Kasu Journal of Computer Science Vol. 1 No. 2 [June, 2024], pp. 134-150
https://doi.org//10.47514/kjcs/2024.1.2.001

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

A Survey on The Effect of Computer Virus Attacks and Its Preventive Measures Among Computer Users

Usman Ismail Abdulmalik[1], Nura Abubakar Anka[1], Shamsudeen Sani Muhammed[1] and Saidu Aliyu Illo[2]
[1]Department of Computer Science, Federal Polytechnic, Kaura Namoda, Zamfara State, Nigeria
[2]ICT Department, Federal Polytechnic, Kaura Namoda, Zamfara State, Nigeria
usmaniamailbox@yahoo.com[1]

Abstract

Computer use is becoming part of people's lives, however, there have been considerable threats of computer virus attacks in the recent past. Viruses have had adverse effects on computer resources ranging from loss of data, destruction of computer, stealing of confidential information, damage to credibility and in some cases, mild effects such as slowdown computer performance or message pop-ups appear on the screen. This research studied the effect of computer virus attacks, identify the most common types of computer virus infections, and provide guidelines on how individuals can protect their computers from virus attacks. The research applied the use of cross-sectional survey method using survey questionnaires of independent variables of 246 personal computer users which include professionals, students of tertiary institutions and computer users using convenient sampling method. The findings of the study revealed that a high percentage (about 65.04%) claimed that antivirus has high impact on computer virus attacks. The findings also revealed that symptoms of all types and ways of computer virus infection are prevalent. However, the findings further revealed that symptoms of memory resident virus, boot sector virus and worm are relatively common (about 32.11%) than other types of viruses. The findings revealed that the majority (about 71.95%) indicates installing license and updating antivirus software is the best preventive measures to safeguard their computer resources from virus attacks. Finally, based on the study's findings, several recommendations are proposed to enhance computer virus protection and safeguard computer resources. These include adopting robust antivirus software, maintaining regular software updates, implementing automatic virus scans, and practicing safe browsing habits.

Keywords: *Computer system, Computer virus, Computer users, Preventive measures.*

1. Introduction

The use of computers is becoming more prevalent in our lives on a daily basis, but there have been significant threats from computer viruses in the recent past. Viruses have had a negative impact on data and programs ranging from formatting hard discs to damaging information infrastructure, abruptly restarting machines, deleting or modifying data, and in some cases mild effects such as slowing down machines or producing irritating sounds. Viruses have been a major source of concern, particularly with technological advances in data processing, storage, and information movement (Rotich *et al*., 2014).

A computer virus is a program or piece of programming code that replicates itself by being copied or initiating copying to another program, hard drive boot sector, or data file (AlBazzaz & AlMuhanna, 2016). A computer virus is a malicious program that copies itself to another program in order to replicate itself. To put it another way, the computer virus replicates itself in other executable code or documents (Comodo Antivirus, 2020). These are called viruses primarily because they share many similarities with

Kasu Journal of Computer Science Vol. 1 No. 2 [June, 2024], pp. 134-150
https://doi.org//10.47514/kjcs/2024.1.2.001
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

viruses in biomedicine, such as being parasitic, infectious, and destructive (Zheng, 2015). A computer virus, similar to a flu virus, is designed to spread from host to host and replicate itself. Similarly, just as flu viruses cannot reproduce and spread in the absence of a host cell, computer viruses cannot reproduce and spread in the absence of programming, such as a file or document (Alison, 2020).

Computer virus is a malicious piece of mobile code that includes viruses, Trojan horses, worms, and logic bombs (Peng *et al*., 2013). Malware refers to these viruses. As a result, malware is defined as any program or file that is harmful to a computer user (AlBazzaz & AlMuhanna, 2016). Emails are one-way viruses spread; opening an attachment in an email, visiting an infected website, clicking on an executable file, or viewing an infected advertisement can all cause the virus to spread to a computer. Infections can also spread when connecting to infected removable storage devices, such as USB drives (Comodo Antivirus, 2020). Computer viruses are essentially pieces of computer code that can copy themselves to other files and perform the tasks specified in their codes (Khan *et al*., 2017). Viruses are executed when the host program file is executed. Execution requires human intervention. A computer virus's structure can be divided into four phases: mark, infection mechanism, trigger, and payload (Bahukhandi & Rana, 2016).

Over 450,000 new malicious programs (malware) and potentially unwanted applications (PUA) are discovered every day. These are examined, classified, and saved based on their characteristics (AV-Test Institute, 2023). Malware, whether viruses, trojans, worms, or other unwanted programs, keeps growing and spreading. Statistics from antivirus software show a significant increase in the number of viruses, with 17.7 million malware programs detected in September 2019 alone (Jovanović, 2023). There are over 1.2 billion pieces of malware and PUA circulating the internet as of 2023. (AV-Test Institute, 2023). Because of malware's unstoppable growth and development, there are now more of these harmful apps than ever before. Malware counts increase by 100 million each year. This expansion has been especially noticeable since 2013 (Jovanović, 2023).

The purpose of this research is to examine the effect of computer virus attacks, identify the common types of computer virus infections and its preventive measures among computer users, also to introduce to the readers the threats that the computer viruses can create and provide guidelines on how individuals can protect themselves against virus attacks. This paper's presentation is organised as follows: Section 2 is review of related works; Section 3 is the study's objectives; Section 4 is the methodology; Section 5 is the discussion of results; Section 6 is the discussion of the findings; Section 7 is the study's conclusion; the study ended in Section 9 with recommendations.

1.1 Types of Computer Virus Infection

There are different types and ways of computer virus infection and each type have their own unique features that differentiate themselves from one another (Khan, 2012). The common types of viruses are described below.

