https://github.com/Hunt3r23/CIS/wiki/Group-Project

# Abstract

In this paper, we will be talking about a variety of ways that cybersecurity can help you online. As well as types of cybercrimes.

# Introduction

Cybersecurity is very important in today's day in age. For as everything we know is all online. This is why we need to inform people about different ways to keep themselves safe, as well as having them identify different types of cyber crimes that happen.

# Methodology

## Benefits of a VPNs

First off to know the benefits of a VPN you first must know what it is. A VPN or also known as Virtual Private Network is a system that connects your network, using security protocols, to other networks that allow the information to travel through the VPN connection of the network system. This sends encrypted data over a network, and with the better VPN, the information passing through will be harder to break into and be more secure. A VPN makes a “tunnel” for information to go through, encrypted so no one can snoop in on it. Once it reaches the other side of the tunnel, it encrypts and is displayed on the other users’ devices. VPNs can be used on your PC, smartphone, tablet, or a server. Some benefits of a VPN are improved security, remote access to your information, buying cheaper tickets, and bypassing restrictions. The most important part of a VPN is improved security. It increases our online safety and privacy while surfing the internet. A VPN does not only help you be protected by hackers, the government, and DNS leakage, but also gives you the ease of mind when at a local Wi-Fi. A VPN hides your actual IP address and encrypts your information against predators. This protects us from someone trying to use an ISP, which views all the information of the customer including their data, password, and personal information. Another benefit of having a VPN is being able to visit the internet without being traced. A VPN allows you to surf the internet anonymously. Allowing you to skip all kinds of geographical restrictions and giving you maximum internet coverage. Also allowing you to visit blocked websites and going through established Internet filters. Another benefit of having a VPN is keeping your browsing history a secret. No matter where you go on the internet you are being tracked by your internet service provider and your web browser. With a VPN you can keep your history private. This can help prevent adware from reading your search history and posting you an ad about what you have been searching for. Also, your internet provider can sell your browsing history at any moment, so it is best to keep it private. VPNs can also help protect you against identity theft. Identity theft occurs when someone steals your personal information and uses it to commit crimes in your name. For example, opening new accounts, filing tax returns, or even renting and buying property. Without a VPN your information is easy to steal since it is not encrypted. Putting a VPN on your smartphone is a good idea as well. If you are one of those people who keep their Wi-Fi on all the time, you could be connected to a public Wi-Fi, and be sharing all your data without even knowing it. Lastly, here are some tips for finding the best VPN for your needs and for your budget. You got to ask questions like Do they respect your privacy? The whole point of a VPN is to protect your privacy in the best way possible, so what is the point of a VPN if it is sharing your personal information with everyone. Next, do they run on the most advanced protocol? You want to make sure that your VPN is staying up to date with technology and with software support. Also, do they set data limits? If you are a person who uses the internet a lot, making sure your VPN does not have a limit of the bandwidth. Continuing, where are the servers located? If you want to make sure you are in a certain area, used for streaming certain shows, make sure to know where the servers are located. Lastly, will you be able to use the VPN on multiple devices as well as the cost? For most people, they have more than one device that they are using. If your VPN only allows you to cover one device, are you willing to make that sacrifice? As well as the price. Make sure you check all of these before deciding on which VPN to purchase. With that, those are some tips on how a VPN can help you stay secure online. As a result, we talked about what a VPN was, how it works, some of the benefits of a VPN as well as how to decide which VPN to use. In conclusion, VPNs are a good basic source of cybersecurity, for they allow protection of your identity, your information, and your history. It also helps to find out which VPN is best for you and your needs. In the future, I could talk about how to use a VPN or even some of the non-cyber security reasons to have a VPN.

## Benefits of an Antivirus

In this portion, I will be giving you examples of why you should be buying an anti-virus for your system. I will be explaining the benefits of an anti-virus. The motivation behind this is to help people have a better understanding of cybersecurity and help them safely surf the web. To under the benefits of what an anti-virus can do to help your system, you first need to know what anti-virus is. As defined by the Oxford dictionary, an antivirus is a form of software designed to detect and destroy computer viruses. Well, you may be asking how do you get a computer virus?

