Digital Forensics and Cyber Security

Kevin Mondy
Cyber-Security
Hampton University
kmondyjr@gmail.com

Abstract- This report discusses Digital Forensics and Cyber-Security and different vulnerabilities that put the users at risk of compromising their sensitive data and making it available to attackers. With the raising of new threats aiming at technology, some people are not aware of hackers stealing their data. This study will discuss what Cyber-Security is and how many people are aware of what it all entails. This study will also recommendations on how to recognize attacks and learn basic terms to help inform the public. The study utilizes surveys of students from Hampton University so the authors can make the proper analysis and recommendations regarding the issue.

I. Introduction

Securing the uprightness and privacy of the data in the arrangement of complex systems is significant and testing. What is more, the greater part of the individuals who are associated with these systems is understudies. Interest and retribution might be essential explanations behind understudies engaging in digital wrongdoings. Often understudies don't know about the ramifications of cybercrime. Young ladies are the most discovered casualties of digital wrongdoing. Numerous reports Colleges and colleges show the digital assaults rates, with a significant number of hacking endeavors onto the data frameworks. While interpersonal organizations and bank account subtleties are likewise at higher hazard, instruction organizations are confronting dangers of losing significant licensed innovation and their examination information, for example, licenses granted to the educators and understudies, and the individual data about the understudies, staff, and workforce.

Due to the higher recurrence of hacking assaults on the foundations of advanced education, the requirement for digital mindfulness has been expanded. Cybercrime is a worldwide issue that has been overwhelming the sequence of media reports. It represents a danger to singular security and a much greater risk to huge global organizations, banks, and governments. Cybersecurity alludes to a lot of strategies used to ensure the uprightness of systems, projects, and information from assault, harm or unapproved get to. From a registering perspective, security involves cybersecurity and physical security both being utilized by ventures to ensure against unapproved access to server farms and other electronic frameworks. Data security, which is intended to keep up the classification, respectability, and accessibility of information, is a subset of cybersecurity. The utilization of digital security can help avoid digital assaults, information ruptures, and data fraud and can help in hazard the board.

Therefore, when discussing cybersecurity, one may ask "*What are we attempting to ensure ourselves against?*" The answer is to previous (i) Unapproved Access, (ii) Unapproved Deletion, and (iii) Unapproved Modification. The CIA Triad is a security model which represents Confidentiality, Integrity, and Availability. Confidentiality means keeping a client's information between you and the client, and not telling others including co-workers, friends, family. Integrity, in the context of computer systems, refers to methods of ensuring that data is real, accurate, and safeguarded from unauthorized user modification. Availability, in the context of a computer system, refers to the ability of a user to access information or resources in a specified location and in the correct format.

II. Methodology

This study used a combination of literature review and user surveys to collect data and gather results directly related to our thesis. Each stage of our methodology is explained as follows:

A. Problem Statement

The higher number of organizations and administrations that utilize digital platforms, the more hackers and criminals will target their vulnerabilities. It is imperative that people comprehend the dangers of utilizing new digital platforms and how to protect themselves as well as prevent these vulnerabilities.

B. Literature Review – Digital Forensics

Digital Forensics: To determine if cyber-forensics is still important today, it is important to first discuss what cyber-forensics is. Digital Forensics "is the investigation of digital data gathered as evidence in criminal cases." [1] Law authorization organizations and private firms battle cybercrime utilizing PC criminology to follow, find and concentrate

advanced data required for criminal examinations. PC legal sciences experts search hard drives to reveal erased or secret documents utilizing record recuperation projects and encryption translating programming. Notwithstanding PCs, these legal sciences experts are likewise adroit at get-together appropriate data from network waiters, data sets, cell phones, tablets, and other advanced gadgets.

"The computer forensics industry is predicted to grow by 17% between 2016-2026, according to the Bureau of Labor Statistics." [1] Due to higher caseloads, state and neighborhood governments are anticipated to enlist extra PC criminological science experts to stay aware of the interest. Inside and out media inclusion of neighborhood and public criminal cases/information breaks, alongside the prevalence of scientific TV programs, assist in more open mindfulness around the significance of PC legal science. Additionally, with the speed of propelling innovation in the present society, PC measurable science specialist calling will be popular to stay aware of the continually evolving scene. Across all businesses, innovation keeps on driving the fate of the world economy. PC legal science is turning out to be more famous across all fields to distinguish PC wrongdoings or ensure information.

