Pasoon Azimi
612 Amelia Place
Ottawa, ON K1W 0A4

December 6, 2016

Claire Farley, TA
75 Laurier Avenue East.
Ottawa, Ontario

Dear Claire Farley:

As agreed in our September 21, 2016, contract, I am submitting the attached report entitled *The Benefits of Protecting Devices and Networks with Anti-Virus Software.*

This report examines the issues of unprotected devices and networks and provides sufficient reasons as to why users should begin protecting their devices with anti-virus software. It also discusses the history and the future of developing anti-virus software, various types of anti-virus software, as well as how this software can protect networks and electronic devices from malware.

I hope you find this report satisfactory. If you have any questions, feel free to contact me at pazim102@uottawa.ca

Sincerely yours,

Pasoon Azimi

Encl.: Research paper on *The Benefits of Protecting Devices and Networks with Anti-Virus Software.*

Benefits of Protecting Devices and Networks with Anti-Virus Software

Submitted
to
Olivia Vanderwal, Claire Farley, and Elena Ilina

by

Pasoon Azimi,
December 6, 2016

The purpose of this report is to inform student users of electronic devices about the advantages of using anti-virus software on their devices and networks. This will ensure students realize the full potential of anti-virus software and how it can ensure a safe user experience on their electronic devices and networks. It will teach readers about anti-virus software, the related cyber threats and how it can counter act these threats.

TABLE OF CONTENTS

LIST OF FIGURES AND TABLES **iii**

EXECUTIVE SUMMARY **iv**

1.0 INTRODUCTION **1**

2.0 BACKGROUND INFORMATION **1**

2.1 The History of Anti-Virus Software 1
2.2 Understanding Cyber Threats 2
2.3 How Anti-Virus Software Works 3

3.0 DISCUSSION OF FINDINGS **4**

3.1 Benefits of Anti-Virus Software 4
3.2 Anti-Virus Software Availability and Comparison 5
3.3 The Future of Anti-Virus Software 6

4.0 RECOMMENDATIONS **7**

5.0 CONCLUSION **7**

6.0 REFERENCES **8**

LIST OF FIGURES

Figure 1. Anti-Virus Software in Motion 4

Figure 2. Local Computer Network 5

Figure 3. The Best Anti-Virus Software for Windows 10 6

EXECUTIVE SUMMARY

The purpose of this report is to inform students about the benefits of protecting their electronic devices and networks with anti-virus software to alleviate the possible issues that come with using these devices.

Protecting devices and networks with anti-virus software is the best possible solution for protection against a plethora of malware in cyber space. These cyber threats can lead users into very dangerous problems that can ultimately ruin lives. It is in the best interest of users to protect their devices as soon as possible because they never know when they can get effected.

Research shows that the future of anti-virus software is very bleak. Anti-virus software technology is losing and will ultimately lose its reliability as the number of hackers is increasing at an alarming rate. As of now it is the best solution to a problem developers are constantly researching. Until newer software is developed, Anti-virus software is the best solution in protecting devices and networks.

1.0 INTRODUCTION

Today, technology can be found nearly everywhere. As the world progresses through this digital age a large portion of students possess some sort of electronic device. These devices store hundreds of emails, pictures, and sensitive information all while connected to wireless networks. Sadly, many users are oblivious to the threats situated with activities like surfing the web or downloading files on these devices. The false sense of safety users acquires from using their devices can lead to very troubling issues. Anti-virus software can alleviate this false sense of safety and ensure a safe user experience on any device.

As technology advances, the need for security and safety for this technology increases with it. As more powerful anti-virus software is released, more advanced cyber threats are also being designed to break down and manipulate this software. Issues like cybertheft, spam and virus acquisition are only a few from a large list of threats that can affect users. Cyber threats are affecting millions of people and ultimately ruining many lives. With anti-virus software installed, many of these issues can be prevented.

This report will ensure students realize the full potential of anti-virus software and provide them with enough reason to use anti-virus software on their devices and networks. It will inform readers on the history of anti-virus software, the various cyber threats that they can face and how anti-virus software can counter act these threats. It will then provide readers with the benefits of anti-virus software, a comparison of various anti-virus software available and then it will begin to expand on the future of anti-virus software.

2.0 BACKGROUND INFORMATION

As electronic devices progressed, security became an issue. Anti-virus software seeked to address these cyber threats by implementing various detection and scanning methods.