Some of the most common ways to get a computer virus is from opening emails that have been spoofed, downloading software from an unknown site, clicking on online ads, strings of social media, and security holes from unpatched software. Even though you can do your best to try and avoid viruses, sometimes it does not always work, and this is when an anti-virus comes into play. Antiviruses have many beneficial uses when you are browsing the web or downloading software on the web. The first, thing to know is anti-viruses run in the background of your computer, checking every file you open. This is usually known as access scanning, but it has many different names. When you have an anti-virus, the program is downloaded to your computer, and you open a file, it seems like the program is launching immediately but it does not. Your anti-virus software checks the program first, comparing known viruses, worms, and other types of malware. But that is not the only thing your anti-virus does when opening a file, it also checks programs for types of bad behavior that may indicate a new, unknown virus. It is possible to use an antivirus without on-accessing scanning, but this is not a good idea because if a virus infects your system from a security hole, it will not be caught by the scanner. And after a virus has infected your system, it is much harder to remove, and you can never be sure if the malware is one hundred percent removed. There are also full system scans. If you are running an on-access scanning, full system scans are not usually that useful, but it does not mean they are useless. Full system scans can be useful when you just bought an anti-virus, it ensures that no viruses are lying dormant on your computer. While most anti-virus software set up a full system scan usually around once a week, to ensure that that there were no viruses that your scan accessing system did not catch. Not to mention, but the full system scans can be helpful when repairing a computer. If you are trying to fix an already-infected computer, inserting its hard drive in another computer and performing a full-system scan for viruses is useful. However, you typically do not have to run a manual full system scan yourself when an antivirus program is already protecting you because it is always scanning in the background and doing its own full system scans. You may be asking how does an antivirus system works? Well, an anti-virus system relies on virus definitions to detect malware. That is why your anti-virus software may update once a day or more. It automatically downloads new, updated definition files. These definition files contain signatures for viruses and other malware that have been encountered in the wild. When the anti-virus program matches a virus with one in the definition, it stops the file from running, putting it into “quarantine.” Depending on your antivirus settings, it may just delete the file, or it may allow you to run it always if you think it is a false positive. Along with the definitions your antivirus software always employs heuristics. Heuristics allow an antivirus program to identify new or modified types of malware, even without virus definition files. But the only problem with this is that heuristic cannot be too aggressive, or it will start flagging legitimate software as viruses. In some situations, while using antivirus software, you will get a false positive. A false positive is when your antivirus programs flag a safe file as a virus file. Even though this is fairly rare on normal use, usually when an antivirus says your file is malicious, you should believe it. One thing to look at when purchasing antivirus software is their detection rates. Depending on the company, it could have more effective heuristics and release more virus definitions than other competitors, resulting in a higher detection rate. If you are looking into purchasing antivirus software, detection rate studies are the place to look. After you have purchased your antivirus software and is installed onto your system, it would not be a bad idea to check your new software to see how effective it is. One way to do this is to download an EICAR test file. An EICAR test file is a standard way to test an antivirus program to make sure it is working right what an EICAR test file does is replicates a virus while having no chance of harming your computer. In this paper, I talked about what an antivirus was, what on access scanning was, what the benefits of full system scans were, what virus definitions are, what heuristics do in an antivirus system, explained what a false positive was in a system, and explained how to test your antivirus program and how to figure out which antivirus program is right for you. In conclusion, I talked about the basics of an antivirus and how they can help you stay safe when downloading files and how to use an antivirus on your computer. For future work, I can give more precise examples of how to use an antivirus, like how to use an antivirus to fix an old, infected computer, as well as compare and contrast some of the best antivirus software so the consumer knows which one to buy.

