ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645
Indian Journal of Science and Technology, *Vol 12(26), DOI: 10.17485/ijst/2019/v12i26/144967, July 2019*

Am I Secured: A Computer Virus Awareness among BSIT Students

Devine Grace D. Funcion* and Lowell A. Quisumbing

Leyte Normal University, Tacloban City Philippines;
dgd_35@lnu.edu.ph, lowellquisumbing@lnu.edu.ph

Abstract

Objective: Computer virus has an alarming threat to data protection evolving, the evolution of computer virus becomes more harmful that duplicates the data in a floppy drive to a more damaging virus that could destroy the computer programs and more it can cause the computer to stop operating. The study aims to reveal the degree of Computer virus awareness of BSIT students in the Leyte Normal University. **Method**: The respondents of the survey are the BS Information Technology students of Leyte Normal University. Further, a total of 205 out of 322 respondents or 63.66% participated in the actual survey. **Findings**: IT students observe preventive measure to avoid from getting computer malware. Some students practice Scan storage device before using (40% and = 82), delete unknown emails (30% and = 64), install only trusted software (38% in = 76), practice safe browsing (35% and = 74). Hence, users should scan first the drives and diskettes for reasonable suspicions of malware before using the device. **Application/Improvements:** There must be a clear policy on the usage of flash drives do conduct virus checking before using the method. IT faculty should formulate seminars and training regarding computer malware for the IT student who possesses limited knowledge about computer malware..

Keywords: Awareness, Computer Virus, Information Technology, Malware, Student

1. Introduction

Computer virus causes an alarming threat to information security. Evolving, the evolution of computer virus becomes more harmful that duplicates the data in a floppy drive to a more damaging virus that could destroy the computer programs and more it can cause the computer to stop operating. The malicious software is known as malware, software that brings harm to a computer device. Malware can be in the form of worms, viruses, Trojans, spyware, adware and root kits, etc., which steal protected information, edit documents or add software not approved by a user[1]. However, detection of the malicious virus is through the executable file, cryptographic functions, decryption code and its structural features[2].

Nonetheless, with the advancement in technology, the computer system becomes vulnerable to the different types of attack. The student uses the internet to search for information where they can easily download any resources they need for their school project. However, the student does not observe any security protocol in downloading and accessing web pages, which makes the computer system defenceless from malware.

Additionally, various vendors of anti-virus in the market promise better security protection from malware attacks - anti-virus software work by maintaining a database of signatures or fingerprints for known viruses[3]. Updating the antivirus database is necessary to append the new strain of computer virus. In one case, infection

**Author for correspondence*

is found in a file; the anti-virus application reports this to the user and hinders the data or program from entering the data processor organization[4]. Investment in Antivirus has become indispensable to some Government office, Business Organization and Education Sector to protect their data from virus attack. Nevertheless, taking in an antivirus does not protect the host computer from virus attack. Nonetheless, computer systems are still vulnerable to the new strain of computer virus[5].

Leyte Normal University is a government institution offering Bachelor of Science in Information Technology (BSIT) program. Access to computer laboratory among Information Technology (IT) students is boundless due to their computer subjects. Moreover, the vulnerability of getting a virus is high because students do not observe good security measure in download and copy files from the internet. In[6] the study of because of unsafe student practices and careless behavior in downloading and copying files, an orientation for information security is needed to ensure safety awareness in downloading files from different sources[6].

1.1 The Objective of the Study

The study aimed to determine the Computer Malware Awareness of BSIT students. Specifically, it seeks to:

- What is the perceived knowledge of the respondents on the difference of virus, worm, Trojan horse, spyware?
- What is the perceived knowledge of the respondents on the type of computer malware infects their computer system?
- What is the perceived knowledge of the respondents on how of computer malware infects their computer system?
- What computer activities does the respondent do to catch computer malware?
- How do the respondents identify computer malware infections?
- What security measures do the respondents observe to prevent computer malware?

