The Importance of Network Security.

Fayed Troy
Computer Science Department
Hampton University
Hampton, VA
(Faculty Advisor: Dr. Chutima Boonthum-Denecke)

Abstract- This report will discuss the importance of network security. Network Security is important because it prevents hackers from gaining access to data and personal information. The issue in society is that users get their data stolen every day and are scared that their information is blasted out to the world. Within this paper I will talk to you about the importance of network security and how it can change your day-to-day life using cyber security. In addition, I will create a survey for computer science majors to see if network security is important. Also, I will send a survey to a DISA employee to get his perspective on this topic and his comments as well. The best method to incorporate both user input and research into this paper is to use user input to back up the research. User input will be a great addition because it gives the readers a real-world opinion on if this topic is valid.

1. Introduction

The use of computers and the creation of the internet is unequivocally one of the greatest tools in which humans rely heavily on today. However, there are many security issues that become prevalent as these devices are vulnerable in the hands of hackers. Devices like phones, laptops, and desktops are very unrestricted as they can be used to commit identity theft and even fraud. The worst part of all is that these actions are done anonymously. To stay safe from these attacks, it is great practice to always update one's computer as well as download security software that prevents malware and viruses.

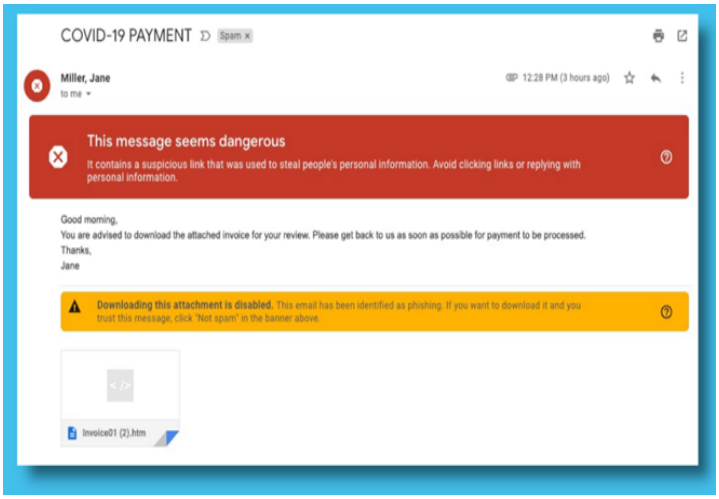

Figure 1: Virus in Email Example

In addition to understanding computer security and how to remain safe on the internet, it then becomes imperative to also be aware of the ethics of computer use to mitigate the issue of information stealing and immoral choices surrounding computers in general. Ethics is the moral understanding of how to conduct oneself through technology. (Tech Terms, 22). It is important to remember to respect other people's devices and to keep accountability for what one does when using different pieces of technology. Most people do not know what network security is. Network Security encompasses all the steps taken to protect the integrity of a computer network and the data within it.() Protecting a computer network is something you always need to think about. Any time of the day hackers can enter your network and see your history, what pictures you have taken, and personal information that you would not like to be seen by

the public. Things you need to be cautious with is links that have statements like “be cautious or we need your social security number. Below is an example of statements that could bug your devices:

If you were to click those links or pop-up ads; programmers can enter your software and see whatever they want. It is not just people; companies have these issues every day. When hackers get hold of such data, they can cause a variety of problems, including identity theft, stolen assets, and reputational harm.() One example is home security. Everyone has WIFI routers in their home that is connected to many devices, but network security is needed because routers could be exploited if not properly secured. A secured network is always good for the risk of data loss, theft, or sabotage. Here are some simple steps you can take to make sure a home network is secure: Change your router admin username and password, change the network name, activate encryption, double up on firewalls, turn off guest networks, and update router firmware(). Most cyber-attacks happen because of the user. There are a lot of strategies that you could use to ensure that users technology is safe and secure. *“The main issue concerning network security is how can it improve your daily life?”* The answer is protecting personally identifiable information (PII), protecting health information (PHI), personal information, intellectual property, and classified data. The ACM Code of Ethics is instilled into Cyber Security. It represents being honest, trustworthy, and respect privacy(). Honesty is an essential component of trustworthiness. A computing professional should be transparent and provide full disclosure of all pertinent system capabilities, limitations, and potential problems to the appropriate parties. The responsibility of respecting privacy applies to computing professionals in a particularly profound way. Technology enables the collection, monitoring, and exchange of personal information quickly, inexpensively, and often without the knowledge of the people affected.