## Cyber Crime

Cybercrime is one of the most dangerous crimes there is in the world. Everything in the world revolves around the internet. There is a code that controls everything in the online world. There are many different languages when it comes to the online world. People can hack into your online world and you may wonder what is stored in it? Your identity, your money, everything that is stored online, you just must be careful of what you click on and the sites you go on. Viruses are one of the biggest threats that you can get on your computer which they can go through everything you have ever done in the online world. They can steal your credit card information and spend all your funds on it. They will try and ruin your life to make their life even better. For example, if you click on a wrong link or and click on the wrong ad and you download whatever the ad said then you probably most likely got a virus. Other people control the viruses that get installed on the computer. But do not worry because there are ways to remove the virus before it is too late. They sell virus protection to prevent you from getting a virus, but they aren’t cheap they also have a monthly description. There are all different types of hackers out in the world. Sometimes we use hacking to our advantage. For example, we use hacking in the FBI, etc. To protect our national security for the safety of all the Americans. Hackers hack into our computers because they want to steal all our information and cheat the system of getting rich. If you ever get caught hacking and they track you then you will be in jail for a long time. The hackers have been stealing stuff since when computers came out. When they first started to learn how to code. The code is for good and for bad. It is good for when you want to start your own business or make something that everyone can use. On the other hand, code is bad that people can hack into stuff and steal stuff from you that you want nobody to see or notice and they will expose you. There are many ways you can be smart when you are in the online world and in many ways you can prevent hackers from getting to your computer and taking all your information. You can get virus protection like Norton, AVG, Malware, Avast. These will prevent you from getting a virus on your computer and they will keep your computer safe. When a threat appears on your r computer it would tell you that a website or a link isn’t safe, and it will tell you not to click on that link or website. If you do click on it and something install the program that you have will open and it will delete/uninstall whatever you downloaded. That is why these are some of the greatest virus protection there is out in the online world. They are recommended by professional computer developers.

That cybercrime is a huge deal in the online world. If you are not smart in the online world you would be an online dummy. The hackers will try and trick you and try to steal your information and money. Everything is online these days and if you get hacked into your life is basically ruined because all your money can be gone and you can’t get it back unless you freeze your account in time. You should always be careful when you are in the online world. The online world and the real world are two different worlds. If you don’t know what you are doing in then you are screwed in both ways. Hackers are no joke. They will destroy/terminate your accounts and everything that you have online.

## Cyber Security

Cybersecurity is very important due to the number of cyberattacks that we have. We can reduce the number of cyberattacks that happen by downloading software and helping out the community. We have many things that can help protect us. We have firewalls which help protect our computers. Firewalls are really important due to the fact that's what stops hackers from coming into your compute. The more firewalls you have the more protection you have. Firewalls and antivirus kinda work the same. Antivirus is the one where is it tells you not to download it because it is unsafe for your computer. People are always trying to hack into your computer. You have to protect it by buying what you need. Also, you want to protect your cloud security and your network security. People can hack into your network aka wifi. What they do is add so many packages to your wifi which makes it crash and really slow. It basically shuts it off. It's called ddosing. It Lags out your router until you have to restart your wifi in the house. One way to protect yourself against that is that you can use a VPN which won't lag out your wifi server. It would lag out another wifi server somewhere in the world. People do that so it is easier to hack you on your computer. For example when your wifi is so laggy and super slow. That leaves your computer wide open. After all, you won't be able to defend it because you have no internet.

## Online Scams

Online scams are different techniques of fraud coordinated by cybercriminals around the world. These scams often happen by the most common type of scams such as phishing emails, social media, SMS messages on your mobile phone, fake tech support phone calls, scareware, and more. The sole purpose of cyber criminals doing this is to access your sensitive personal information such as your social security, credit card information, user login information, and even identity theft. Following the motive behind this is to steal your identity and use your hard-earned money for their benefit without getting caught or without the victim noticing.

This is where cybersecurity comes in to protect your sensitive information from these cybercriminals. We as a society want to believe that the internet is a safe place where you can do your daily activities for example shopping, but that isn't the case. Following your credit cards is exposed the more you do online shopping. This online scam is called credit card fraud or bank loan scam. People who are easily persuaded often fall into this trap facilitated by cybercriminals. The “to good to be true” offer from the bank that guarantees a large sum of money will be transferred to your account. Of Course, anyone wouldn't say no to free money, that's where these criminals work. They are very persuasive and tricky. Also mainly target non informed victims about cybersecurity especially the elderly. Even though it is very unlikely that you get trapped by this online scam there is still some loss. For example, a majority of people that get caught in this situation often have to pay the “mandatory” processing fees created by cybercriminals. You can prevent this from happening by paying attention to your accounts closely and often, taking advantage of free consumer protection services, and signing up for free credit monitoring.

