# *Does Anti-Virus Software Really Work?*

Angela Darden
Computer Science Department
Hampton University
Hampton, VA

**Abstract - Anti-Virus Software is designed to keep your computer and other devices safe from viruses and other malware. Some popular free softwares that many people use are Norton, Kaspersky, Avira, and even more. If your device does get a virus, the software is supposed to isolate that file to prevent the file from infecting the rest of your device. To ensure that you are protected to the fullest extent, you must keep the anti-virus software up to date. But during that time that the anti-virus is getting updated, is it still keeping you safe? Many viruses get created every day, let alone every hour, so after your anti-virus is updated it's already putting you at risk because those new viruses may not be in the update. All anti-virus software companies all claim to be the best frontline protectors, but this paper will see what anti-virus software will give you the best protection from viruses.**

## I. Introduction

The Internet is a great place to find information, but it has its dangers as well. One danger that the Internet poses is malware. Malware is short for malicious software and it comes in different forms, the most common being worms, ransomware, and Trojan Horses. Even though it comes in different forms, all of the types have one objective, to do as much damage as possible to the infected system. Malware has become a more common problem due to the increase of devices that are being used, this is the result of more people having multiple devices (iPads, iPhones, computers, etc.). How can we combat this growing problem? A potential solution is by using an anti-virus software.

Anti-virus software is designed to prevent you from being a victim of a malware attack. Anti-virus software works by scanning files to see if their contents match known malware signatures. If the program does find that a file matches a known signature, the program puts that file in quarantine or deletes it and all traces of it from your system. Putting a file in quarantine is essentially isolating the file so that it can't do any damage and so it's possible to inspect the file to see if it is actually malicious or a false positive.

You can come in contact with malware when downloading files off the Internet from shady websites, Email attachments, or even as simple as visiting a website that looks legitimate. Hackers will create files that look like they are safe when in reality the file has been changed so that it either can gather information from your computer to send to them or to damage your system to make it vulnerable to more attacks. Hackers assume that people don't check the files that they are downloading, attachments that they open, and the websites that they visit, then use that to their advantage.

This paper will look into different free anti-virus software programs to determine if they protect your system like the developers say that it does. The reason for using free software is due to the fact that not everyone in the world is tech savvy or they might not have the means to spend money on anti-virus software.

### *A. Problem Statement*

Anti-virus software has one main purpose and that is to protect your device(s), but does it really do what it claims? We all know that you must keep your anti-virus software up to date to ensure that you are protected, but when you run scans does this detect everything or can things

slip through the crack. Many viruses get created every day, let alone every hour, so even minutes after updating that software, you already run the risk of a new potential virus that was not put in the update to slide past the anti-virus software.

## II. Methodology

This study will use a combination of literary reviews, experiments, and surveys in order to gather information directly relating to the thesis. Each stage of the methodology will be explained as follows:

### *A. Literary Review*

We will discuss how anti-virus software works and the importance of it by referencing scholarly articles. We will also discuss how unprotected systems are more likely to fall victim to attacks than systems that have an anti-virus software installed, also referencing scholarly articles. These articles will give us a basis to build on with additional research and to either support or contradict the thesis and findings through other methods.

### *B. Experiments*

The experiment will be myself testing out how popular free anti-virus systems protect a user from malware in a virtual environment. The virtual environment will be used to simulate a user's system. The results will then be analyzed to determine if the results support or contradict the thesis.

### *C. Surveys*

We will collect data about our topic by having a survey that allows respondents from all backgrounds to answer questions about their knowledge and experience with anti-virus software. The survey will include 10 questions with follow up questions (where necessary). The data collected from the survey will be analyzed to determine if the respondents' experience and the findings from the experiments are related.

## III. Results/Raw Data

This section will cover the cumulative results defined Section II, Methodology.