2. Theoretical Framework

The study anchored on the Protection Motivation Theory (PMT), which explains that protective behavior is both motivated by an individual's assessment of threat and how to cope with that threat[7]. The first element of PMT is the threat appraisal, which refers to how an individual perceives a threat. It posits that if a threat is perceived to be high, then it motivates the person involved to protect the assets, e.g., information, property or life in a heavily weighted manner such that the individual exhausts all means necessary to protect his assets against that perceived threat. More so, risks can also determine behavioral intentions to adopt protections or security intentions. It refers to the study since malware are perceived to be threats to personal data and the students' views on how the rogue software may affect the protection of their valuable information influences the type of protection approach that they will practice against it.

The common perception of Internet users against viruses, worms or Trojans is that it is harmful to online safety, thus the need for security-related behaviors[8]. Subjective norms may also be a significant predictor of how individuals understand threats. It means that the interpretation of a malware threat by a student maybe due to influence from other people. Such as the knowledge transmitted by teachers to learners or social norms, which refers to how others are doing in connection with the threat. Either way, this implies that when we take proactive measures to safeguard our information, especially in using the internet, it is because we regard the idea that online transactions are not always safe. Therefore, we acknowledge that threat severity is an essential predictor to security-related protection[9].

The coping appraisal of PMT refers to the effectiveness, response, avoidance and self-efficacy measures that we individuals practice to be able to adapt to the security threats. It refers to the mechanisms and techniques that we employ to manage or control security-related behaviors. It means that individuals can have the ability to create their subjective representations of how to deal with a security concern. It implies that the knowledge of

how to practice security, including coping mechanisms, are constructed based on personal experiences and hypotheses of the environment in which they work. Thus, the theory applies to the study because it shows that the behaviors that the student's practices on how to deal with malware infections and threats are based on their experiences when dealt with the problem. The habits that they exhibit towards security threats are the product of their skills, practices, and responsibilities.

3. Methodology

3.1 Research Design

The researcher uses the descriptive method of the study, which utilizes a questionnaire to determine the awareness of the BS Information Technology on a computer virus.

3.2 Research Procedure

The research use Google form to conduct the survey. The questionnaire consists of the following parts first (profile of the student), second (knowledge about computer virus), third (security measures to prevent from getting computer virus). For the clarity of the survey, the following the definition of terms:

- Virus - a malicious program that can execute itself and spreads by infecting other programs or files.
- Worm - is a type of malware that can self-replicate without a host program.
- Trojan horse - is a malicious program that is planned to appear as a legitimate program; once activated following installation, Trojans can execute their malicious purposes.
- Spyware - is a kind of malware that is designed to collect information and data on users and observe their activity without users' knowledge.
- Phishing - the type of malware delivery; emails disguised as legitimate messages contain malicious links.

3.3 Respondents of the Study

Figure 1 shows the respondents of the study are the BS Information Technology students of Leyte Normal University. Further, a total of 205 out of 322 respondents or 63.66% participated in the actual survey. Below presents the population of the respondents.

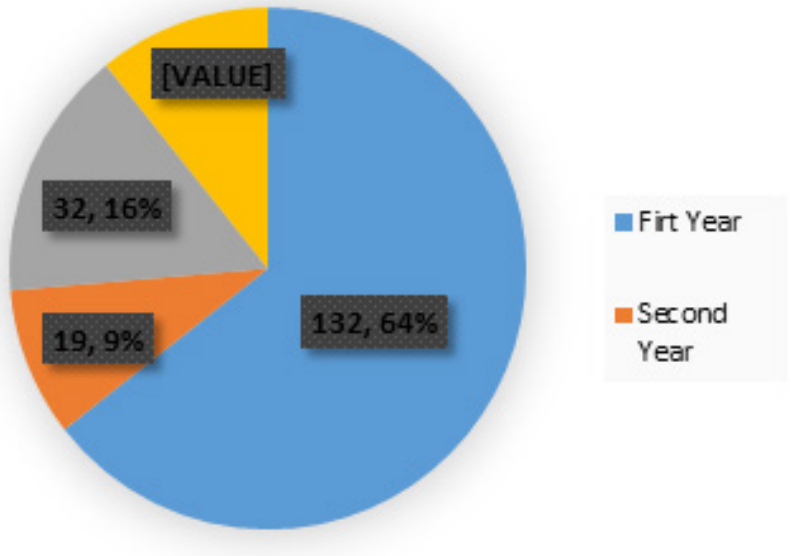


Figure 1. Year level respondents.