Online criminals can reach us further than in past years due to advances in technology and hacking software. Because of this, there is little we can do on our own to prevent these online crimes from happening. Cybercriminals use malicious software and take advantage of vulnerabilities of all applications and programs even the most popular such as google chrome. Contrasting an ingenious method that is often used is called fishing that can come from all over the world this makes it even more difficult to capture cybercriminals. More than one-third of all security incidents start with the phishing scam, these are often sent to companies employees. The results of phishing scams can lead to disheartening results and can leave you defenseless. This is why you should become aware of what you're getting yourself into online. This form of online scam is mainly based off of online communication services such as email or on social networks. In often cases, these will bait people to expose their sensitive information such as login information, Credit cards, and SSN. These are taken from you and used to the benefit of the criminal and depending on where he is from there is little you can do about it. Although this method is the most commonly used scam online people have become more aware so the scammers have had to change their method. Adding to that cybercriminals have created a sense of urgency within these phishing emails. This will make it seem as if your bank account is at ultimate risk and you need to take action as soon as possible. Then they take your login information and lock you outside of your account and it is a scary situation.

According to the Federal Trade Commission, cybercriminals are most likely to target Millennials and are more vulnerable. Their research shows that 40 percent of people ages 20-29 have lost money in their fraud cases. Following that the oldest and most popular is the “Nigerian Scam”. Also to be known as the “Nigerian 419”, it was named this because the country of Nigeria has banned this scheme in their country. This scam starts off via email, text, or social media and will contain an emotional letter. This letter is most likely to ask you to help a “wealthy” person withdraw a certain amount of money. The scammer wants you to sympathize with the bait in the text to reel you in. Also, an added bonus is that you're promised some money for even helping. Basically, they get you to pay their cost for additional services like transfers. The scammer will be very persistent and ask you for more and more money. Then eventually you will be left with a large amount of money missing because you were tricked into sending money to a random criminal across the globe.

Scams are baited to people with things that appeal to the modern family such as family vacations or getaways. These are usually more popular when seasons change such as winter and summer. This is because of the popularity of going out of town because kids are on winter or summer break. Before this happens families will fall into the loop of fake vacations so that the criminal can obtain family members' social security numbers or bank information. Some advisors say if it looks too good to be true do not fall for the scam. The criminals that set this up will take money from you with “hidden fees”. This can range from various billings such as airport fees, tickets, and even simple items such as meals. How to avoid this is to travel with trusted travel agencies. This is to avoid the risk of losing money and being caught in a vacation scam scheme.

A recap of how to prevent this from happening to you in the future. Stay away from unknown numbers that call saying that they are tech experts and are requesting sensitive information. In addition to this is do not buy a 3rd party application and enter your personal information this can lead to stolen identity theft. That being said make sure you are not on any sketchy websites that would seem to be fake. Another way to prevent yourself from being a victim of cybercrime is to not let anyone access your computer from another device. This will leak all the saved information that you have on your pc and can lead to a devastating result. Also do not take a stranger calling you for granted you have no idea who is on the other side of that call and their intentions.

It is not likely for people to get scammed but it does still happen to those unlucky ones. This is why you should always be aware of the situation and have common sense. Scammers are very smart, that's what makes them the most dangerous. They have schemes that they create that are very complex and organized. It's hard for officials to track these criminals because you can get hit from any location on the planet. Scammers know who they are targeting with their demographics so the percentage of their scam working is increased. This being said you should always be aware of who you are talking to and what information you are giving out.

## Encrypted Viruses

An encrypted virus is a computer virus that encrypts its payload intending to make detecting the virus more difficult. However, because anything encrypted needs a decryptor or a key an antivirus can use the decryptor as the method of detection. If you believe your computer or storage device, like a USB flash drive, is infected with a virus, run an antivirus scan on the computer. Open your antivirus scanner through the Windows notification area or Start menu and run a full system scan to check all files on your computer for a virus. If the antivirus program detects the virus, a prompt to either move the virus to the virus vault or delete the infected files will be given. Both options are a good way to remove the virus from the computer. If you do not have an antivirus or Windows Defender, but still believe a file is infected with a virus, try running an online virus scan. These websites scan your computer hard drive for any infections. You may also consider installing a free antivirus program. Unfortunately, many non-virus related issues are often blamed on computer viruses. Nine times out of ten, a computer problem is a software, driver, or hardware-related issue and not a virus. If, after running the antivirus, no virus is found, it's very likely the computer is not infected. If you still believe your computer is somehow infected, you may also consider running an online virus scan and scanning the computer with a malware protection program, as mentioned below. There are several ways a computer can become infected with spyware, viruses, and malware. Below is a list of methods of how your computer can become infected. We have made this list in the order we believe to be most to least common. While browsing the Internet, an Internet advertisement or window appears that says your computer is infected or that a unique plug-in is required. Without fully understanding what it is you're getting; you accept the prompt. When installing or updating a program, you're often asked if you want "additional software" to be installed. Often, this option is presented as a check box, which is already checked. So, if you click "Next" or "OK," the program considers that as permission, and installs the software — whether you want it or not. For this reason, be incredibly careful when installing software. Make sure to read everything on every screen of the installation process before clicking any buttons. If you are running a computer with Microsoft Windows, we highly recommend you have some form of antivirus and spyware or malware protection. This software can remove any existing viruses and spyware, and it helps prevent future infections.