### *A. Literary Review*

Anti-Virus software works by utilizing a database full of signatures collected from malware files. Signatures are how files are identified, each file that is analyzed will have its own unique identifier. And if different versions of the same file are uploaded, the signatures will be similar [9]. Then while the anti-virus is scanning the system, if a file has a signature that either matches or is similar to a signature in the database, it will mark the file as suspicious [2]. After the file is marked suspicious, the anti-virus will allow the user to either isolate the file or if the file was a false positive, do nothing. There are cases when a file is marked as malware when it isn't, this occurs when files' signatures are closely related to those in the malware database. And just as there are false positives, there are false negatives. False negatives present a true danger because a false negative is a file that is malware but isn't being detected as so.

By not using an anti-virus software, you are leaving your system at risk. It is true that some systems already come equipped with a standard protection program, but the standard program does not give you in depth protection. Paid or free anti-virus softwares give you advanced features like automatic virus updates, scheduled scans, real time scans, etc., by using an anti-virus does not come equipped with the system, you're adding another layer of protection. And after discussing false negatives and false positives, you must think about do you want to have a program on your system to help protect your system when you can't or do you want your system to be unprotected at all times. Most pick having a program that will help protect their system.

Malware creators are getting smarter and so are their creations. So anti-virus software companies have to look at their past actions and predict how they would make code. Malware creators have the ability to make code that can evade detection [8]. This is quite difficult for the anti-virus creator to predict what the code might do. This is good for the creator because they can release multiple versions of their malware as long as it

hasn't been added into the signature database for detection.

### *B. Experiment Results*

To conduct an experiment on the effectiveness of Anti-Virus software I will be running different types of malware in a controlled virtual environment. The different types of malware were downloaded from verified source that has confirmed malware files. The different types of Anti-Virus softwares will be a range of free softwares that will be downloaded on the controlled environment.

Avira Antivirus is a free anti-virus that claims to block spyware, adware, ransomware, and other forms of malware. During the experiment the malware files were already downloaded when the anti-virus was downloaded and ran. Avira only detected one out of the five malware samples.

Avast Free Antivirus is another free anti-virus that claims to have the ability to catch new and emerging threats. But during the experiment, just as with Avira, the five malware files were already downloaded before Avast. Avast did not detect any of the malware files on the system.

BitDefender is also another free anti-virus that makes the same claims as all the other anti-virus softwares. The results of the scan were disappointing as well. BitDefender did not detect any one of the malware samples that were on the computer during the scan.

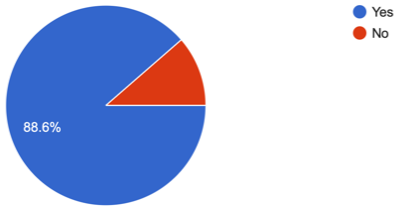
AVG claims to be a top rated anti-virus software with 6 layers of protection. But the results from the experiment don't seem to back up that statement. AVG did not detect the five downloaded malware samples on the system during the scan.

Microsoft Defender is the built-in anti-virus software on all Windows systems. Windows Defender is backed by all that use it and is highly recommended. Microsoft Defender did just as bad as the other anti-viruses, it did not pick up any of the malware samples while running scans.

### *C. User Survey Results*

A survey was conducted to get respondents' feedback about the effectiveness of the Anti-Virus Software they are using. The survey consisted of ten questions and asked the respondents various questions of Anti-Virus Software. This included questions about if they used one, what features stood out to them, and if they ever had a virus and if so, what actions did the Anti-Virus Software recommend. The answers from the survey were anonymous and the survey was distributed to a wide group of different individuals with a range of computer knowledge.

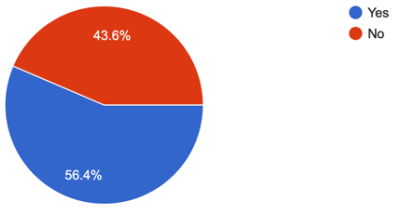
The first question asks if the respondent is familiar with anti-virus software:




| Respondents' familiarity with Anti-Virus Software | | |
|---|---|---|
| **Response** | **Number** | **Percentage** |
| **Yes** | 179 | 88.6% |
| **No** | 23 | 11.4% |

**Figure 1: User familiarity with Anti-Virus Software**

The second questions asks if the respondent uses anti-virus software:

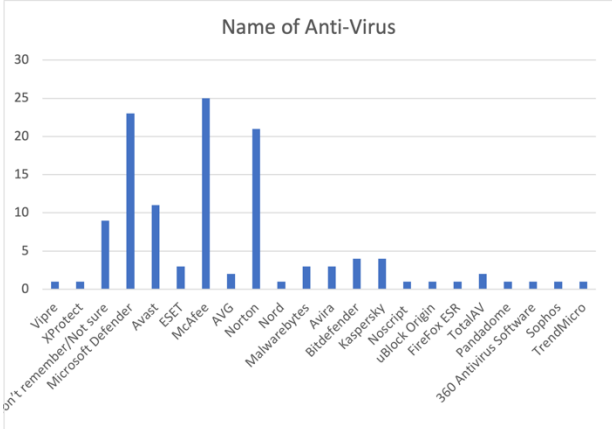



| Respondent Anti-Virus Use | | |
|---|---|---|
| **Response** | **Number** | **Percentage** |

| | | |
|---|---|---|
| **Yes** | 114 | 56.4% |
| **No** | 88 | 43.6% |

**Figure 2: Anti-Virus Software Use**

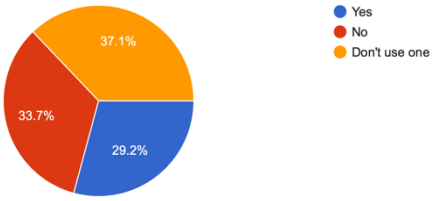
The second sub-question asks if the respondent does use an ant-virus software, which one:




| Name of Anti-Virus | | |
|---|---|---|
| **Response** | **Number** | **Percentage** |
| **Vipre** | 1 | 0.83% |
| **XProtect** | 1 | 0.83% |
| **Don't remember/Not sure** | 9 | 7.5% |
| **Microsoft Defender** | 23 | 19.7% |
| **Avast** | 11 | 9.17% |
| **ESET** | 3 | 2.5% |
| **McAfee** | 25 | 20.83% |
| **AVG** | 2 | 1.67% |
| **Norton** | 21 | 17.5% |
| **Nord** | 1 | 0.83% |
| **Malwarebytes** | 3 | 2.5% |
| **Avira** | 3 | 2.5% |
| **Bitdefender** | 4 | 3.33% |
| **Kaspersky** | 4 | 3.33% |
| **Noscript** | 1 | 0.83% |
| **uBlock Origin** | 1 | 0.83% |
| **FireFox ESR** | 1 | 0.83% |
| **TotalAV** | 2 | 1.67% |
| **Pandadome** | 1 | 0.83% |
| **360 Antivirus Software** | 1 | 0.83% |
| **Sophos** | 1 | 0.83% |
| **TrendMicro** | 1 | 0.83% |

**Figure 3: Anti-Virus Software Type**

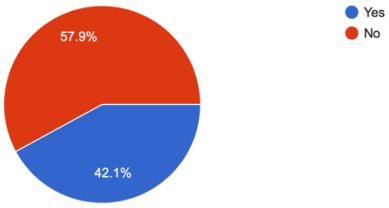
The third question asks if the anti-virus that the respondent uses is free:




| Free or Paid Anti-Virus Software | | |
|---|---|---|
| **Response** | **Number** | **Percentage** |
| **Yes** | 59 | 29.2% |
| **No** | 68 | 33.7% |
| **Don't use one** | 75 | 37.1% |

**Figure 4: Free or Paid Anti-Virus Software**

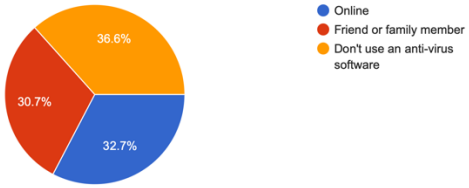
The fourth question asks if the respondent regularly updates their anti-virus software:




| Regularly Update | | |
|---|---|---|
| **Response** | **Number** | **Percentage** |
| **Yes** | 85 | 42.1% |
| **No** | 117 | 57.9% |