2.1 The History of Anti-Virus Software

The birth of anti-virus software came with the birth of the computer virus. The first ever major outbreak of a virus was named “Brain.” Brain is what lead to the development of anti-virus software. In early years, developers knew that viruses could be developed but not for the very purpose to carry malicious content. In early stages, viruses did not possess any malicious content until the internet was introduced in the 1990s. In the late 80s, right before internet was introduced, anti-virus software made a more prominent presence as popular companies like MacAfee began developing anti-virus for both hardware and software. There were many flaws in the design of these products due to the lack of communication available. With the release of the internet, the demand for anti-virus software increased as developers began to realize the full potential of viruses. Being able to upload, download, send, and run scripts gave hackers the foundation to design viruses with malicious content. (Sujith, 2013, p. 1)

2.2 Understanding Cyber Threats

As devices and networks become increasingly sophisticated, and stable, it is common to assume that cyber security becomes less of an issue. This is not the case. Presently, hackers are advancing at an alarming rate. (Castelluciu, 2015, p.55). As more robust

and complex anti-virus software is released; advanced viruses and cyber threats are also being released.

Due to the vastness of the internet, there are millions of cyberthreats users can encounter on nearly any device. The average user spends almost three hours a day on their mobile device, therefore mobile device users are a common target for hackers. Hackers send malicious software fragments with the intent to steal information. (Markelj & Zgaga, 2016, p.514)

According to Symantec (2015) in "The 11 most common computer security threats… And what you can do to protect yourself from them" more common cyber threats include viruses, spam, spyware, keystroke loggers, and Trojan horses.

A **virus** is a piece of software that can infect a device without the permission or knowledge of a user. Once on the device, a virus begins to duplicate itself, taking up storage, RAM and ultimately making the device extremely slow.

Spam is the most common piece of cyber threat today. Nearly every single user that uses the internet has an email and has encountered some sort of spam. Spam is mail that is automated to send to thousands of emails. Spam mail can be filled with various things like impersonation and malware.

Spyware on the other hand is a type of malware that is designed with the intent to spy on the user without their permission or knowledge. It monitors all user activity and can take control of the device.

A **keystroke logger** is a very dangerous piece of software. A keystroke logger installs itself, without the owner's knowledge or permission and then monitors and captures all activity that has been typed on their keyboard. For example, if a user decides to check his/her bank statement online and enters their bank card information and password into the website. A key logger would have access to their bank information because it would have kept track of all the keystrokes they pressed. Key logger is one of the most common ways cybertheft is accomplished.

Finally, **Trojans** are pieces of software that encapsulate threats on the exterior by appearing to perform legitimate actions on the exterior, once a user encounters a Trojan, it allows hackers to access that device (Symantec, 2015, p.1).

Many of these attack techniques can be combined and formed into one threat with increasing complexity. Because of these actions, security monitoring done by anti-virus software has become increasingly more difficult due to the sheer size and complexity of these attacks (Borrent, Carter, & Wespi, p. 165).

2.3 How Anti-Virus Software Works

There are many different types of anti-virus software with the same functionality. Scan a file and determine whether it is malicious or not. If it is malicious remove it immediately. Doing so may sound very easy when said, but anti-virus software's run on very complex algorithms and techniques.

As said explained by Zelster (2011) In “Detection Techniques,” a common way anti-virus software detect viruses is called **signature based detection**. The way signature based detection works is by analyzing very key elements of a specific file, these include components such as a series of bytes in the file or a specific section in the file. If the file possesses a very unusual element, the anti-virus software will flag the file as malicious and let the user know. A common issue with signature based detection is that it is unable to flag malicious files with signatures that have not been identified or developed yet. This can make hackers jobs a lot easier.

To counter act this, developers implemented **heuristics** into their anti-virus software. Heuristics are what allow anti-virus software to determine and discover new unidentified pieces of malware. Since anti-virus software programs lack the signature and identification for every single piece of malware, heuristics allow the software to test files in various ways and flag files that could ultimately harm the device.

Another detection method is **behavioral detection**. Behavioral detection is a method used by anti-virus software that looks at the specific behavior of a file. Behavior in this sense is the analysis of how a file or program executes. If the program that is being executed portrays unusual behavior like accessing the network, the anti-virus software will identify the previously unidentified malware and flag it.