There are six types of different forensics. They are computer forensics, network forensics, mobile device forensics, digital image forensics, digital video/audio forensics, and memory forensics. "Computer forensics is a field of technology that uses investigative techniques to identify and store evidence from a computer device" [2].

Computer Forensics: PC criminology can be a fundamental feature of current examinations. At the point when wrongdoing is carried out and an examination is begun, one of the more normal spots to search for signs is the PC or cell of a suspect. This is the place where a PC crime scene investigation proficient enters the image. At the point when a presume has been distinguished and their PC or phone was taken into proof, a PC legal science proficient goes looking for information that applies to the examination. While looking for data, they should be mindful to follow nitty-gritty strategies that permit their discoveries to be utilized as proof. The data they uncover, regardless of whether it be recorded, perusing data, or even metadata may then be utilized by indictment to make a convincing argument against the suspect. The information recuperated is regularly utilized as proof in criminal preliminaries, yet at times is recuperated for organizations after an information misfortune occurrence. Moreover, the hoodlums that PC criminology experts explore are not generally cybercriminals. Since nearly everybody utilizes a PC, there are regularly significant data on their gadget that can add to an examination. Network safety, then again, is more worried about safeguard. Digital protection experts work under an assortment of occupation titles; however, virtually every one of them works to assemble organizations and frameworks that are secure from likely assailants. Here and there they use hacking to test their organizations or the organizations of a customer to find spaces of shortcoming and support them.

Network Forensics: Network Forensics "is a sub-branch of the practice of digital forensics itself a branch of forensic science - whereby experts and law enforcement look into technology or data that may contain evidence of a crime or attribute evidence to suspects, cross-reference statements or check alibis." [3] Network criminology alludes to the examination and investigation of all traffic going across an organization associated with use in digital wrongdoing, say the spread of information taking malware or the examination of digital assaults. Law authorization will utilize network criminology to examine network traffic information collected from an organization associated with being utilized in a crime or a digital assault. Investigators will look for information that focuses on human correspondence, control of records, and the utilization of specific catchphrases for instance.

Mobile Device Forensics: Mobile device forensics is a part of computerized legal sciences identifying with the recuperation of advanced proof or information from a cell phone under forensically strong conditions. The expression cell phone for the most part alludes to cell phones; in any case, it can likewise identify with any computerized gadget that has both inside memory and correspondence capacity, including PDA gadgets, GPS gadgets, and tablet computers. Some of the portable organizations had attempted to copy the model of the telephones which is illicit. Thus, we see such countless new models showing up consistently which is the forward advance to the further ages. The process of cloning the cell phones/gadgets in wrongdoing was generally perceived for certain years; however, the criminological investigation of cell phones is a moderately new field, dating from the last part of the 1990s and mid-2000s.

Digital Image Forensics: Digital image forensics is "the discipline focuses on image authenticity and image content. This helps law enforcement leverage relevant data for prosecution in a wide range of criminal cases, not limited to cybercrime." [4] Advanced picture legal sciences are performed on nearby machines and can be utilized in both open and shut source examinations. It's a profoundly modern field of examination that requires a few programming applications and expert preparation. The extent of advanced picture criminology is so wide coming to because computerized symbolism is information-rich, by correlation with film photography. Utilizing an assortment of strategies, advanced picture criminology specialists can mine beginning and end from camera properties to individual pixels for data.

Digital Video/Audio Forensics: "Audio and video are the digitalized source of evidence that can be found at the scene of a crime or with the victim or the accused in the form of audio-video from a mobile device or any CCTV footage." [5] Such sorts of computerized confirmations are of most extreme significance in common or criminal cases. Hence, sound and video criminology are the main part of scientific science in the digitalized period. In measurable science, sound video criminology structures three fundamental standards like obtaining, investigating, and assessment of sound and video accounts that are permissible in the courtroom. One of the principal errands of sound and video criminological specialists is to set up the genuineness and validity of the advanced proof. The legal assessment of sound and video is done to upgrade the accounts to further develop discourse clarity and perceptibility of the sounds.