1. Boot sector virus: This type of virus can take over when you start - or boot - your computer. It can be spread by inserting an infected USB drive into your computer (Alison, 2020). It infects the disc and hard drive, which contain small sections of data known as sectors (Ilmudeen, 2013).

2. Web scripting virus: This type of virus takes advantage of the code of web browsers and web pages. If you visit such a website, the virus could infect your computer (Alison, 2020). This type of code is frequently used to perform undesirable actions. They are mostly spread by infected web pages or browsers (Thakur & Vaidya, 2017).

Kasu Journal of Computer Science Vol. 1 No. 2 [June, 2024], pp. 134-150
https://doi.org//10.47514/kjcs/2024.1.2.001
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

3. **Browser hijacker virus:** This type of virus "hijacks" specific web browser functions and may automatically redirect you to an unintended website (Alison, 2020). It can be spread while downloading; it interferes with the browser's functionality, essentially redirecting the user to specific sites (Bahukhandi & Rana, 2016).
4. **Memory resident virus:** This is a catch-all term for any virus that inserts itself into the memory of a computer system. When an operating system is loaded, a resident virus can execute at any time (Alison, 2020). It conceals itself in computer memory (Thakur & Vaidya, 2017).
5. **Direct action virus:** This type of virus is activated when you run a virus-infected file. Otherwise, it is dormant (Alison, 2020). Once executed, a direct-action virus primarily replicates or takes action. When a specific condition is met, the virus infects the files in the directory or folder specified in the AUTOEXEC.BAT file. The virus is typically found in the hard disk's root directory, and its location is constantly changing (Thakur & Vaidya, 2017).
6. **Polymorphic viruses:** These viruses change their code each time an infected file is executed. It does this to avoid detection by antivirus software (Alison, 2020). It acts like a chameleon, changing its virus signature frequently as it multiplies and prepares to infect the next new-fangled file. It is also known as a binary pattern (Ilmudeen, 2013).
7. **File infector virus:** This virus inserts malicious code into executable files, which are files that are used to perform specific functions or operations on a system (Alison, 2020). Some file infector viruses are attached to program files such as.com or.exe files, while others infect any program for which execution is requested, such as.sys,.ovl,.prg, and.mnu files. As a result, when the specific program is loaded, the virus is also loaded (Comodo Antivirus, 2020).
8. **Multipartite virus:** This virus infects and spreads in a variety of ways. It has the ability to infect both program files and system sectors (Alison, 2020). The actions of multipartite viruses vary based on the operating system present and the existence of certain files. It hides in the memory of the computer but does not infect the hard disc (Thakur & Vaidya, 2017).
9. **Macro virus:** This virus is written in the same macro language as software applications. When you open an infected document, such as an email attachment, the virus spreads (Alison, 2020). Macro viruses infect files created with macro-enabled applications or programs such as doc, pps, xls, and mdb. It infects macro-infected files as well as templates and documents contained within the file (Thakur & Vaidya, 2017).
10. **Overwrite virus:** This virus deletes all information in the files it infects, rendering them partially or completely useless once infected. When this type of virus infiltrates a computer, it replaces all file content but does not change the file size (Thakur & Vaidya, 2017).
11. **Directory Virus:** This virus is also known as a cluster virus or a file system virus. It infects the computer's directory by changing the file location's path. It is usually found on the disc, but it affects the entire directory (AlBazzaz & AlMuhanna, 2016).
12. **Worm:** A worm is a self-replicating virus that does not modify files but instead resides in active memory and duplicates itself. A worm frequently spreads from computer to computer, consuming valuable memory and network bandwidth and causing a computer to stop responding (AlBazzaz & AlMuhanna, 2016). Although a worm is

Kasu Journal of Computer Science Vol. 1 No. 2 [June, 2024], pp. 134-150
https://doi.org//10.47514/kjcs/2024.1.2.001
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

not technically a virus, it has the ability to self-replicate and can cause harm to a computer system, but it is usually detected and removed by antivirus software (Khan, 2012).

13. **Trojan horse or Trojan:** This is a malicious code (not a virus) that reproduces by infecting other files and does not self-replicate like worms. A Trojan horse program appears to perform a useful and desired function, but in reality, the program performs other undesired functions. It may destroy data or compromise a system by allowing another computer to gain access and thus bypassing normal access controls (Khan, 2012). Unlike a computer virus, which attaches itself to other programs, a trojan horse is a self-contained program that can be included in free software or as attachments in email messages without your knowledge (AlBazzaz & AlMuhanna, 2016).
14. **Back door:** A method of gaining access to a computer program that circumvents security mechanisms. A program may occasionally include a back door to allow access to the program for troubleshooting or other purposes. Attackers, on the other hand, frequently use back doors that they discover or instal themselves. In some cases, a worm is designed to exploit a back door left open by an earlier attack (AlBazzaz & AlMuhanna, 2016).
15. **Logical fallacies:** This is also not a virus, but rather segments of other programs that have been disguised. Its goal is to delete data on the computer once certain conditions are met. Logic bombs are undetected until they are detonated, and the consequences can be disastrous (Khan, 2012).
16. **Spyware:** This is any technology that aids in gathering information about a person or organization without their knowledge (AlBazzaz & AlMuhanna, 2016).