4. Result and Discussion

Figure 2 illustrates the understanding of the IT student on the difference of virus, worm, Trojan horse and spyware. It demonstrates that most of the IT students have a slight experience (34.1%), no idea at all (10.7%), highly knowledgeable (2.9%), somewhat experience (29.3%). It implies that those students who possess No Idea (10.7%) on the difference of virus, worm, Trojan horse, spyware can cause danger to the computer system and security. It is because students are not familiar with and conscious of the characteristics of malware that could penetrate the computer and inflict threats to the user. Any users can become a victim of malware attack because of some students who possess no knowledge about computer malware.

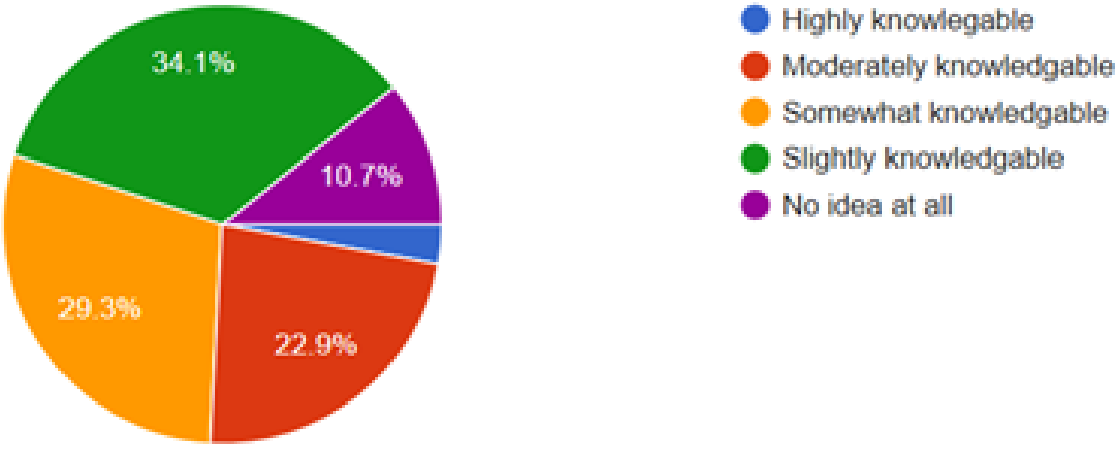


Figure 2. IT students level of knowledge in terms of computer malware.