Memory Forensics: "Memory forensics is the process of capturing the running memory (Random Access Memory, RAM) of a device and then analyzing the captured output for evidence of malicious software." [6] Dissimilar to hard-circle legal sciences where the document arrangement of a device is cloned and each record on the plate can be recuperated and investigated, memory criminology centers around the genuine projects that were running on a device when the memory dump was captured.

Study on Privacy and security Awareness: In 2018, 1,024 specialists from 7 industry divisions participated in the State of Privacy and Security Awareness study and were presented requests relating to the whole of the above pieces of assurance and security. The consequences of this study were stunning.

- 75% of representatives needed security attention somewhat and addressed less than 90% of the inquiries accurately.
- 77% of chiefs (or more) were found to need security mindfulness contrasted with 74% of lower laborers.
- In 2017, 8% of representatives got phishing questions wrong. This year, 14% of representatives neglected to address the inquiries accurately.
- There was likewise an absence of understanding email dangers, Business Email Compromise (BEC) tricks, which 58% of representatives neglected to accurately characterize.
- While 8 out of 10 workers could recognize phishing messages in the test, 18% decided to open a surprising connection or snap on a connection in an email from an obscure source to discover where it went. In view of these measurements there is a gathering out in the labor force that are uninformed what digital protection is and that mindfulness should be vital. A method for expanding mindfulness is through the school local area. There was a study done on undergrads in Tamil Nadu. The point of the review is to investigate the familiarity with network protection on undergrads in Tamil Nadu by centering different security dangers in the web. This study inspects the understudies' mindfulness and the degree of mindfulness about the security issues. The outcomes from the study are recorded beneath.
- Over 70% of understudies from every one of the urban communities are cognizant with regards to the fundamental infection assaults and are utilizing antivirus programming (refreshing oftentimes) or Linux stages to shield their framework from infection assault.
- 11% of them are utilizing antivirus however they are not refreshing the antivirus programming. Over 97% of them don't have the foggiest idea about the wellspring of the infection
- Only 10 students from overall 379 claimed that they will complain about this phishing mail/messages to Cyber Crime wing.
- Students are more unsafe in social networks, and they are aware of phishing and virus attack
- The cyber security awareness among college
- students in Tamil Nadu are measured as 69.45%. in which male is 38.6% and female is 30.85%.

C. Attacker Techniques

Ransomware assaults are accepted to cost unfortunate casualties billions of dollars consistently, as programmers convey advancements that empower them to truly seize an individual or association's databases and hold the entirety of the data for emancipate. The ascent of cryptographic forms of money like Bitcoin is attributed with energizing ransomware assaults by permitting buy-off requests to be paid secretly. There were some statistics done in 2018 by the phoenixNAP and some of them were very alarming. [8]

- "50% of a surveyed 582 cybersecurity professionals do not believe their organization is prepared to repel a ransomware attack."
- "75% of companies infected with ransomware were running up-to-date endpoint protection."
- "A new organization will fall victim to ransomware every 14 seconds in 2019, and every 11 seconds by 2021."
- Almost half of the ransomware incidents reported in 2018 involved healthcare companies.

Crypto Jacking is another major hacking tactic. This is the digital currency development likewise influences digital security in different manners. For instance, crypto jacking is a pattern that includes digital crooks capturing outsider home or work PCs to mine for cryptographic money. Since digging for digital currency requires huge measures of PC handling influence, programmers can profit by furtively piggybacking on another person's frameworks. For organizations, crypto-jacked frameworks can cause genuine execution issues and expensive down time as IT attempts to find and resolve the issue.

- Crypto-jacking activity surged to its peak in December 2017, when more than 8 million crypto-jacking events were blocked by Symantec. While we have seen a slight fall in activity in 2018, it is still at an elevated level, with total crypto-jacking events blocked in July 2018 totaling just less than 5 million.

The next type of cyber-attack is called a **Man in the Middle attack** (MitM attack). This attack is when a hacker gets in between the communication of a client and a server. Some types of this attack include Session Hijacking and IP spoofing. Session Hijacking is when "an attacker hijacks a session between a trusted client and network server. The attacking computer substitutes its IP address for the trusted client while the server continues the session, believing it is communicating with the client." [9] Diagrams are shown below that explain how this attack works.