2. Methodology

This study will use a combination of literature review, user surveys, and a subject-expert interview to collect data and gather results directly related to my thesis. Each methodology is explained as follows:

A. Problem Statement

Cyber Attacks are increasing day-by-day and is becoming a huge threat to users and the world. The main issue is users do not know how to secure their devices and make sure that it does not fall into the wrong hands. My research will make sure that users will always use network security to secure their data and know how to protect their information from hackers as well.

B. Literature Review

Experts have stated that most cyber-attacks come from the user. Users hitting pop-up blocks, asking if you accept cookies on a website. **Network Security: “**Network security is one of the most important aspects to consider when working over the internet, LAN or other method, no matter how small or big your business is. While there is no network that is immune to attacks, a stable and efficient network security system is essential to protecting client data” (). Technology corporations always need to be aware of harmful software. A minor software breach could leave a company in sham bulls, and have data leaked for their competitors to use and take an edge on their technology. “It has been suggested that 66 percent of small businesses would be forced to shut down following a data breach” according to STL. Due to data breaches companies face tremendous consequences because of it. Software needs to be secure and

safe here are some ways you can stop hackers from taking your information.

There are 6 main network security protections that are used: network segmentation, firewall, data loss prevention, sandboxing, email safety, and verification. “Network Segmentation is separating the infrastructure into discrete confined pieces; network segmentation successfully eliminates the design flaw and makes it extremely difficult for intruders to damage the entire system” ().

Network Segmentation:

Threats to cybersecurity in the IT industry are increasingly important to consider. Most enterprises still use antiquated perimeter security settings, yet they are no longer sufficient to safeguard their entire network. Many organizations are resorting to network virtualization, notably the Zero Trust security model and micro segmentations as security strategies to lessen security incidents faced by various firms, to combat this type of network security threat. Micro-segmentation security technique, which divides information into portions to give network and security teams the chance to have greater control and visibility over all data on each organization's network, is becoming a plan benefit for security teams as networks of various organizations are virtualized. These network security methods are used by businesses.

Firewall:

Firewalls will block malware and application-layer attacks. In addition, they react quickly to detect attacks within networks. Network security firewalls are very useful in traffic management as they minimize the spread of web threats. They also keep a visual on users by fraudulent traffic to access operating systems. A firewall is a barrier that stands between computers and networks to keep information safe and away from hackers. Most systems have security software that have pre-installed firewalls. A firewall acts as a protective barrier between a computer or network and the internet, blocking unauthorized access while allowing authorized communications. It can also be hardware- or software-based and helps to secure the network from various security threats like malware, cyber-attacks, etc. Within firewalls, there are four main types: packet filtering, proxy service, stateful inspection, and next generation. Packet filtering firewall analyze small amounts of data Proxy service firewall. Stateful inspection firewall. Next-generation firewall.

Data loss prevention:

In the current state of information security, we are always searching for new defensive mechanisms to guard against data breaches. More precisely, we wish to prevent cybercriminals from stealing or losing our sensitive data. To prevent cybercrime and protect sensitive data, several best practices can be followed:

- Use strong passwords and enable two-factor authentication.
- Keep software and systems up to date with the latest security patches.
- Regularly backup important data and store it securely.
- Educate employees on cyber security and social engineering tactics.
- Use encryption for sensitive data both at rest and in transit.
- Use a firewall to protect against network attacks.
- Monitor systems for suspicious activity and regularly review logs.
- Limit access to sensitive data and regularly review permissions.
- Use a reputable antivirus/anti-malware software.

- Have a plan in place for responding to a security breach.