Cloud-based detection or “Sandboxing” takes a specific file and tests it externally on another server. This detection method redirects any possible harm that can result in testing the file onto a different infrastructure to avoid any damage to the current device. (Zeltser, 2011, p.1)

In addition, anti-virus software provides **on-access scanning** and **full system scanning**. On-Access scanning makes sure the anti-virus software is constantly running in the background of the device. (Hoffman, 2012, p.1) Every file and program that is opened is scanned in real time as the device is being used to make sure there is no malicious content. This is extremely useful as it constantly watches over users to ensure the safest possible user experience on their device. Full system scanning is a scan that is done with the consent of the user. Whenever the user wants to complete a full system scan the user can do so by going into their anti-virus software and allowing the software to do so. During this scan, it is not recommended that the device is used. Full system scans are recommended to be done occasionally to ensure that the device is clean.

Explained in figure 1 below, when anti-virus software identifies malicious software (Interception), they quarantine the file and safely remove it from the device (Disinfection) and alert the user.

Anti-Virus Software in Motion

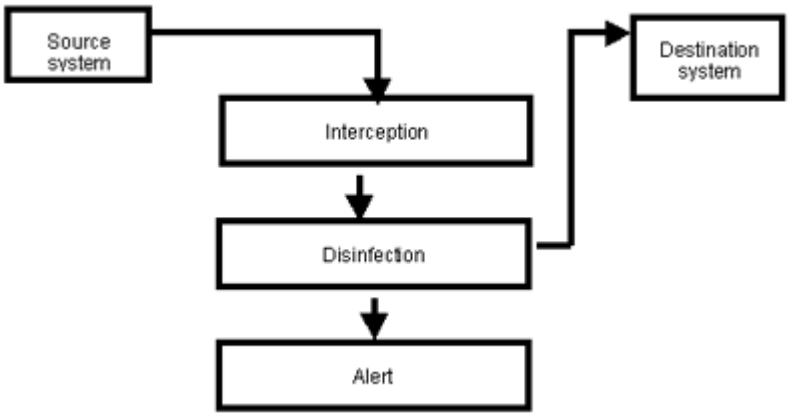

Figure 1: Anti-Virus Software in Motion. *Source:* Antibiotics and Vitamins for Your Computer!, 2012.

3.0 DISCUSSION OF FINDINGS

Anti-virus software seeks to provide the safest possible user experience when users are using their electronic device on their network. With the future of anti-virus software in trouble, the various anti-virus available now can keep users secure until the time for change arrives.

3.1 Benefits of Anti-Virus Software

The benefits of protecting devices and networks with anti-virus software are certainly present. Securing a device or network with anti-virus software can prevent the possibility of harming the device or the user themselves. Issues like cybertheft and identity theft are less apparent when anti-virus is installed because of its reliability and functionality. As Brandl (2006) explains "If the question is 'Should it run anti-virus software?' then the answer is usually an easy 'yes'." (para 1)

Additionally, If the anti-virus software that is being run has real time control applications like on access scanning, it is recommended that users disable scheduled full system scans and make sure users always keep their applications servers clean by uninstalling unnecessary programs and files. (Brandl, 2016, p. 34). Additional firewall features also come with many anti-virus software. Visualized in figure 2 below. Firewalls work by creating a barrier between a network and the internet. Everything that comes into local networks from the internet is monitored and flagged if unusual.

Local Computer Network

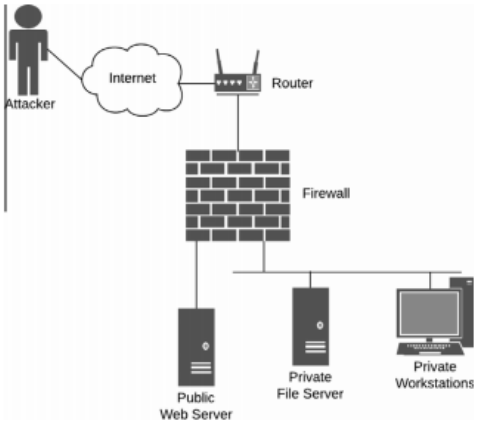

Figure 2. Local Computer Network. *Source:* Ben Asher & Gonzales, 2015.