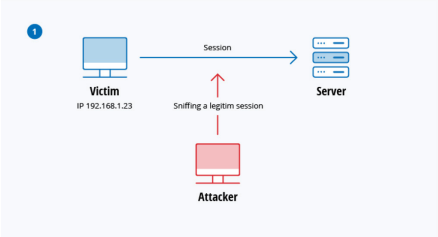

Figure 2: Session Hacking Example

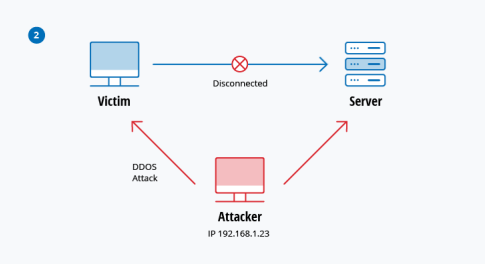

Figure 3: Session Hacking Example

IP spoofing works differently than a MitM attack. This attack tricks a system into thinking that it is communicating with a trusted system. It is however communicating with the hacker instead.

The next cyber-attack is called a **Drive-by Attack**. This attack is defined as being a way that hackers spread malicious software. Hackers look for low-security websites and insert malware into the HTML code. They do this because when a user clicks on that website then the user is now downloading the malware onto the machines. This attack is dangerous because the user does not have to click on anything for this malware to download. The way to mitigate this attack is to keep all internet browsers updated and operating systems up to date as well.

A **Password Attack** is also another attack hackers use to gain access to information. The most common types of password attacks are brute-force and dictionary attacks. A brute force attack is an attack where a hacker uses a different password in hope that one works. A dictionary attack is a hacker uses a list of common passwords to access a user's computer and network. A safeguard against these types of attacks is to implement a policy that lockouts an account. This will lock an account after a couple of wrong passwords.

An **SQL Injection Attack** is when a hacker executes a query to a database through the input data from a client to a server. The commands are inserted into a data plane to run pre-defined SQL commands. If the SQL injection is successful the injection exploits "can read sensitive data from the database, modify (insert, update or delete) database data, execute administration operations (such as shutdown) on the database, recover the content of a given file, and, in some cases, issue commands to the operating system." [9] These attacks only work if a website uses dynamic SQL. A SQL injection is very common with applications known as PHP and ASP. This is because these applications are older than most. There are ways a person would protect themselves from an attack like this. The first way is to change the permissions on a database. The next way is to stick to set procedures and prepared statements that help prevent attacks like this.

The next hackers use is an attack called **Cross-site Scripting Attack**. These attacks use a web resource to run a script to the person's browser or script application. The hacker inserts malicious JavaScript into a website database. When the person "requests a page from the website, the website transmits the page, with the attacker's payload as part of the HTML body, to the victim's browser, which executes the malicious script." [9] This attack can cause a person to have their cookies stolen, log keystrokes, take screenshots, access, and control their machines, and collect information about their respective networks. A diagram is used to show how this attack works.

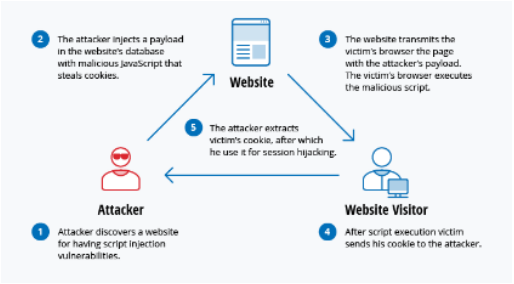

Figure 4: SQL Injection Attack Example

To prevent an attack like this, developer can clean their data input by users using an HTTP request. Another way to prevent this attack is to always check to see if data is correct before sending it back to a user.

An **Eavesdropping Attack** works when network traffic is intercepted. The purpose of this attack is to obtain credit card information, passwords, and any confidential information that a user may be transmitted over a network. There are two types of eavesdropping attacks, passive and active. Active eavesdropping is when the hacker is actively attempting to gain information by hiding as a friendly person. They do this through probing, scanning, and tampering. Passive eavesdropping is when a hacker detects the information by listening to the message transmissions in the network. It is important to detect passive attacks before active. This is because it takes longer for a person to recognize a passive attack is happening before an active one. The best way to mitigate this attack is to implement data encryption.