Data loss prevention, or DLP, has being used more frequently as a solution to the issue. There are many reasons why businesses have failed to avoid data loss, but DLP has emerged to monitor data and identify potential breaches. You can locate your data in some of the following states:

Sandboxing

To defend networks from both emerging and enduring threats, sandbox environments function as a proactive layer of security. APTs are specialized, targeted attacks that are frequently used to breach corporate defenses and steal data. They are made to avoid detection, and they frequently go undetected by more conventional detection techniques. With the use of sandboxes, suspect programs can be safely run without endangering the host system or network. Additionally, it can be utilized for advanced malware detection, which adds another line of defense against growing security dangers like zero-day malware and covert attacks. To stop system failures and the spread of software vulnerabilities, sandboxes are present outside of the system. Sandboxes can play an important role in preventing system failures and the spread of software vulnerabilities. A sandbox is an isolated environment used to test and execute potentially dangerous code without affecting the system. By running potentially malicious software in a sandbox, security teams can identify and isolate any vulnerabilities or threats before they can cause harm to the rest of the system. This helps prevent system failures and reduce the risk of security breaches.

Email Safety:

Cybercriminals have changed the way in which they conduct business as well as conduct out their crimes. The most frequent email-borne threats are phishing and data breaches, but business email compromise attacks are not far behind: More than 90% of those surveyed admit that these types of invasions have happened at their company.

Verification:

There are many different forms of authentication and verification methods that are related to the idea and importance of network security and preventative measures that lead to danger. There are several forms of authentication and verification methods used to ensure the security of networks and prevent unauthorized access. Some common methods include:

1. Password authentication: users are required to provide a password to access a network or system
2. Two-factor authentication: in addition to a password, users are required to provide a second form of authentication, such as a fingerprint or security token
3. Biometric authentication: uses a user's unique physical characteristics, such as their face, fingerprint, or iris, to verify their identity
4. Digital certificates: used to verify the identity of a website or device and encrypt communications

These methods help prevent unauthorized access to networks and systems and reduce the risk of security breaches. By requiring multiple forms of authentication and verifying identities, organizations can ensure that only authorized individuals have access to sensitive information and systems.

C. User surveys

To fully assess the different topics surrounding this paper, I will be conducting a survey to understand the purposes that people play when using network platforms, how verse they are in the security of these platforms, as well as a space

to promote the growth and education to promote safety. We will collect data about cyber-security knowledge through conducting surveys. The purpose of the surveys is to understand the type of knowledge people know about security and how aware they are of certain things. We will analyze our findings along with our other sources of information to find patterns and make conclusions and recommendations related to our thesis.

1. Is Network Security Important?
    a. Short Answer
2. Do you know what Network Security is?
    a. Yes
    b. No
    c. Maybe
3. Do you have any anti-virus software on your devices?
    a. Yes
    b. No
    c. Maybe
4. If you do explain why, you have it?
    a. Short Answer
5. What anti-virus software do you know exist?
    a. Short Answer
6. Is it important to back up your files?
    a. True
    b. False
7. What is Cyber Security?
    a. Short Answer

3. Results

This section will cover the cumulative results obtained from our research methodology outlined in Section II. Our survey comprised of ten questions, and we had -- respondents complete the study. The appropriate responses of our overview
were anonymous and compromised of students in a non-computer science background. The discoveries of this study are as per the following.

Before the survey results are listed, below will be the questions asked on the survey with the different
answer choices.

Question 1:

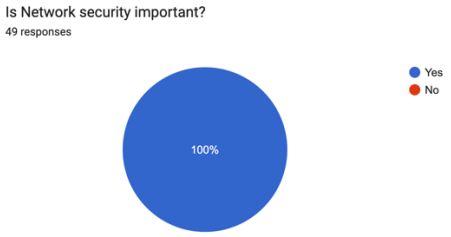

Figure 2: Question One Pie Chart

- 100% or 49 people responded to the first answer
- 0% or 0 people responded to the second answer

Question 2:

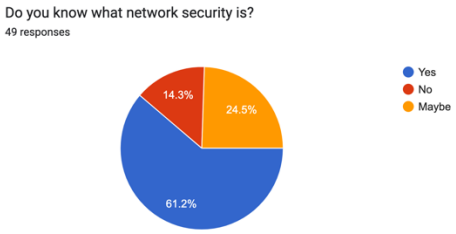

Figure 3: Question Two Pie Chart

- 61.2% or 30 people responded to the first answer
- 24.5% or 12 people responded to the second answer
- 14.3% or 7 people responded to the third answer

Question 3:

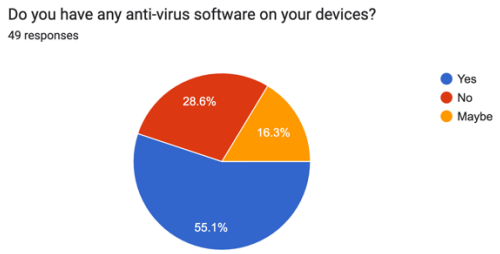

Figure 4: Question Three Pie Chart

- 55.1% or 27 people responded to the first answer
- 28.6% or 14 people responded to the second answer
- 16.3% or 8 people responded to the third answer

Question 4:

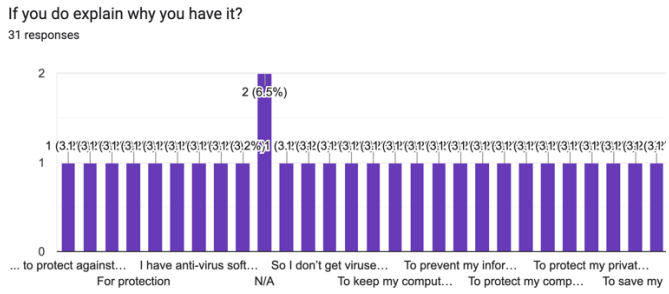

Figure 5: Question Four Bar Graph

- Answers Include:
  - To keep my computer clean and free of viruses
  - To protect myself from hackers
  - I have zscaler on my corporate laptop which is more like a VPN to provide a secure network connection so that others cannot hack the servers.
  - It came installed on my computer
  - To protect my computer
  - To keep my devices safe
  - I do not want viruses
  - To protect my computer from websites that could lead to virus or hacking
  - To save my information from hackers
  - To ensure I do not get virus on my computer

Question 5:

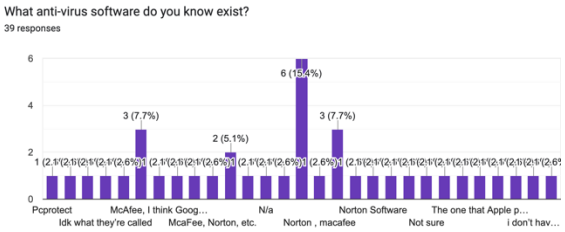

Figure 6: Question Five Bar Graph

- Answers Include
  - 10 people left response blank
  - 6 people responded Norton
  - 3 people responded McAfee
- Some individual answers
  - Norton Software
  - Protect
  - Apple software
  - Webroot and McAfee
  - Google

- North
- NordVPN
- Zscaler

Question 6:

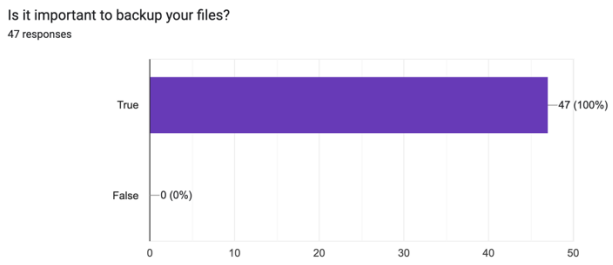

Figure 7: Question Six Bar Graph

- 100% or 47 people responded to the first answer
- 0% or 0 people responded to the second answer

Question 7:

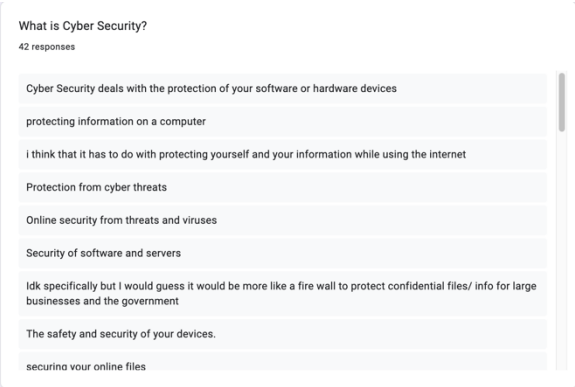

Figure 8: Question Seven Short Answer

- 7 people left the responses blank
- Some individual answer
  - The safety and security of your devices
  - Protection of the triad
  - Protection for our devices such as computers, phones, and tablets from and our personal information from being compromised
  - Is securing your online information
  - Protecting networks and information
  - Keeping my digital things safe
  - Protection of data and sensitive information
  - Computer Security
  - Security of software and servers
  - Protection against things like hacks
  - Protecting networks

4. Analysis

Students in school need to understand what Cyber-Security is and how it is used. This 7-question survey includes all that. When looking through the results of this survey most people knew what cyber was. When sending out these surveys I did not want all computer science majors filling it out. The more variety the better so I asked different major students to fill it out as well. Ex: Business, Journalism, Finance and more. There were a small percentage of people who left answers blank or did not answer at all. Most students who did not fill some questions out probably do not know cyber or don't have an interest in finding out. All the questions that were provided all had the same results. The first question: Is network security important? I know everyone must understand that your information is important, and I do not think students want their data on the internet. The most controversial question was Question 3: Only 55% of people keep their software safe from hackers. In other majors, professors should tell their students how important anti-software is. Question 4 and 5

were user input. Most people had different answers which was great but 25% of people left their responses blank. It is a problem when people do not know what anti-software is. The most used answer was Norton, and McAfee. Those were probably the computer science students most likely. For Question 7 everyone put different answers. 10% did not answer the question which is odd. To find out what the definition of cyber-security you can go on google or if you are a computer science major you should know it at the top of your head. While creating the survey it was a challenge to find questions that people would answer. Most students will not answer long open-ended question on a survey, True or False and Pick A, B, C, or D. Most people I know did not feel comfortable with this survey, but I am glad they took the time to fill it out. After completing this survey, I hope non-STEM majors understand that network security is very important and is needed on a day-to-day basis.

8. Conclusion

Computers are advancing and the internet and networking is only getting bigger and brighter. With this, there are many things to be aware of when in the use of the internet. While the internet is growing, the forms of malicious software that is being used. Not only are malicious software on the verge of destroying a person's computer, but it is on the verge of destroying a person's life as well. Computer technology and the use of networks become more widespread and essential in daily life and business operations, ensuring the security of those networks is increasingly important. This helps protect sensitive information, prevent data breaches and cyber-attacks, maintain privacy and confidentiality, and ensure the reliable functioning of critical systems. Network security helps ensure the confidentiality, integrity, and availability of sensitive information and critical systems by preventing unauthorized access, theft, and damage. This helps organizations maintain privacy and comply with legal and regulatory requirements and reduces the risk of business disruption from cyber-attacks or system failures. Also, Network security helps organizations maintain privacy, comply with legal and regulatory requirements, and reduce the risk of business disruption from cyber-attacks or system failures. By protecting sensitive information and critical systems, network security helps ensure the confidentiality, integrity, and availability of that information, and helps organizations maintain their operations and protect their assets. In conclusion, with the growth of the internet throughout human society, it can be stated that the framework of the internet and is has the power to quickly scale up an innovation within the computer science field has more influence than could have been possible without the internet.

ACKNOWLEDGEMENTS

This work is partly supported by the National Science Foundation CyberCorps: Scholarship for Service program under grant award# 1754054.