**Figure 5: Regularly update Anti-Virus Software**

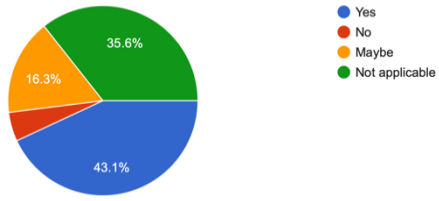
The fifth question asks how the respondent found out about their current anti-virus software:



| Found out about current Anti-Virus Software | | |
|---|---|---|
| **Response** | **Number** | **Percentage** |
| **Online** | 66 | 32.7% |
| **Friend or family member** | 62 | 30.7% |
| **Don't use an Anti-Virus Software** | 74 | 36.6% |

**Figure 6: Found out about current Anti-Virus Software**

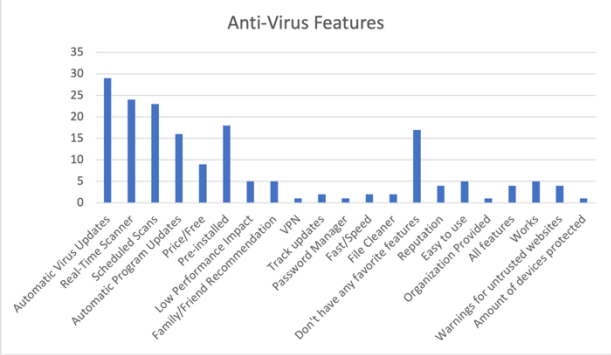
The sixth question asks if the respondent will continue to use their current anti-virus:




| Continue to use Anti-Virus | | |
|---|---|---|
| **Response** | **Number** | **Percentage** |
| **Yes** | 87 | 43.1% |
| **No** | 10 | 5% |
| **Maybe** | 33 | 16.3% |
| **Not applicable** | 72 | 35.6% |

**Figure 7: Continue to use Anti-Virus**

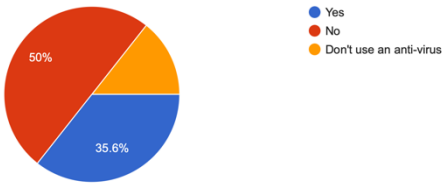
The seventh question asks what features stood out to them about their current anti-virus:




| Anti-Virus Features | | |
|---|---|---|
| **Response** | **Number** | **Percentage** |
| **Automatic Virus Updates** | 29 | 16.29% |
| **Real-Time Scanner** | 24 | 13.48% |
| **Scheduled Scans** | 23 | 12.92% |
| **Automatic Program Updates** | 16 | 8.99% |
| **Price/Free** | 9 | 5.06% |
| **Pre-installed** | 18 | 10.11% |
| **Low Performance Impact** | 5 | 2.81% |
| **Family/Friend Recommendation** | 5 | 2.81% |
| **VPN** | 1 | 0.56% |
| **Track updates** | 2 | 1.12% |
| **Password Manager** | 1 | 0.56% |
| **Fast/Speed** | 2 | 1.12% |
| **File Cleaner** | 2 | 1.12% |
| **Don't have any favorite features** | 17 | 9.55% |
| **Reputation** | 4 | 2.25% |
| **Easy to use** | 5 | 2.81% |
| **Organization Provided** | 1 | 0.56% |
| **All features** | 4 | 2.25% |
| **Works** | 5 | 2.81% |
| **Warnings for untrusted websites** | 4 | 2.25% |
| **Number of devices protected** | 1 | 0.56% |

**Figure 8: Anti-Virus Features**

The eighth question asks the respondent if they've had a computer get infected by a virus:

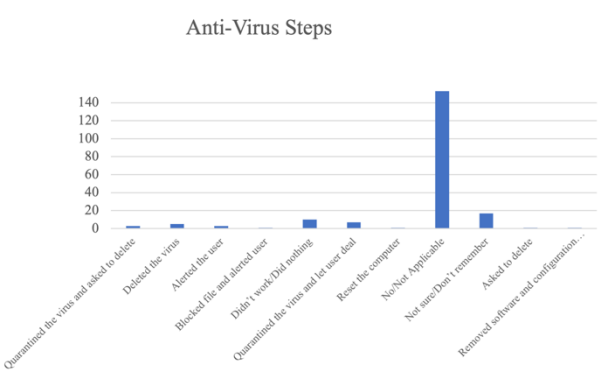



| Previous Computer Infection | | |
|---|---|---|
| **Response** | **Number** | **Percentage** |
| **Yes** | 72 | 35.6% |

| | | |
|---|---|---|
| **No** | 101 | 50% |
| **Don't use an Anti-Virus** | 29 | 14.4% |

**Figure 9: Previous Computer Infection**

The sub-question to eight asks the user if they had a computer get infected, what did steps did the anti-virus take:

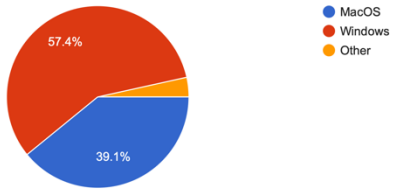



| Anti-Virus Steps | | |
|---|---|---|
| **Response** | **Number** | **Percentage** |
| **Quarantined the virus and asked to delete** | 3 | 1.49% |
| **Deleted the virus** | 5 | 2.48% |
| **Alerted the user** | 3 | 1.49% |
| **Blocked file and alerted user** | 1 | 0.50% |
| **Didn't work/Did nothing** | 10 | 4.95% |
| **Quarantined the virus and let user deal** | 7 | 3.47% |
| **Reset the computer** | 1 | 0.50% |
| **No/Not Applicable** | 153 | 75.74% |
| **Not sure/Don't remember** | 17 | 8.42% |
| **Asked to delete** | 1 | 0.50% |
| **Removed software and configuration files** | 1 | 0.50% |

**Figure 10: Anti-Virus Steps**

The ninth question ask the respondent what operating system they use:

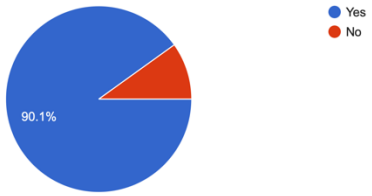
| Operating System |
|---|




| Response | Number | Percentage |
|---|---|---|
| **MacOS** | 79 | 39.1% |
| **Windows** | 116 | 57.4% |
| **Other** | 7 | 3.5% |

**Figure 11: Operating System**

The last question asks the respondent if they are familiar with the dangers of not having an anti-virus:




| Dangers of unprotected system | | |
|---|---|---|
| **Response** | **Number** | **Percentage** |
| **Yes** | 182 | 90.1% |
| **No** | 20 | 9.9% |

**Figure 12: Dangers of unprotected system**

## IV. Analysis

An analysis of the results from the Windows operating system. Each of the different anti-viruses have their own environment and on each environment is the same. There are five samples of malware downloaded. Below is the five malware samples that have been downloaded:

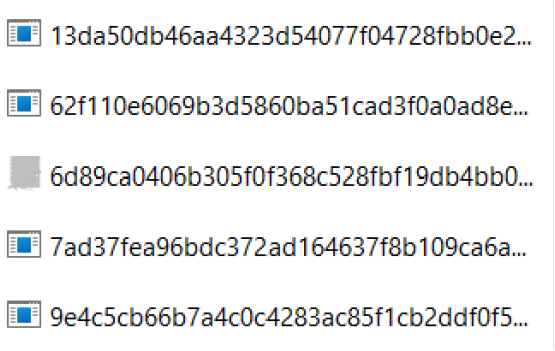



**Figure 13: Screenshot showing the downloaded malware samples**

### *A. Avira Antivirus*

Avira Antivirus is a free anti-virus that claims to block spyware, adware, ransomware, and other forms of malware. Below is how the Avira anti-virus application looks like when it's opened.