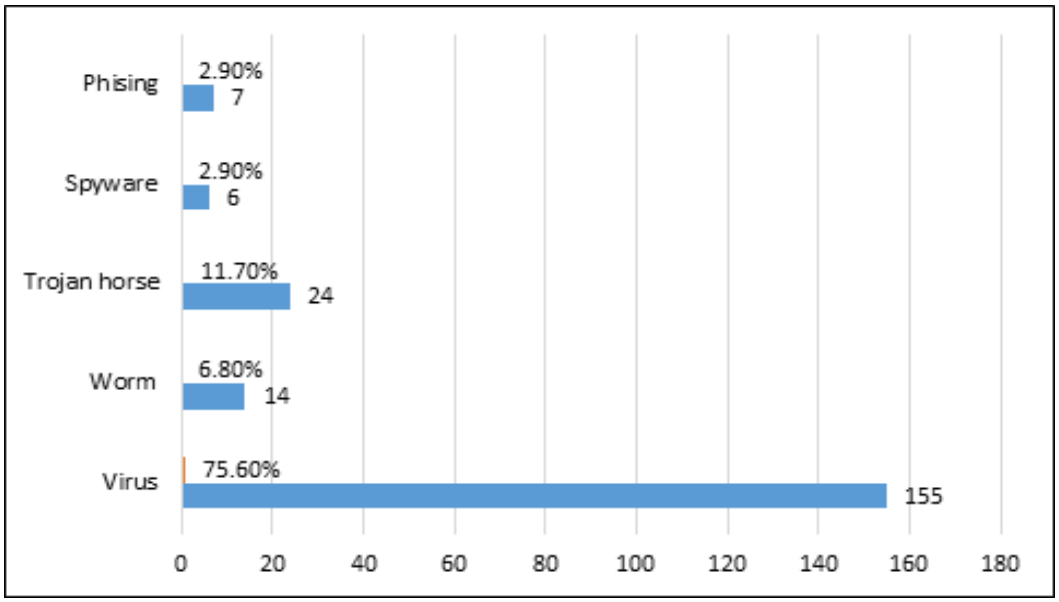
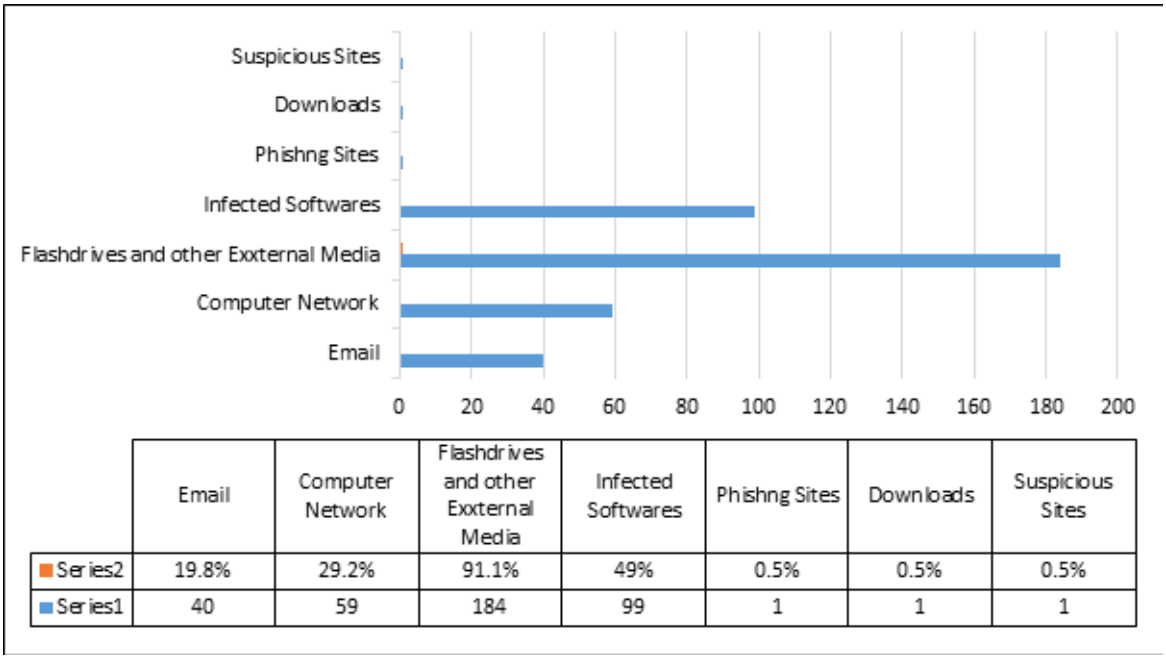


Figure 3. Types of computer malware that commonly infects hardware/software.

Figure 3 shows the type of computer malware that commonly infects the computer laboratory. Phishing (2.9% n = 7), Spyware (2.9% n = 6), Trojan horse (11.7%, n = 24), Worm (6.8% n = 14), Virus (75.6% n = 155).

Hence, Figure 4 shows that transmission malware is through flash drives and other external devices (91.1%, n = 184), followed by infected software (49%, n = 99), next to the computer network (29.2%, n = 59), and email (19.8%, n = 40). Lastly, through downloads, phishing site and suspicious sites (0.5%, n = 1). Sharing of files using thumb drives are the primary source of spreading a computer virus. It shows that students use a flash



	Email	Computer Network	Flashdrives and other Exxternal Media	Infected Softwares	Phishng Sites	Downloads	Suspicious Sites
Series2	19.8%	29.2%	91.1%	49%	0.5%	0.5%	0.5%
Series1	40	59	184	99	1	1	1

Figure 4. How computer virus transmitted.