1.2 Common Symptoms of Computer Virus Infections

There are common problems that occur due to virus attacks which means that a computer is infected. AlBazzaz and AlMuhanna (2016), Bahukhandi and Rana (2016), Elmundeen (2013), Rotich *et al*. (2014) and Thakur and Vaidya (2015) highlighted some basic signs that a computer may be infected with a virus as follow:

- Slow computer speed or system performance.
- Computer freezes, stops responding or keeps rebooting.
- Complete disk drive is erased or rendered inaccessible.
- A partition of the hard drive disappears.
- Data files are changed in format and very difficult to reopen.
- The command Ctrl+Alt+Del no longer works.
- New icons appear on desktop and cannot be removed.
- Missing file error message display on the screen.
- Unexplained images appear on the desktop.
- Antivirus software detects the presence of a computer virus.
- The appearance of a two-part extension on recently opened documents, such as.doc.exe
- An antivirus software is disabled for no reason or the antivirus program cannot be restarted.
- Unexplained messages and pop-ups appear on the screen.
- Menus and dialogue boxes are seen in distorted form.

Kasu Journal of Computer Science Vol. 1 No. 2 [June, 2024], pp. 134-150
https://doi.org//10.47514/kjcs/2024.1.2.001
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

- Program disappears from the computer even though it has not been intentionally removed.
- Out-of-memory error messages are received even though the computer has sufficient RAM
- Windows Task Manager is unable to start.
- Slow internet connection.
- Internet browser homepage changed.
- Application software seems to be changed and does not work correctly.
- Unexplained printing problems occur.

2. Related Works

Several studies have been done to investigate and explore computer virus attacks, detections and preventions in every angle of study in the field. This section reviews the related works previously done.

Thakur and Vaidya (2015) researched on the prevention of computer viruses and reviewed several related studies in the field. In addition, the study discussed the importance of using algorithms in computer virus protection and prevention, as well as their implications in designing and developing antivirus technologies and policies. The research concluded that, despite its limitations, some models bring new hope for solving the computer virus problems.

Liu and Li (2015) researched a novel virus-antivirus spreading model. The study looked into the impact of countermeasure propagation on viral spread. A new virus antivirus spreading model is proposed for this purpose. When the threshold is less than one, the global asymptotic stability of the virus-free equilibrium is demonstrated, and when the threshold is greater than one, the existence of the viral equilibrium is demonstrated. The effects of various model parameters on the threshold are also investigated. According to the results of numerical simulations, the spread of countermeasures contributes to the suppression of viruses, which is consistent with reality.

Zheng (2015) studied virus detection methods based on computer virus invasion pathways, such as the appearance inspection method, the feature code method, the system data comparison method, and the software simulation method. The study also researches computer virus prevention technology from three perspectives: prevention, cleaning computer viruses, and computer system repair. Bahukhandi and Rana (2016) researched the origins and history of computer viruses. The study provided an overview of computer viruses, including definitions, examples of common viruses, and instructions on how to protect a computer system from viruses.

AlBazzaz and AlMuhanna (2016) researched how to avoid computer viruses and malware threats. The study introduced the concept of computer viruses, as well as the harm and problems that can arise as a result of virus infection. The study addressed the importance of anti-virus software as well as its performance indicators. The research looked at cloud antivirus, which uses a powerful combination of virus monitoring technologies to protect your computer from all malware in the cloud computing environment. The study made recommendations for avoiding viruses and malware threats.

Khan *et al*. (2017) conducted a lab-based study on computer viruses and protection methods. The study looked into the possibility of a computer virus threat and how destructive it could be if executed on a specific machine. What countermeasures are available to protect computers from these threats? The study analysed data extracted from various scenarios and labs conducted in a test environment. According to the study's findings, proper security implementations and the use of up-to-date operating system patches and antivirus programs assist users in preventing data loss and viral attacks on the system.

Kasu Journal of Computer Science Vol. 1 No. 2 [June, 2024], pp. 134-150
https://doi.org//10.47514/kjcs/2024.1.2.001
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Al-Daoud *et al*. (2018) investigated computer virus strategies and detection. The research revealed that some problems must be solved in order to develop new reliable antivirus software, such as developing a new method to detect all metamorphic virus copies, developing new reliable monitoring techniques to discover new viruses, or attaching a digital signature and a certificate to each new software.

Kumar & Dey (2019) conducted a study on computer virus transmission. Focusing on the heightened attention researchers are giving to computer viruses compared to Trojans and worms. They explored virus control analysis across various networks, including mail networks, virtual networks, and wireless local area networks. The authors also introduced a mathematical model for computer virus transmission based on the classical Susceptible-Infected-Susceptible (SIS), Susceptible-Infected-Recovered (SIR), and Susceptible-Exposed-Infected-Recovered (SEIR) frameworks proposed by Kermack and McKendrick.

Savant and Kasar (2021) conducted research on computer virus attacks and their preventative mechanisms. The study provided definitions for viruses and elucidated terms such as virus phases, types, and worms. It outlined common symptoms of virus attacks and proposed solutions beyond relying solely on antivirus software. Additionally, the study addressed the future trajectory of computer viruses and concluded that the Internet's role in interconnecting computers encourages the spread of viruses. The authors offered recommendations for virus protection, emphasizing the importance of personal computer users taking proactive measures to safeguard their devices. They endorsed virus detection and preventive strategies as the simplest and most cost-effective methods to combat virus attacks, including keeping firewalls and antivirus software updated, avoiding risky internet browsing habits, and promptly deleting suspicious emails. Following these safety measures diligently can help users mitigate the risk of virus attacks on their personal computers.

Wang (2022) conducted an analysis of computer virus defence strategy based on network security. By delving into the propagation mechanisms and characteristics of computer network viruses, the study aimed to explore preventive measures, particularly focusing on their applicability in China. The research delved into the main strategies and technologies of computer network security, addressing current security challenges in computer network information and proposing corresponding solutions. Furthermore, the study provided a concise analysis and discussion on the spread of computer viruses across networks and suggested protection methods, with the intention of offering valuable insights to the industry.