Having some sort of security on devices is better than having no security at all, which is why there is no reason not to have anti-virus installed on a device. The design of malware is increasing at an alarming rate and getting protection now can alleviate the possible issues in the near future. Features like on-access scanning can constantly monitor users as they browse the web or use programs by looking over every possible threat. Cyber threats like spam, phishing, spyware, Trojans, and viruses can be less of a worry, Townsend describes, "Anti-virus software doesn't just seek to protect you from viruses, then, it seeks to protect you from all of this bad stuff." (p. 29)

3.2 Software Availability and Comparison

As of date, there are a wide variety of choices available when selecting anti-virus software. Companies are pushing their products with various features, optimization techniques, and reliability to guarantee security on consumer's electronic devices. With so many options, the choice isn't that easy. Presently, many companies are providing pre-installed anti-virus software on devices. Apple is well renown for their security and with many of their products, anti-virus by the name of Sophos is pre-installed. Sophos also sells a paid-for AV scanner for OS X to give users the option for extra security on their apple devices**. (**Anti-virus for Macs, 2010, p. 2**)** With the installation of windows, users are also given windows defender but are not limited to it.

To help users select from a variety of anti-virus software products, here is a list of some of the best anti-virus software available for the windows platform.

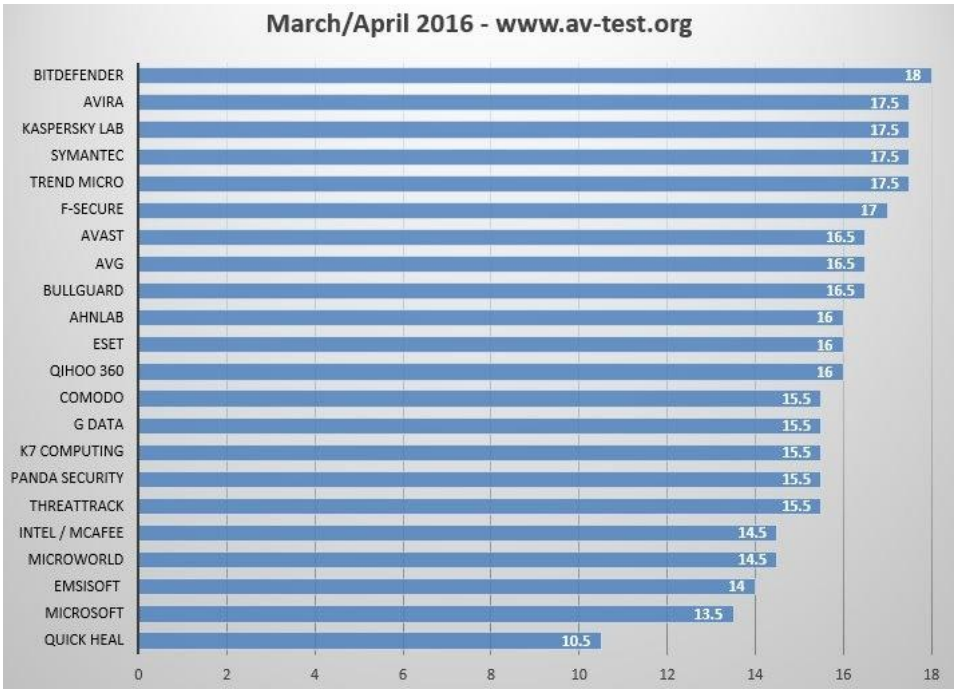

Figure 3. The Best Anti-Virus Software for Windows 10. *Source:* Verma, 2016.

Figure 2 above clearly shows users the various anti-virus software products available to use on their personal windows computers. This diagram can assist in facilitating the choice users have when selecting anti-virus software. Comparing protection, performance and usability are three things consumers look at when selecting an anti-virus. For mobile devices, there is also a plethora of software that is available on both app store and play store. Many of the software products mentioned in figure 2 have also been developed for mobile devices like AVG and MacAfee.

3.3 The Future of Anti-Virus Software

The rate at which hackers and saboteurs are designing newer malware with increasing complex designs is alarming. Malware is becoming exceedingly stealthy because many of the designers already have access to the anti-virus software they are trying to manipulate. Cyberthreats like phishing are only increasing in number and becoming less vulnerable to anti-virus software. The future of anti-virus software is looking very grim. (Spafford, 2014, p.4) Hackers having access to anti-virus software has put developers at an instant disadvantage.