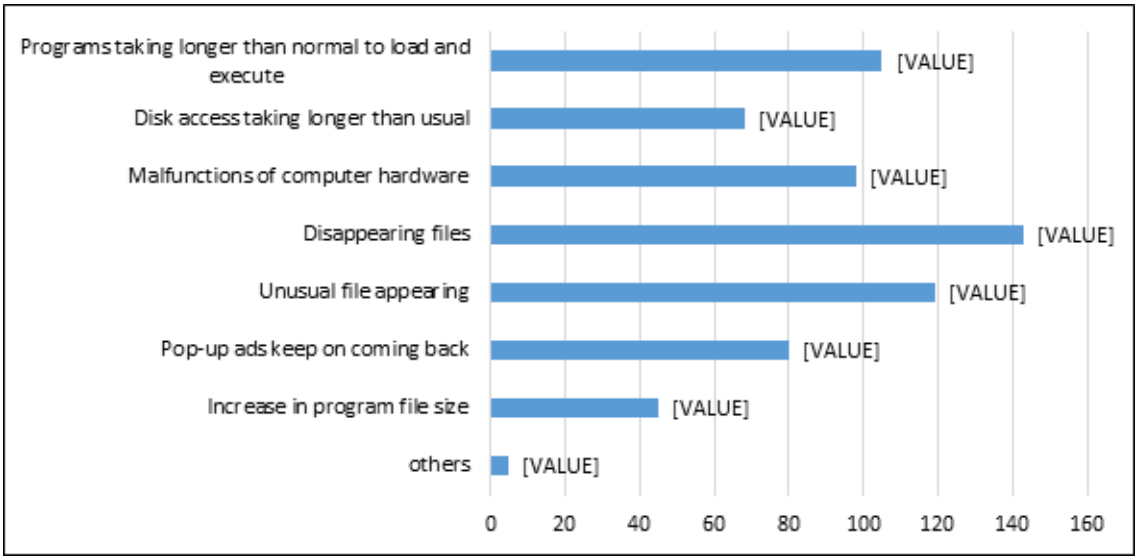


Figure 5. Characteristics of computer malware.

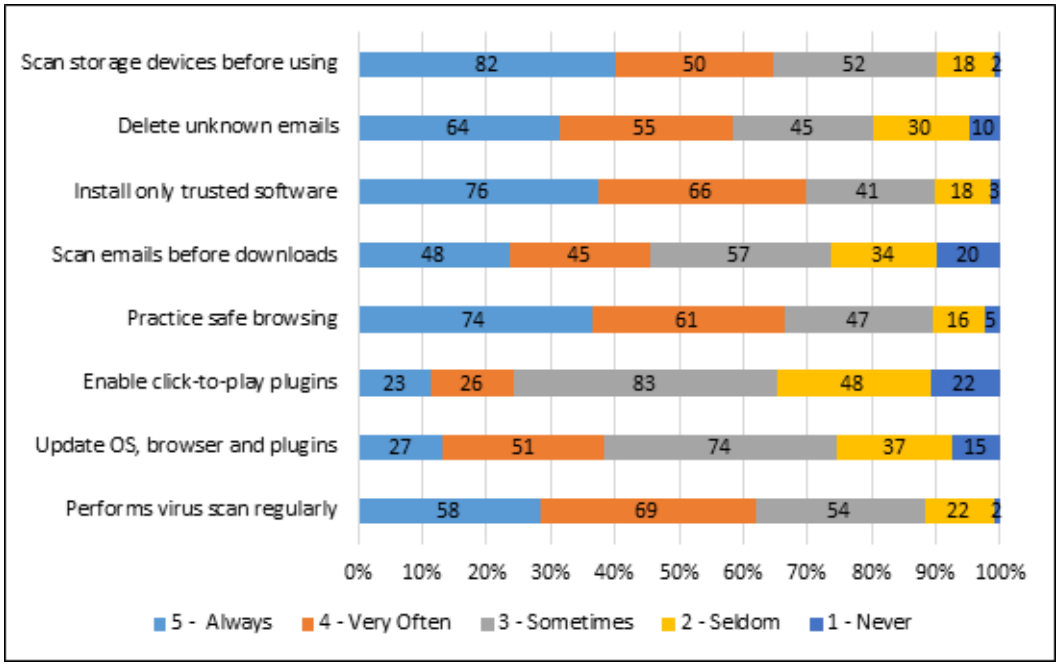


Figure 6. Security measure to prevent computer malware attacked.

drive in saving files respondents agree that transmission of computer virus is through the use of flash drives[10] a computer virus can intrude any form of writable storage that includes a hard disk, floppydisk, tape, optical media or memory. Once an infected disk is opened and booted, the virus will easily intrude and spread its disease to the computer hardware/software[11].