Bhargava Choudhary & Gupta (2022) conducted a review on computer virus. The study provides readers with an overview to assess the potential threat posed by these malicious programs. The authors emphasised that understanding the magnitude of this threat entails analysing various factors. Their research suggests that creating a computer virus requires more perseverance than specialised expertise. To help users mitigate the risk of virus infections, the study offers recommendations aligned with standard computer security practices, serving as a defence mechanism against such threats.

Chalurkar, Tandekar & Deharkar (2024) conducted a study on hazards of computer viruses. The research provided a comprehensive definition of a virus and elucidated related terms such as malicious software, worms, and Trojan horses. It also highlighted the vulnerabilities of operating systems in relation to viruses and compared the strengths of Linux versus Windows. Additionally, the study outlined the current state of affairs concerning virus protection measures, emphasizing that aside from utilizing anti-virus software, there are other procedures that can help safeguard against viruses. Furthermore, the research explored the future trajectory of computer viruses and concluded that the Internet serves its purpose of interconnecting computers, thereby facilitating the distribution of viruses. Finally, the study offered recommendations for addressing virus-related challenges.

Kasu Journal of Computer Science Vol. 1 No. 2 [June, 2024], pp. 134-150
https://doi.org//10.47514/kjcs/2024.1.2.001
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

The research gap addressed by this study rest in the comprehensive examination of the effect of computer virus attacks, identification of common types of infections, and provision of preventive measures among computer users. While prior studies have explored various aspects of computer viruses, this paper contributes by synthesising findings from multiple angles, including reasons for virus attacks, common symptoms of infections, and effective preventive measures. Previous research has often focused on specific aspects such as malware incident prevention, virus detection methods, or historical perspectives of viruses. However, this study delves into a broader spectrum, encompassing the experiences and perspectives of computer users across different demographics, which include professionals, students and other computer users. Moreover, the study fills a gap in understanding the prevalence of various symptoms of virus infections and the effectiveness of different preventive measures. By surveying a diverse group of computer users, it provides valuable insights into the most common symptoms experienced by users and the preventive measures they find most effective

2.1 Objectives of the Study

As the use of computers and the internet as a means of connecting with the rest of the world has grown in today's society, so has the risk of contracting a computer virus. Computer viruses have become a worldwide problem because they can spread quickly via the internet and cause havoc. To combat the growing threat of these viruses, computer users must have comprehensive virus protection measures in place. The main aim of this research is to examine computer virus attacks and its preventive measures among computer users. However, the objectives of the research are as follow:

a) To identify the reasons which cause computer virus attacks among computer users.
b) To identify the common type of computer virus infection.
c) To suggest the possible preventive measures to safeguard the computer resources from virus attacks.

3. Methodology

The survey method was used for this study. Questionnaire was used as instrument for data collection. The questions in the questionnaire were constructed in line with the expected response of the respondents. The questions were all in options for respondents to choose. A total of seven questions were asked. 250 questionnaires were distributed through face-to-face contact with respondents at their respective locations. 246 respondents' data were considered for analysis, while 4 respondents' data were found to be incorrect or incomplete. On the basis of a convenient sampling method, the sample was drawn from professionals, students of tertiary institutions, and other personal computer users. The researchers were able to easily collect data from these categories. The questionnaire is divided into two sections, section A demography of the respondents (which include gender, age group and type of computer user) while section B contains the targeted questions to convey the entire enquiry (which include has their computer ever been infected with computer virus, reason for computer virus attacks, recognized symptoms of virus infection and best preventive measures against computer virus attacks).

4. Results and discussion

Kasu Journal of Computer Science Vol. 1 No. 2 [June, 2024], pp. 134-150
https://doi.org//10.47514/kjcs/2024.1.2.001
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

The gathered data were analysed using the Statistical Package for Social Science (SPSS) 22 and descriptive and inferential statistics to assess the study's objectives. The results of the analyses are presented below.

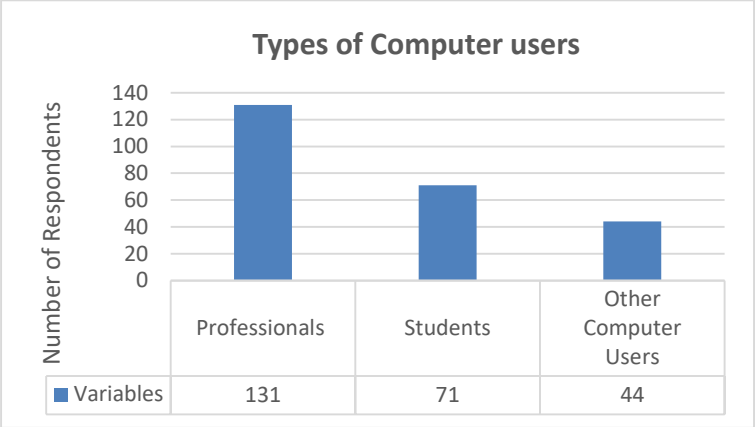

Figure 1: Types of computer users

This study explored the types of computer users. Respondents were asked to indicate the types of computer user they belong to, which include professional users, students of tertiary institutions and others users. Figure 1 above shows the type of computer users. The number of professionals cutting across various field is 131(53.25%), the number of students is 71(28.86%) while the number of other computers users is 44(17.89). This suggested that professionals use computer for professional task than other users.