In the article "Anti-virus: a technology update" (2010) Townsends explains that wherever there is a large concentration of users, like Facebook or twitter there will also be malware. As Apple grows its market, the number of hackers will also grow with it. The smart phone industry is currently on the rise and the anti-virus industry is aware of the attacks on various virtual machines. As of now none of these attacks have showed up in public but the anti-virus industry is aware that it will happen undoubtedly. (p.29**)** Townsend then states "If there are enough fridges connected to the internet, fridge malware will no doubt follow suit." (p. 29) If the device is connected to the internet, there will always be cyber criminals ready to attack.

In the coming years, anti-virus software will not be able to handle the complexity and strength of newly designed malware. Anti-virus software will still be present but as it progresses it will slowly diminish in strength. The question remains whether society will continue to take the same path in regards to cyber security or whether a new technology can be developed to continue to secure electronic devices and networks.

4.0 RECOMMENDATIONS

The research clearly shows that using electronic devices and networks without security can be very dangerous. Using anti-virus software is in the benefit of the user. The only thing anti-virus software can do for users is enhance the security on their electronic devices while providing a safe user experience. Hackers and saboteurs are becoming increasingly sophisticated and talented in what they do and its in user's best interest to protect themselves from the possible threats that these cyber criminals can develop.

5.0 CONCLUSION

Ben-Asher and Gonzalez (2015) explained it best by saying "Cyber-attacks—the disruption of computers' normal functioning and the loss of sensitive information through malicious network events—are becoming more widespread." (para 2) It is best to keep devices and networks as safe as possible. The future may not look bright for anti-virus software, but the future is not here yet. Anti-virus software is the best possible way to keep the devices used daily safe and secure. Until then users must use what they can to counter act hackers and saboteurs by protecting their devices and networks with Anti-Virus software.

6.0 REFERENCES

Ben-Asher, N., & Gonzales, C. (2015). Effects of cyber security knowledge on attack. detection. *Computers in Human Behavior*, *48*, 51-61. doi: 10.1016/j.chb.2015.01.039

Brandl, D. (2006). How good is anti-virus? *Control Engineering*, *53*, 34. doi: 10.1016/S1353-4858(12)70107-1

Borrent, M.,Carter, R., & Wespi, A. (2013). How is cyber threat evolving and what do organisations need to consider? *Journal of Business Continuity & Emergency Planning*, *7*, 162-171.

Castellucciu, M. (2015). Emerging cyber threats. *Strategic Finance*, *96*, 55.

Anti-virus for Macs. (2010). *Network Security*, *11*, 2 doi: 10.1016/S1353-4858(10)70131-8

Week 7: Antibiotics and Vitamins for Your Computer. (2012). GetMeWithThoseGreenEyes. Retrieved from: https://getmewiththosegreeneyes.wordpress.com/2012/10/15/week-7-antibiotics-and-vitamins-for-your-computer/

Hoffman, C. (2012). How Anti-Virus Software Works. Howtogeek. Retrieved from: http://www.howtogeek.com/125650/htg-explains-how-antivirus-software-works/

Markelj, B., & Zgaga, S. (2016). Comprehension of cyber threats and their consequences in Slovenia. *Computer Law & Security Review*, *32*, 513-525. doi: 10.1016/j.clsr.2016.01.006

Sujith, A. (2013). A Brief History of Antivirus Software. TechLineInfo. Retrieved from: http://www.techlineinfo.com/a-brief-history-of-antivirus-software/

Spafford, E.C. (2014). Is Anti-Virus Really Dead? *Computers & Security*, *44*, 4 doi: 10.1016/S0167-4048(14)00082-0

Symantec. (2015). The 11 most common computer security threats… And what you can do to protect yourself from them. Norton. Retrieved from: http://www.symantec-norton.com/11-most-common-computer-security-threats_k13.aspx

Townsend, K. (2010). Anti-virus: a technology update. *Infosecurity*, *7*, 28-31 doi: 10.1016/S1754-4548(10)70109-1

Verma, A. (2016). BitDefender, 22 Best Antivirus Software For Windows 10 Home PCs. FossBytes. Retrieved from: https://fossbytes.com/22-best-antivirus-software-windows-10-home-pc/

Zeltser, L. (2011). detection techniques. Search Security. Retrieved from: http://searchsecurity.techtarget.com/tip/How-antivirus-software-works-Virus-detection-techniques