The next type of attack is known as a **Birthday Attack**. These attacks verify the strength of a message, software or digital signals using hash algorithms. "A message processed by a hash function produces a message digest (MD) of fixed length, independent of the length of the input message; this MD uniquely characterizes the message. The birthday attack refers to the probability of finding two random messages that generate the same MD when processed by a hash function." [9] It is very hard to detect a replacement if the attack is done correctly.

The last attack is known as a **Malware Attack**. This is defined as unwanted software that is installed in a person's system without the person's consent. The type of malware are macro viruses, file infectors, system or boot-record infections, polymorphic viruses, stealth viruses, trojans or worms, adware, and spyware.

- Macro viruses are a type of virus that infects applications like Word or Excel. They attach to an application start-up process. This works when the application is opened the virus will replicate itself and it attaches itself to the computer.
- File infectors are infectors that attach themselves to executable code.
- System or boot-record infections is a virus that attaches to a boot record on a hard disk. This will act when a system is started. The virus will attach itself to the memory.

- Polymorphic viruses are viruses that "conceal themselves through varying cycles of encryption and decryption. The encrypted virus and an associated mutation engine are initially decrypted by a decryption program." [9] The way to combat these viruses are through anti-virus software and free open-source tools to detect them.
- Stealth viruses are viruses that take over the functions of systems to hide. These viruses work because they attack detection software, so they report false positives.
- Trojans are a type of malware that hides in a program until it is time for it activates. There is a big difference: a virus self-replicates while a trojan does not.
- Worms are a type of malware that does attach to a host file but operates on its own. Worms attach themselves to a contact list in a person's email and spread that by sending copies of themselves to other people.
- Adware is a "software application used by companies for marketing purposes; advertising banners are displayed while any program is running. Adware can be automatically downloaded to your system while browsing any website and can be viewed through pop-up windows or through a bar that appears on the computer screen automatically." [9]
- Spyware is a program that is used to stall information about a person's habits. When spyware is installed, it is unaware to the user that they are being watched.

These types of attacks are only the most common attacks. It is important to raise awareness that these attacks are happening and how to recognize them.

D. User Surveys

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. What is Cyber-Security?
    a. It is an ongoing effort to protect Internet-connected systems and the data associated with those systems from unauthorized use or harm.
    b. It is the name of a comprehensive security application for end users to protect workstations from being attacked.
    c. It is a standard-based model for developing firewall technologies to fight against cybercriminals.
    d. It is a framework for security policy development.
2. Which of the following should you do to restrict access to your files and devices?
    a. Update your software once a year.
    b. Share passwords only with colleagues you trust.
    c. Have your staff members access information via an open Wi-Fi network.
    d. Use multi-factor authentication.
3. Backing up important files offline, on an external hard drive or in the cloud, will help protect your business in the event of a cyber-attack.
    a. True
    b. False
4. Which is the best answer for which people in a business should be responsible for cybersecurity?
    a. Business owners. They run the business, so they need to know cybersecurity basics and put them in practice to reduce the risk of cyber-attacks.
    b. Managers, because they are responsible for making sure that staff members are following the right practices.
    c. All staff members should know some cybersecurity basics to reduce the risk of cyber-attacks.
    d. IT specialists, because they are in the best position to know about and promote cybersecurity within a business.
5. Which of the following is the best answer for how to secure your router?
    a. Change the default name and password of the router.
    b. Turn off the router's remote management.
    c. Log out as the administrator once the router is set up.
    d. All of the above.
6. Cyber criminals only target large companies?
    a. True
    b. False
7. VPN is a network connection method for creating an encrypted and safe connection.
    a. True
    b. False
8. Which of the following is an example of a "phishing" attack?
    a. Sending someone an email that contains a malicious link that is disguised to look like an email from someone the person knows
    b. Creating a fake website that looks nearly identical to a real website to trick users into entering their login information
    c. Sending someone a text message that contains a malicious link that is disguised to look like a notification that the person has won a contest
    d. All of the above
9. Criminal's access someone's computer and encrypt the user's personal files and data. The user is unable to access this data unless they pay the criminals to decrypt the files. This practice is called …
    a. Botnet
    b. Ransomware
    c. Driving
    d. None of the Above
10. What is spyware?
    a. When a cybercriminal takes on your identity
    b. The clothing James Bond wears
    c. Software that collects data from your computer
    d. A website that sells on personal data