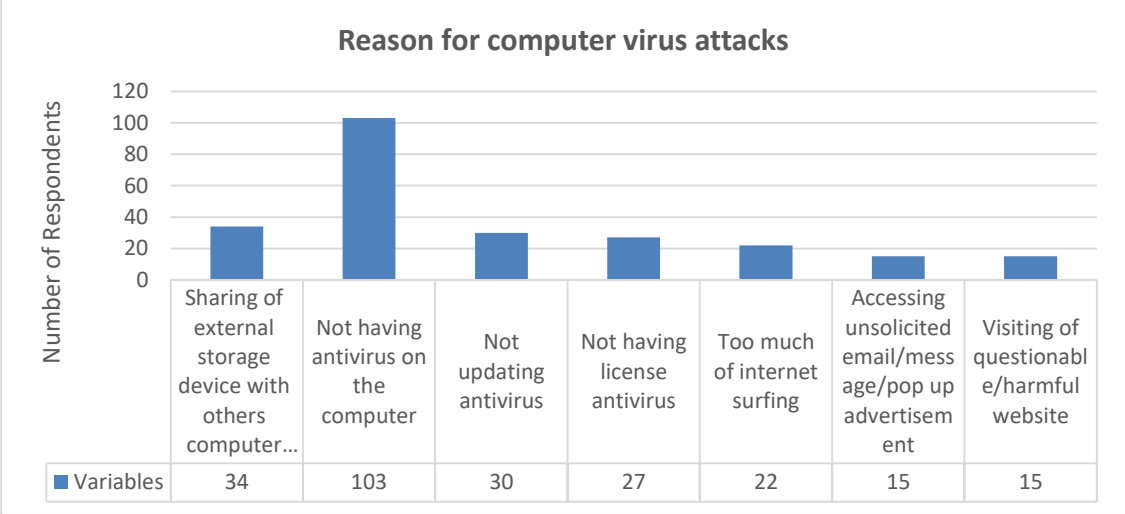

Figure 2: Reason for computer virus attacks

This study explores the reasons for computer virus attacks. Respondents were first asked if their computer has ever been infected with computer virus, all the respondents said yes, then the respondents were asked the reasons for computer virus attacks. Sharing of external storage device with others computers (such as flash/thumb drive, portable hard drive), not having an antivirus on the computer, not updating antivirus, not using license antivirus, too much of internet surfing, accessing unsolicited email/message/pop up advertisement and visiting of questionable/harmful website, were used as answer options.

Kasu Journal of Computer Science Vol. 1 No. 2 [June, 2024], pp. 134-150
https://doi.org//10.47514/kjcs/2024.1.2.001
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Figure 2 above shows the reasons for computer virus attacks as answered by the respondents: 34 (13.82%) respondents indicate sharing of external storage devices with other computers (such as flash/thumb drive, portable hard drive), 103 (41.87%) indicate not having an antivirus on the computer, 30 (12.19%) indicate that not updating antivirus, and 27 (10.98%) indicate not using license antivirus, 22 (8.94%) indicate too much of internet surfing, 15 (6.10%) indicate accessing unsolicited email/message/pop up advertisement, and 15 (6.10%) indicate visiting questionable/ harmful website.

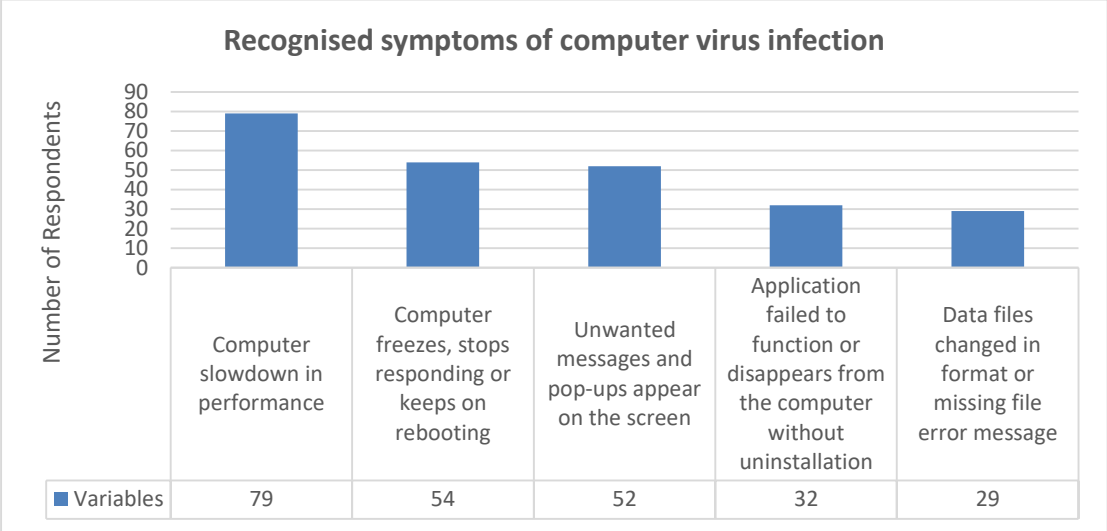

Figure 3: Recognized symptoms of computer virus infection

This study also explores the recognised symptoms of computer virus infection. Respondents were asked the recognized symptoms of computer virus infection. Computer slowdown in performance, computer freezes, stops responding or keeps on rebooting, application failed to function or disappears from the computer without uninstallation, data files changed in format or very difficult to reopen and computer display “missing file” error message, were used as answer options.

Figure 3 above shows various recognized symptoms of computer virus infection as answered by the respondents: 79 (32.11%) respondents indicate computer slowdown in performance, 54 (21.95%) respondents indicate computer freezes, stops responding or keeps on rebooting, 52 (21.14%) respondents indicate unwanted messages and pop-ups appear on the screen, 32 (13.01%) respondents indicate application failed to function or disappears from the computer without uninstallation and 29 (11.79%) respondents indicates data files changed in format or missing file error message.