## Secured Passwords

Having a secure password is very important. Without a secure password, cybercriminals have easy access to any of your personal information/accounts. We need to keep our passwords private to protect our personal lives, and that includes financial information. Some cybercriminals hack social networks or email accounts, but most want the financial part by hacking bank accounts. If someone gains access to your email account, they can use the “forget your password?” link on other websites you use, like online shopping, or banking sites. These cybercriminals can also scam your friends through you. They can send out links to dangerous and unsafe websites. Also, they can post messages asking for money. A good password is what basically stands between you and a cybercriminal. There are many ways cybercriminals can figure out your password other than phishing attempts and spyware. One way they can do this is by attempting to log in to your account and surprisingly guessing your password-based off on personal information gained from your security questions. So it’s best to not include personal information in your passwords. Another way hackers can attempt to gain access to your passwords is through a password cracker. A password cracker uses force by using multiple combinations of characters repeatedly until it gains access to the account. The more short and less complicated your password is, the quicker it can be for this program to come up with the correct combination of characters.

The longer and more complicated your password is, the more likely the hacker will not use the brute force method. This will mainly happen because of the amount of time it will take for the program to figure it out. Instead of this, they’ll use a method called the dictionary attack where the program will cycle through a predefined list of common words that are used in passwords. Now when trying to create a strong and secure password there are some dos and don'ts. It's good to use a combination of uppercase and lowercase letters, symbols, and numbers. Don’t use commonly used passwords such as 123456, the word “password”, and anything else as simple as those. Do make sure that your password is at least 8 characters long. The more characters and symbols you have the more difficult it will be to guess. Don’t use the name of family members, schools, pets, and even your name. Also, don’t use the same password for multiple websites and accounts. It’s also good to change your passwords regularly. Following these things will keep you safe from some cybercriminals and will keep your information/accounts safe. Always keep your passwords a secret. Do not share passwords with anyone no matter the circumstance. Anyone will try and take advantage when given the chance.

# Results

As a result, we went over a variety of different topics talking about cybersecurity as well as giving some inside information about cybercrime.

# Conclusion

After reading this paper, you now have a better idea of what to be doing online to keep you safe. As well as different things to look out for when surfing the web.

# Future Work

For future work, we can talk about more detailed ways to help you stay safe online with more examples and more advanced ways. We can also explain the more advanced cybercrimes that come with increased intelligence in the cyber thief.

# References

<https://www.lifehack.org/533452/5-significant-benefits-using-virtual-private-network-vpn>

<https://us.norton.com/internetsecurity-privacy-what-is-a-vpn.html>

<https://insights.motherg.com/blog/5-common-ways-computer-viruses>

<https://www.desktopclass.com/computer-it/some-benefits-of-using-antivirus-software.html#:~:text=Some%20important%20benefits%20of%20using%20antivirus%20programs%20are,virus%20so%20that%20it%20may%20not%20harm%20computer>.

<https://www.howtogeek.com/125650/htg-explains-how-antivirus-software-works/>

https://www.computerhope.com/issues/ch001045.htm

Author name: Doesn’t have one.

Title website: How does a computer get infected with a virus or spyware?

Name of the publisher: Computer hope

Last updated: 11/13/2018

https://economictimes.indiatimes.com/tech/internet/internet-security-101-six-ways-hackers-can-attack-you-and-how-to-stay-safe/articleshow/61342742.cms

Authors name: Ankush Johar

Title of the website: Internet security 101

Name of the publisher: ET CONTRIBUTORS

Date: October 30, 2017

https://www.acorn.gov.au/learn-about-cybercrime

Author: No author

Title of the website: Learn about cybercrime.

Name of the publisher ACORN

Date: November 6, 2018