III. 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 204 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:

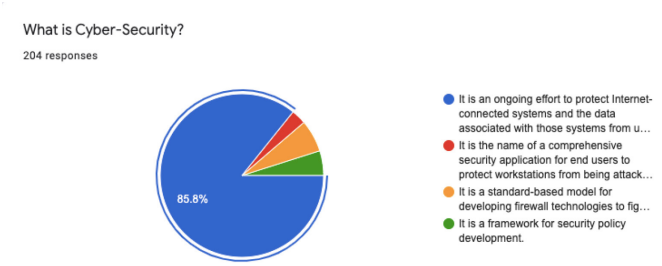

Figure 5: Question One Pie Chart

- 85.9% or 174 people responded to the first answer
- 6.4% or 13 people responded to the third answer
- 4.9% or 10 people responded to the third answer
- 2.9% or 6 people responded to the third answer

Question 2:

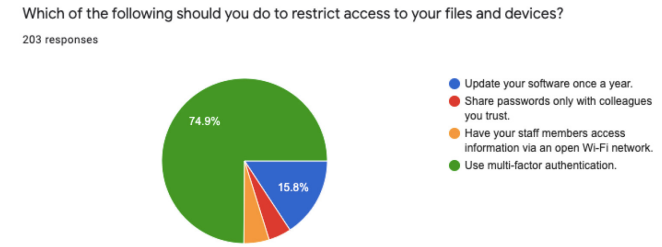

Figure 6: Question Two Pie Chart

- 74.9% or 152 people responded to the fourth answer
- 15.8% or 32 people responded to the first answer
- 4.9% or 10 people responded to the third answer
- 4.4% or 9 people responded to the second answer

Question 3:

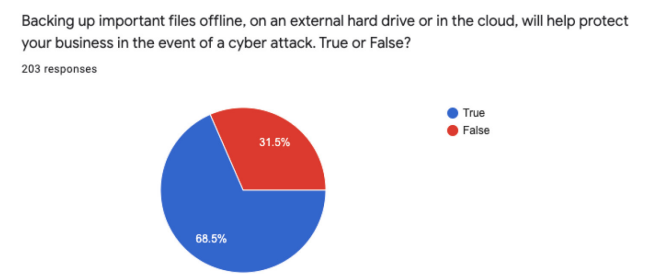

Figure 7: Question Three Pie Chart

- 68.5% or 139 people responded True
- 31.5% or 64 people responded False

Question 4:

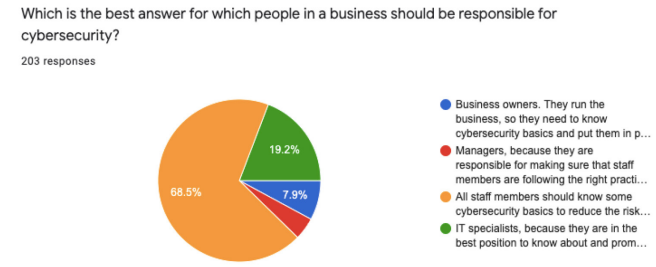

Figure 8: Question Four Pie Chart

- 68.5% or 152 people responded to the third answer
- 19.2% or 32 people responded to the fourth answer
- 7.9% or 10 people responded to the first answer
- 4.4% or 9 people responded to the second answer

Question 5:

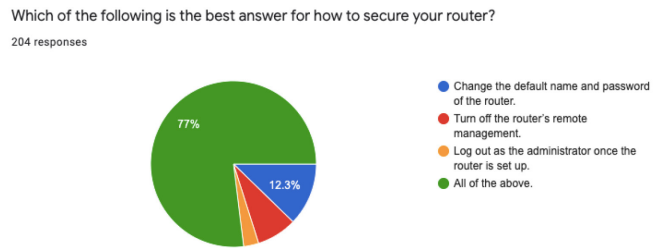

Figure 9: Question Five Pie Chart

- 77% or 157 people responded to the fourth answer
- 12.3% or 25 people responded to the first answer
- 7.8% or 16 people responded to the third answer
- 2.9% or 6 people responded to the second answer