Kasu Journal of Computer Science Vol. 1 No. 2 [June, 2024], pp. 134-150
https://doi.org//10.47514/kjcs/2024.1.2.001
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

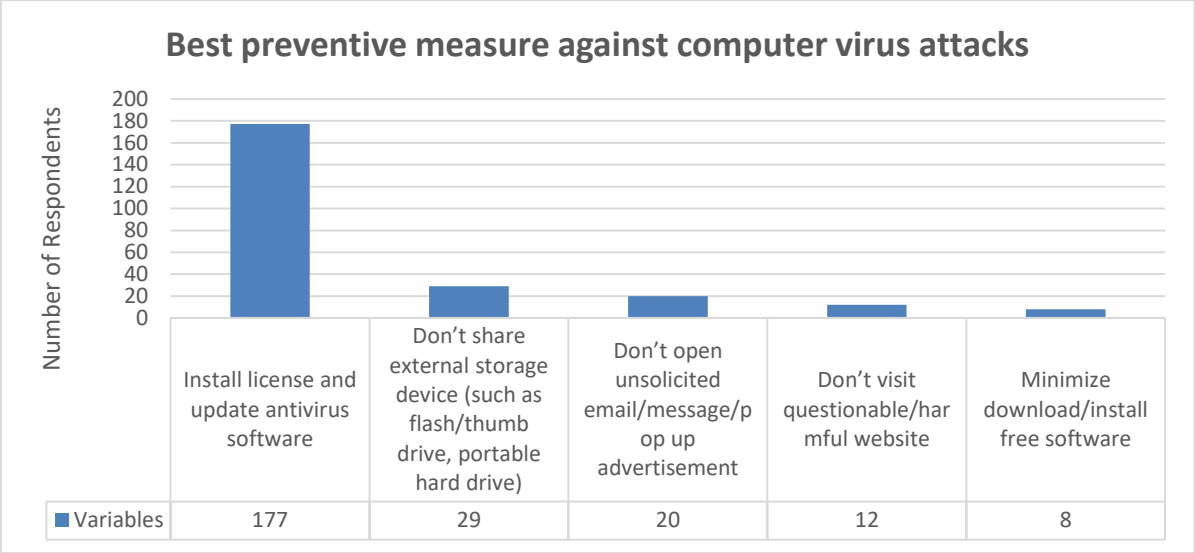

Figure 4: Best preventive measure against computer virus attacks

This study further explores the best preventive measure against computer virus attacks. Respondents were asked the best preventive measure against virus attacks. Install license and update antivirus software, don't share external storage device (such as flash/thumb drive, portable hard drive), don't open unsolicited email/message/pop up advertisement, don't visit questionable/harmful websites, minimize download/install free software, were used as answer options.

Figure 4 above shows different preventive measures against computer virus attacks believed to be the best as answered by the respondents: 177 (71.95%) respondents indicate install license and update antivirus software, 29 (11.79%) respondents indicate don't share external storage device (such as, flash/thumb drive, portable hard drive), 20 (8.13%) indicate don't open unsolicited email/message/pop up advertisement, 12 (4.88%) respondents indicate don't visit questionable/harmful website, 8 (3.25%) respondents indicate minimize download/install free software.

4.1 Discussion of Findings

The study's findings will be discussed in relation to each of the objectives outlined.

The first objective was to identify the reasons which cause computer virus attacks among computer users. The findings revealed that a high percentage (about 65.04%) claims that antivirus has high impact on computer virus attacks.

The second objective was to identify the common type of computer virus infection. These findings revealed that virtually all types of computer virus infections are common. 32.11% indicates computer slowdown in performance which are symptoms of memory resident virus, boot sector virus and worm infections. 21.95% indicates computer freezes, stops responding or keeps on rebooting which are symptoms of memory resident virus, boot sector virus, FAT virus and multipartite virus infections. 21.14% indicates unwanted messages and pop-ups appear on the screen which are symptoms of trojan, browser hijacker virus and web scripting virus infections. 13.01% indicates application failed to function or disappears from the computer without uninstallation and 11.79% indicates data files changed in format or missing file error message which both are symptoms of macro virus, direct-action virus, overwrite virus, file infector virus and polymorphic virus infections. These findings revealed that symptoms of all types and ways of computer

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

virus infection are prevalent. However, the findings further revealed that symptoms of memory resident virus, boot sector virus and worm are relatively common (about 32.11%) than symptoms of other types of viruses.

The third objective is to suggest the possible preventive measures to safeguard the computer resources from computer virus attacks. The findings revealed that the majority (about 71.95%) indicates installing license and updating antivirus software is the best preventive measures to safeguard the computer resources from virus attacks.

5. Conclusion

This study has provided a comprehensive overview of the effect of computer virus attacks and the preventive measures among computer users. The prevalence and severity of computer virus attacks have been highlighted, ranging from slowing down system performance to rendering data inaccessible or deleting files entirely. Through an extensive review of related works and empirical data analysis, this study has shed light on the common types of computer virus infections and the symptoms associated with them. The findings of this research emphasised the critical need for proactive measures to protect computer systems from virus attacks. Installing and regularly updating antivirus software emerged as the most effective preventive measure, as indicated by the majority of respondents. Additionally, avoiding unsolicited emails, refraining from visiting questionable websites, and minimizing the download/installation of free software were identified as important precautions to mitigate the risk of virus infections. Overall, this study underscores the importance of raising awareness among computer users about the threats posed by computer viruses and the necessity of implementing robust preventive measures. By understanding the reasons behind virus attacks and recognising the symptoms of infection, individuals can take proactive steps to safeguard their computer resources and minimise the impact of malicious software. It is imperative for both individuals and organisations to prioritise cybersecurity measures in today's digital landscape to mitigate the risks associated with computer virus attacks.

