias or inaccuracies. Future research could expand the sample size, explore specific causes of malware infections, or assess the effectiveness of tailored training interventions.

Ultimately, safeguarding student devices from cyber threats requires a collective effort. Educational institutions must take proactive steps to integrate digital security into academic programs, and students must commit to adopting safer online practices. By cultivating cybersecurity awareness and reinforcing responsible digital behavior, we can build a safer online environment that empowers students to thrive in today’s connected world.

References

Acharya, M., & Sharma, A. (2020). Student awareness and prevention techniques for computer viruses. *Asian Journal of Information Technology.*

Al-Mutairi, H., & Rania, K. (2021). Enhancing cybersecurity awareness through gamification: Design an interactive cybersecurity learning platform for Multimedia University students. *Journal of Interactive Technology, 19*(2), 89–105. https://journals.mmupress.com/index.php/jiwe/article/view/1103

Alharbi, M., & Rania, A. (2020). Cybersecurity awareness and behaviors among university students. *Journal of Cybersecurity Education, 15*(2), 124–139.

Alotaibi, M. B. (2020). Factors affecting cybersecurity awareness among university students. *Applied Sciences, 12*(5), 2589. https://www.mdpi.com/2076-3417/12/5/2589

Clark, S. E., & Harris, M. L. (2020). Cybersecurity awareness among school students: Exploring influencing factors, legal implications, and knowledge gaps. *International Journal of Information Security and Systems, 25*(4), 203–212. https://ijirss.com/index.php/ijirss/article/view/4696

Hadlington, L. (2017). Human factors in cybersecurity: Examining the link between internet addiction, impulsivity, attitudes toward cybersecurity, and risky cybersecurity behaviors. *Heliyon, 3*(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences, 80*(5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005

Khan, M. A., & Khan, S. (2020). Cyber security awareness among university students: A case study. *International Journal of Computer Applications, 175*(7). https://www.researchgate.net/publication/341364046

McCormac, A., Parsons, K., Butavicius, M., Pattinson, M., & Jerram, C. (2015). Understanding the target of endpoint security: Human behavior. *Computers & Security, 48*, 221–233. https://doi.org/10.1016/j.cose.2014.11.002

Nwankwo, C. (2019). *IT security managers' strategies for mitigating data breaches in higher education institutions* (Doctoral dissertation). Walden Dissertations and Doctoral Studies. https://scholarworks.waldenu.edu/dissertations/7536/

Parsons, K., Butavicius, M., Pattinson, M., & McCormac, A. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security, 42*, 165–176. https://doi.org/10.1016/j.cose.2013.12.003

Rodriguez, L. A., & Panganiban, C. R. (2019, October). *Am I secured: A computer virus awareness among BSIT students*. ResearchGate. https://www.researchgate.net/publication/336406476

Samson, L. V., & Parker, B. K. (2022). Evaluating online security behavior: Development and validation of a personal cybersecurity awareness scale for university students. *Journal of Cybersecurity Education, 18*(1), 124–138. https://www.mdpi.com/2227-7102/14/6/588

Siddiqui, F., & Khan, M. Z. (2021). Impact of malware on academic devices and data loss: A university-based study. *International Journal of Cyber Security and Digital Forensics.*

Suleiman, A. D., Mukhtar, M. I., Galadanci, B. S., & Muaz, S. A. (2019). Effect of virus on computer systems: A survey of student's perception. *Journal of Computer Science and Its Application, 26*(1), 78–85. https://www.ajol.info/index.php/jcsia/article/view/193079.