Moreover, Figure 5 presents the characteristics of malware once it penetrates the computer system. An infected computer with malware indicate features such as disappearing files (69.8%, n = 143), unusual file appearing (58%, n = 119), program takes longer than usual to load and execute (51.2%, n = 105), malfunctions of computer hardware (47.8%, n = 98), pop-up ads keep on coming back (39%, n = 80), disk access taking longer than usual (33.2%, n = 68%), increase in program files (22%, n = 45) is available. It implies that most computers infected with malware shows some symptoms of disappearing files. Wherein some IT students grumble about missing data because of the computer virus an assumption were made that universal characteristic of a computer infected with malware is Unusual file appearing or Disappearing data[12].

Figure 6 proves that some IT students observe preventive measure to avoid becoming infected with computer malware. Some students practice Scan storage device before using (40% n = 82), delete unknown emails (30% n = 64), install only trusted software (38% n = 76), practice safe browsing (35% n = 74)[10].

5. Conclusion

As shown in the result, computer virus is the common malware that infiltrates the system that causes damage to the computer hardware and software. Although some IT students who practice safety measures in accessing files from the computer. Information processing system security is comprised of those IT students who demonstrate Moderate to No knowledge about computer virus since they can rapidly open the virus through the usage of flash drives. Common symptoms of the computer that are tainted with the virus are disappearing and unusual

file appearing. Thus, it is recommended that there must be a clear policy on the usage of flash drives does conduct virus checking before using the gimmick. Seminars and training on computer virus are extremely recommended for those pupils who possess limited knowledge about computer malware.

6. References

1. Malicious Software (Malware). 2018. https://www.techopedia.com/definition/4015/malicious-software-malware.
2. Schmid MN, Weber M, Haddox-Schatz M, Geyer D. U.S. Patent No. 7,644,441. Washington, DC: U.S. Patent and Trademark Office; 2010.
3. Gupta S. Types of malware and its analysis. International Journal of Scientific and Engineering Research. 2013; 4(1).
4. Souppaya M, Scarfone K. Guide to malware incident prevention and handling for desktops and laptops. NIST Special Publication. 2013. p. 800–83. https://doi.org/10.6028/NIST.SP.800-83r1.
5. Sukwong O, Kim HS, Hoe JC. Commercial antivirus software effectiveness: An Empirical Study. IEEE Computer. 2011; 44(3):63–70. https://doi.org/10.1109/MC.2010.187.
6. Quisumbing LA. Preemptive evaluation through information security awareness: Perception of Information Technology Students in a Philippine State University. International Journal of Applied Engineering Research. 2019; 14(4):900–7.
7. Tsai HYS, Jiang M, Alhabash S, LaRose R, Rifon NJ, Cotten SR. Understanding online safety behaviors: A protection motivation theory perspective. Computers and Security. 2016; 59:138–50. https://doi.org/10.1016/j.cose.2016.02.009.
8. Anderson CL, Agarwal R. Practicing safe computing: A multimedia empirical examination of home computer user security behavioral intentions. MIS Quarterly. 2010; 34(3):613–43. https://doi.org/10.2307/25750694.
9. Zahedi FM, Abbasi A, Chen Y. Fake-website detection tools: Identifying elements that promote individuals' use and enhance their performance. Journal of the Association for Information Systems. 2015; 16(6):448–84. https://doi.org/10.17705/1jais.00399.
10. Oyelere SS, Oyelere LS. Users' perception of the effects of viruses on computer systems-An empirical research. African Journal of Computing and ICT. 2015; 8(1):121–30.
11. Chanda N. Bound together: How traders, preachers, adventurers and warriors shaped globalization. Yale University Press. 2008.
12. Funcion DG. Apriori algorithm application on the prevalence of computer malware. Indian Journal of Science and Technology. 2019; 12(17):1–6. https://doi.org/10.17485/ijst/2019/v12i17/143328