6. Recommendations

In the light of the findings and conclusion drawn from this study, the following recommendations are suggested towards preventing and protecting computer viruses and other malware from getting into computer and ensuring that computers are continuously protected from virus attacks.

1) It is crucial to educate computer users about the risks associated with computer virus attacks and the importance of implementing preventive measures. Conducting awareness campaigns, workshops, and seminars can help individuals understand the potential threats and how to protect themselves.
2) The study found that installing and regularly updating antivirus software emerged as one of the most effective preventive measures. Therefore, it is recommended that computer users ensure their antivirus software is up-to-date to protect against the latest threats.
3) Sharing external storage devices, such as flash drives or portable hard drives, was identified as a common reason for computer virus attacks. Therefore, individuals should exercise caution when sharing or using external devices, especially on multiple computers, to prevent the spread of viruses.

Kasu Journal of Computer Science Vol. 1 No. 2 [June, 2024], pp. 134-150
https://doi.org//10.47514/kjcs/2024.1.2.001
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

4) Avoiding unsolicited emails, messages, and pop-up advertisements, as well as refraining from visiting questionable or harmful websites, can help reduce the risk of virus infections. It is important to practice safe internet browsing habits and be cautious when clicking on links or downloading files from unknown sources.
5) Free software downloads can sometimes contain malware or viruses. Therefore, individuals should minimize the downloading and installation of free software from untrusted sources. It is recommended to only download software from reputable sources and verify the legitimacy of the software before installation.
6) In addition to antivirus software updates, individuals should implement other security best practices such as using strong passwords, enabling firewall protection, and regularly backing up important data. These measures can help enhance overall cybersecurity posture and mitigate the risk of virus attacks.
7) Organizations and individuals should establish incident response plans to effectively handle and mitigate the impact of virus attacks. These plans should include procedures for detecting, containing, and eradicating malware infections, as well as guidelines for restoring systems and data from backups. Regularly testing and updating incident response plans can ensure preparedness in the event of a virus attack.
8) Collaboration with cybersecurity professionals and organizations can provide valuable insights and expertise in combating virus attacks. Seeking guidance from certified cybersecurity professionals and staying informed about emerging threats and best practices can help individuals and organizations stay one step ahead of cybercriminals.
9) Implementing continuous monitoring and conducting regular risk assessments can help identify potential vulnerabilities and weaknesses in cybersecurity defences. By proactively identifying and addressing security gaps, individuals and organizations can better protect against virus attacks and minimize the likelihood of successful breaches.
10) Employees play a critical role in maintaining cybersecurity hygiene and preventing virus attacks. Investing in comprehensive training programs and awareness initiatives can empower employees to recognize and report suspicious activities, avoid risky behaviours, and follow established security protocols. Regularly reinforcing cybersecurity awareness can help foster a culture of security within organizations and contribute to overall resilience against virus attacks.

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Reference

AlBazzaz, J. M. A. and AlMuhanna, N. E. (2016). Avoiding computer viruses and malware threats. *International. Journal of Advanced Research in Computer and Communication Engineering*, 5 (11), 288-291. https://doi.org/10.17148/IJARCCE.2016.51161

Alison, G. J. (2020). What is a computer virus? Retrieved 13th September, 2023 from https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html

AV-Test Institute. (2023). Malware. Retrieved 13th September, 2023 from https://www.av-test.org/en/statistics/malware/

Bhargava, P. Choudhary, R. and Gupta, A. (2022). A review study on computer virus. *World Journal of Research and Review*, 14 (5), 39-44. www.wjrr.org

Bahukhandi, S. and Rana, S. S. (2016). Introduction and history of computer viruses. *International Journal of Scientific & Engineering Research*, 7 (12). 44-47. http://www.ijser.org

Chalurkar, M. S., Tandekar, P. and Deharkar, A. (2024). A study on hazards of computer viruses. *International Research Journal of Modernization in Engineering, Technology and Science*, 6 (5), 835-839. www.irjmets.com

Comodo Antivirus. (2020). What is a computer virus and how do they work? Retrieved 13th September, 2023 from https://antivirus.comodo.com/blog/computer-safety/what-is-a-computer-virus/

Ilmudeen, A. (2013). The impact of computer virus attacks and its preventive mechanisms among personal computer (pc) users. *The proceedings of 3rd International Symposium*, 6-7 July 2013, Oluvil, Sri Lanka. 97-103. http://ir.lib.seu.ac.lk/handle/123456789/382

Jovanović, B. (2023). Virus alert: Antivirus statistics and trends in 2020. Retrieved 13th September, 2023 from https://dataprot.net/statistics/antivirus-statistics/

Khan, H.A., Syed, A., Mohammad, A. & Halgamuge, M. N. (2017). Computer virus and protection methods using lab analysis. *The Proceedings* of *IEEE 2nd International Conference on Big Data Analysis*, 882-886. Beijing, China. https://www.semanticscholar.org/paper/Computer-virus
-and-protection-methods-using-lab-Khan-Syed/

Khan, I. (2012). An introduction to computer viruses: problems and solutions. *Library Hi Tech News*, 29(7), 8-12. http://dx.doi.org/10.1108/07419051211280036

Kumar, R. and Dey, S. (2019). Study of computer virus transmission. *International Journal of Research*

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

and Analytical Reviews, 14 (5), 542-549. www.ijrar.org

Liu, B. and Li, C. (2015). A new virus-antivirus spreading model. *The proceedings of 12th International Symposium on Neural Networks*, October 15-18, Jeju, South Korea, 481-488. https://doi.org/10.1007/978-3-319-25393-0_53