Question 6:

Figure 10: Question Six Pie Chart

- 91.6% or 185 people responded False
- 8.4% or 17 people responded True
- 2 people left the question blank

Question 7:

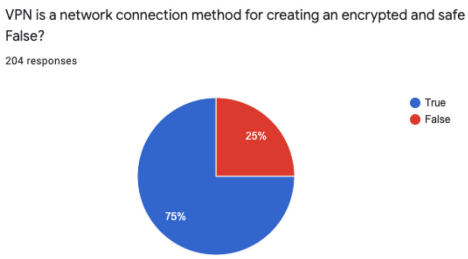

Figure 11: Question Seven Pie Chart

Cyber Security? Who Knows About It?

- 91.6% or 153 people responded True
- 8.4% or 51 people responded False

Question 8:

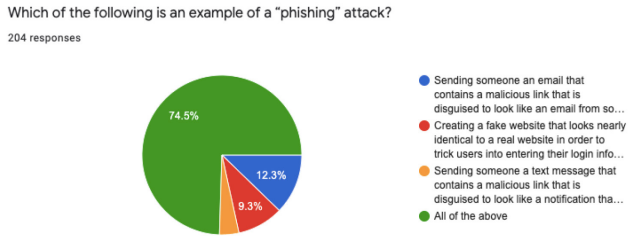

Figure 12: Question Eight Pie Chart

- 74.5% or 152 people responded to the fourth answer
- 12.3% or 25 people responded to the first answer
- 9.3% or 19 people responded to the second answer
- 3.9% or 8 people responded to the second answer

Question 9:

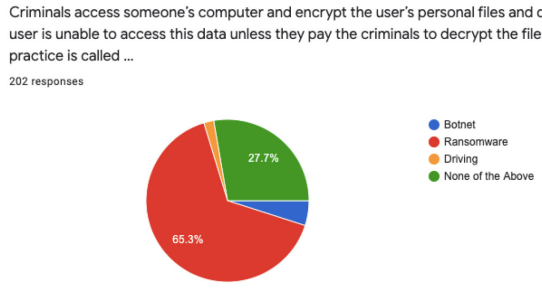

Figure 13: Question Nine Pie Chart

- 65.3% or 152 people responded to the third answer
- 27.7% or 25 people responded to the fourth answer
- 5% or 19 people responded to the first answer
- 2% or 8 people responded to the second answer

Question 10:

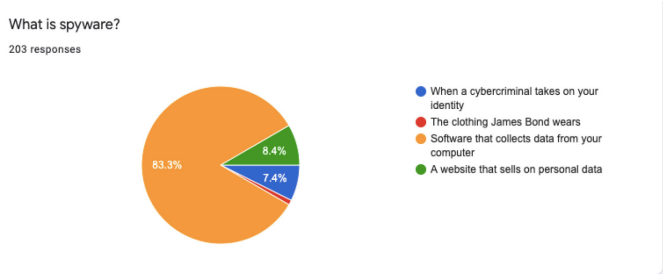

Figure 14: Question Ten Pie Chart

- 83.3% or 169 people responded to the third answer
- 8.4% or 17 people responded to the fourth answer
- 7.4% or 15 people responded to the first answer
- 1% or 2 people responded to the second answer

IV. Analysis of Results

We discussed what Cyber-Security was and its definition. When looking at the first question majority of the people understood the definition of cyber-security. It is safe to assume that people understand the basic definition of what Cyber-Security is. There was a small percentage of people who however didn't get this question right. This could be because of a couple of things. The first reason is that students truly don't know cyber-security is or they were just rushing through the survey. The second question results were very like the first response results. The majority of the people got the answer right. The next answer people selected was to update your software once a year. This lets me know that some people don't understand what multi-factor authentication is and don't know the risk of only updating your software once a year.

The third question results were in, and these results were closer to 50/50. Only 68.5% of people got this answer right. It is safe to say that for the 31.5% of people who got this wrong don't understand the importance of backing up data, whether its personal or at a business, is. When it came to question four majority of the people got this question right as well. However, like the third question less than 70% of the people got this question wrong. The next closest answer was it was the job of IT people to take care of all cyber-risk. It is very understandable to see why people chose that answer, but if the people understand why, it was incorrect it can help ensure clearance.