9. References:

1. Herzing University. (2017, August 2). *What is Network Security and Why is it Important?* https://www.herzing.edu/blog/what-network-security-and-why-it-important

2. *Importance of Network Security: Safety in the Digital World*. (n.d.). https://www.ecpi.edu/blog/importance-of-network-security-safety-in-the-digital-world

3. Abbey, N. (2022, August 23). *The Importance of Network Security in this Digital Age*. STL Blog. Retrieved February 2, 2023, from https://www.stl.tech/blog/the-importance-of-network-security-in-this-digital-age/

4. Cambridge College of Healthcare and Technology. (2022, February 10). *What Is Network Security & Why Is It Important?* Cambridge College of Healthcare & Technology. https://www.cambridgehealth.edu/blog/what-is-network-security-why-is-it-important/

5. T, T. (2021, July 19). *Why is Network Security Important?* Cyber Threat & Security Portal. Retrieved February 2, 2023, from https://cyberthreatportal.com/why-is-network-security-important/

6. Rouse, G. (2022, June 8). *What Is a Firewall and Why Is it Important in Cyber Security?* Datto. https://www.datto.com/blog/what-is-a-firewall-and-why-is-it-important-in-cyber-security#:~:text=Firewalls%20with%20an%20integrated%20intrusion,the%20spread%20of%20web%20threats.

7. *The Importance of Using a Firewall for Threat Protection | DigiCert*. (n.d.). https://www.websecurity.digicert.com/security-topics/importance-using-firewall-threat-protection

8. Fidelis Cybersecurity. (2022, June 29). *What is Network Data Loss Prevention? | DLP | Fidelis*. https://fidelissecurity.com/resources/edu/data-security/network-data-loss-prevention-dlp/#:~:text=Why%20is%20Network%20Data%20Loss,and%20augment%20employee%20security%20awareness

9. Veracode. (n.d.). *Data Loss Prevention | Veracode*. https://www.veracode.com/security/guide-data-loss-prevention

10. Tech, C. (2021, June 25). *6 reasons why Data Loss Prevention is necessary for business?* CloudSecureTech. https://www.cloudsecuretech.com/6-reasons-why-data-loss-prevention-is-necessary-for-business/

11. Tribe, R. (2022, December 1). *The Importance of Verification in Cybersecurity*. Network Perception. https://network-perception.com/the-importance-of-verification-in-cybersecurity/

12. November, E. D. (n.d.). *What Are the Benefits of Network Segmentation?* https://www.compuquip.com/blog/4-security-benefits-of-network-segmentation

13. *What Is Sandboxing? Sandbox Security and Environment | Fortinet*. (n.d.). Fortinet. https://www.fortinet.com/resources/cyberglossary/what-is-sandboxing

14. Rosencrance, L. (2021, September 23). *sandbox (software testing and security)*. Security. https://www.techtarget.com/searchsecurity/definition/sandbox

15. Coy, N. (2022, August 5). *Why Email Security Is Important - Safest Email Provider*. NeoCertified Secure Email. https://neocertified.com/blog/why-email-security-is-important/

16. Chkadmin, C. (2022, May 11). *Why Email Security is Important*. Check Point Software. https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-email-security/why-email-security-is-important/

17. Moore, M., PhD. (2022, July 25). *Cybersecurity vs. Information Security vs. Network Security*. University of San Diego Online Degrees. https://onlinedegrees.sandiego.edu/

cyber-security-information-security-network-security/#:~:text=Under%20this%20view%2C%20cybersecurity%20is,IT%20infrastructure%20from%20online%20threats.

18. GeeksforGeeks. (2022, June 13). *Difference between Network Security and Cyber Security*. https://www.geeksforgeeks.org/difference-between-network-security-and-cyber-security/

19. Rosencrance, L. (2021a, March 31). *antimalware (anti-malware)*. Security. https://www.techtarget.com/searchsecurity/definition/antimalware

20. *What is a cyberattack? | IBM*. (n.d.). https://www.ibm.com/topics/cyber-attack

21. Habte, F. (2022b, April 25). *What is Network Security? The Different Types of Protections*. Check Point Software. https://www.checkpoint.com/cyber-hub/network-security/what-is-network-security/