Peng, M., He, X., Huang, J. and Dong, T. (2013). Modelling computer virus and its dynamics. *Hindawi Publishing Corporation Mathematical Problems in Engineering*, 2013, 1-5. http://doi.org/10.1155/2013/842614

Rotich, E. K., Kimutai, M. S., Daniel, S. K. and Siele, L. (2014). Trends in computer viruses: a review. *Journal of Engineering, Design and Technology*, 3(3), 9-11. www.gifre.org

Savant, V. B. and Kasar, R. D. (2021). Computer virus attack and their preventive mechanisms: A review. International journal of Technology. 11(2), 78-82. https://doi.org/10.52711/2231-3915.2021.00011

Thakur, P. P. and Vaidya, S. (2017). The impact of computer virus attacks and its detection and mechanism among personal computer pc users. *International Journal of Science and Research*, 6 (6). 2245-2247. www.ijsr.net

Wang, P. (2022). Analysis of Computer Virus defence strategy based on network security. *Academic Journal of Computing & Information Science*, 5 (14) 33-39. https://doi.org/10.25236/AJCIS.2022.051405

Zheng, D. (2015). Study on the technology of detection and prevention of computer virus. *The proceeding of 3rd International Conference on Management, Education, Information and Control*, 585-589. https://doi.org/10.2991/meici-15.2015.104.

Kasu Journal of Computer Science Vol. 1 No. 2 [June, 2024], pp. 134-150
https://doi.org//10.47514/kjcs/2024.1.2.001

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Appendix 1: Research Questionnaire

1. Please indicate your gender:
   Male ☐ Female ☐

2. Please indicate your age:
   18 - 24 years ☐ 25 - 44 years ☐ 45 - 64 years ☐ 65 and above ☐

3. Please indicate the type of computer user you are:
   Professional ☐ Student ☐ Other computer user ☐

4. Has your computer ever been infected with computer virus?
   Yes ☐ No ☐

5. If yes, what is the reason for computer virus attack?
   Please tick your response from the below options:
   - Sharing of external storage device with others computer (such as flash/thumb drive, portable hard drive) ☐
   - Not having antivirus on the computer ☐
   - Not updating antivirus ☐
   - Not having license antivirus ☐
   - Too much of internet surfing ☐
   - Accessing unsolicited email/message/pop up advertisement ☐
   - Visiting of questionable/harmful website ☐

6. What is the recognised symptom of computer virus infection?
   Please tick your response from the below options:
   - Computer slowdown in performance ☐
   - Computer freezes, stops responding or keeps on rebooting ☐
   - Unwanted messages and pop-ups appear on the screen
   - Application failed to function or disappears from the computer without uninstallation ☐
   - Data files changed in format or missing file error message ☐

7. What is your best preventive measure against computer virus infection?
   Please tick your response from the below options:
   - Install license and update antivirus software ☐
   - Don't share external storage device (such as flash/thumb drive, portable hard disk ☐
   - Don't open unsolicited email/message/pop up advertisement ☐
   - Don't visit questionable/harmful website ☐
   - Minimize download/install free software ☐

Kasu Journal of Computer Science Vol. 1 No. 2 [June, 2024], pp. 134-150
https://doi.org//10.47514/kjcs/2024.1.2.001
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Appendix 2: Research Result

Gender of respondents

S/No	Gender	Frequency	Percentage (%)
1	Male	167	67.89
2	Female	79	32.11
	Total	246	100

Source: Field work (2023)

Age group of respondents

S/No	Age Group	Frequency	Percentage (%)
1	18-24 years	84	34.15
2	25-44 years	93	37.80
3	45-64 years	67	27.24
4	65 and above	02	0.81
	Total	246	100

Source: Field work (2023)

Type of computer user

S/N	Variables	Frequency	Percentage (%)
1	Professionals	131	53.25
2	Students	71	28.86
3	Other computer users	44	17.89
	Total	246	100

Source: Field work (2023)

Reason for computer virus attacks

S/N	Variables	Frequency	Percentage (%)
1	Sharing of external storage device with others computer (such as flash/thumb drive, portable hard drive)	34	13.82
2	Not having antivirus on the computer	103	41.87
3	Not updating antivirus	30	12.19
4	Not having license antivirus	27	10.98
5	Too much of internet surfing	22	8.94
6	Accessing unsolicited email/message/pop up advertisement	15	6.10
7	Visiting of questionable/harmful website	15	6.10
	Total	246	100

Source: Field work (2023)

Kasu Journal of Computer Science Vol. 1 No. 2 [June, 2024], pp. 134-150
https://doi.org//10.47514/kjcs/2024.1.2.001

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Recognized symptoms of computer virus infection

S/N	Variables	Frequency	Percentage (%)
1	Computer slowdown in performance	79	32.11
2	Computer freezes, stops responding or keeps on rebooting	54	21.95
3	Unwanted messages and pop-ups appear on the screen	52	21.14
4	Application failed to function or disappears from the computer without uninstallation	32	13.01
5	Data files changed in format or missing file error message	29	11.79
	Total	246	100

Source: Field work (2023)

Best preventive measure against computer virus attacks

S/N	Variables	Frequency	Percentage (%)
1	Install license and update antivirus software	177	71.95
2	Don't share external storage device (such as flash/thumb drive, portable hard drive)	29	11.79
3	Don't open unsolicited email/message/pop up advertisement	20	8.13
4	Don't visit questionable/harmful website	12	4.88
5	Minimize download/install free software	8	3.25
	Total	246	100

Source: Field work (2023)