Question 5 more than 70% of the people choose the right answer. It is safe to say that there is a great understanding of simple ways a person can secure their router. On question 6, more than 90% of people got this correct which exceeded expectation. Question 7 the percentage dropped to 75%. It is safe to say that people do have an accurate understanding of what a VPN is and how it can secure a person system. Question 8 more than 70% have a basic understanding of what phishing is and some different ways it can affect a person. When it came to question 9, the goal of 70% or higher was not achieved. We can assume that more than 30% of people are confused on what ransomware is. The last question reached our goal with 70% or higher. Even though majority of people got the questions right

there is still need for a concern. While conducting the survey, a great number of people told me they did not feel confident when they took this test, or they thought they failed. This is a problem that needs to be fixed.

V. Recommendations

Cyber-Security is becoming more relevant as technology evolves. Because of this, it means that people will be affected by whether they believe it or not. 204 respondents completed the study and the majority of the people had a basic understanding of what cyber-security was. However, there are still ways students at Hampton University can do to help stay secure.

The first recommendation is that all students are required to take a modified Intro to Cyber-Security class to teach all students. The school requires students to take an intro to computers class where they learn how to use Microsoft, Word, Excel, and many other things. An introductory class will help college freshmen understand the dangers of the internet and ways they can stay secure in the manner.

Another recommendation is that a Hampton University Cyber-Security Manual be made to give out to Hampton University students. This manual would be given during freshman orientation week. The manual would briefly touch over what cyber-security is, what are some threats, and ways students can help secure themselves. As technology is evolving it is important that our students stay up to date as well.

Another suggestion is that Hampton University requires students to take a day course before they step on campus. This process would be similar to how a human resource department trains new hires. There would be set made videos that students need to watch over cyber-security explain what cyber-security is. After the videos are watched students when then be required to take a test and receive a certain score. If the student does not receive a certain score, then they should take an intro to cyber-security course class.

VI. Conclusion

With regards to digital security its fundamental reason it's to verify the PCs, frameworks, and projects from such computerized ambushes. A huge bit of these mechanized attacks is gotten ready for getting to, changing, or eradicating unstable information; pressuring money from abused individuals; or barging in on common business assignments. Technology is evolving every day, and it is important that with every update it stays secure as well. The world today has become a digital world. People in the world must realize this and learn how to move forward. Part of moving forward is them learning how to stay secure. There are many threats in the world today that can affect people on a day-to-day base. The more knowledgeable people are the safer they can make their lives.

ACKNOWLEDGEMENTS

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

References

[1] "Computer Forensics Career Guide: Bridging Criminal Justice and CIS," [Online]. Available: https://www.gmercyu.edu/academics/learn/computer-forensics-career-guide.

[2] "What is Computer Forensics?," [Online]. Available: https://www.devry.edu/online-programs/area-of-study/technology/what-is-computer-forensics.html.

[3] K. Afifi-Sabet, "What is network forensics?," 07 12 2021. [Online]. Available: https://www.itpro.com/cyber-attacks/31660/what-is-network-forensics.

[4] M. Burns, "A quick guide to digital image forensics in 2020," 06 03 2020. [Online]. Available: https://www.cameraforensics.com/blog/2020/03/06/a-quick-guide-to-digital-image-forensics-in-2020/.

[5] "AUDIO AND VIDEO FORENSIC ANALYSIS," [Online]. Available: https://forensicexpertinvestigation.com/audio-and-video-authentication-and-analysis-services/.

[6] N. Fox, "Memory Forensics for Incident Response," 26 07 2021. [Online]. Available: https://www.varonis.com/blog/memory-forensics.

[7] H. Journal, "Study Reveals 75% of Employees Lack Security Awareness," 25 10 2018. [Online]. Available: https://www.hipaajournal.com/study-reveals-75-of-employees-lack-security-awareness/.

[8] B. Dobran, "27 Terrifying Ransomware Statistics & Facts You Need To Read," 31 1 2019. [Online]. Available: https://phoenixnap.com/blog/ransomware-statistics-facts.

[9] J. Melnick, "Top 10 Most Common Types of Cyber Attacks," 13 01 2022. [Online]. Available: https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/.