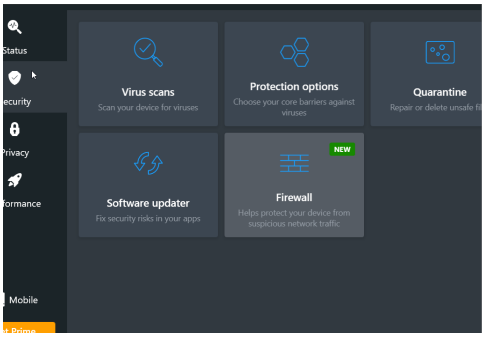



**Figure 14: Avira Home Screen**

Avira having this home screen lets users know the main components of their application and gives them quick access to them. While the application was opened for the first time, I was prompted with a virus scan. This is a good sign because the software wants to ensure that your software is secure. But I got a notification from Avira that a threat was blocked and moved to quarantine. Another good sign that it is automatically moved to quarantine.

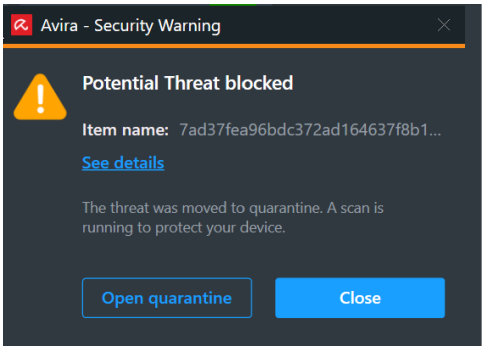



**Figure 15: Threat Notification**

But I was expecting that after I clicked close, that another message would pop up for the other four malware samples that I had downloaded, but to my surprise there were none. The scan was complete and that was the only threat, according to Avira, that was found.

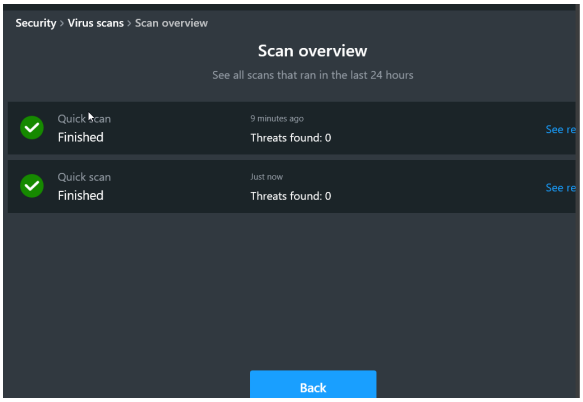



**Figure 16: Second Attempt**

The above screenshot was taken after a second scan was run to hopefully pick up the other four malware samples. But disappointingly, the other four malware samples were not found. I can conclude that Avira Antivirus does not provide the best protection due to only finding one out of the five malware samples. I suspect that the virus database either found a match with that virus or a similar virus and that's why it was detected. But there was no reason that the other four shouldn't have been detected either.

### *B. Avast Free Antivirus*

Avast Free Antivirus is another free anti-virus that claims to have the ability to catch new and emerging threats. Upon opening Avast, I was greeted with a scan page. This is a good sign, the

software wants to get a current status of the state of your system.

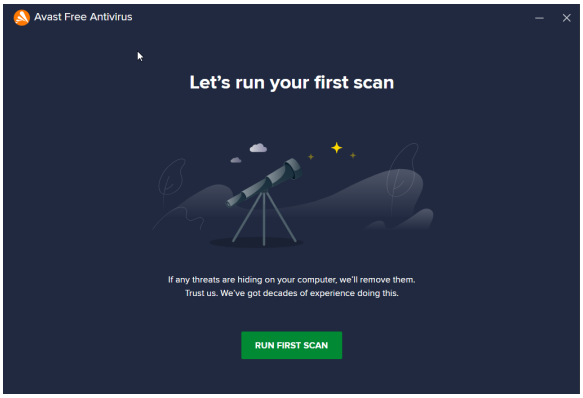



**Figure 17: Avast Home Screen**

While running the scan, there's three different sections that they are checking for: operating system, viruses and malware, and advanced issues. The following three screenshots show the status of each of the three sections. Surprisingly, none of the malware samples were found. This is concerning because the company is labeling this software as an anti-virus and it can't find five malware samples.

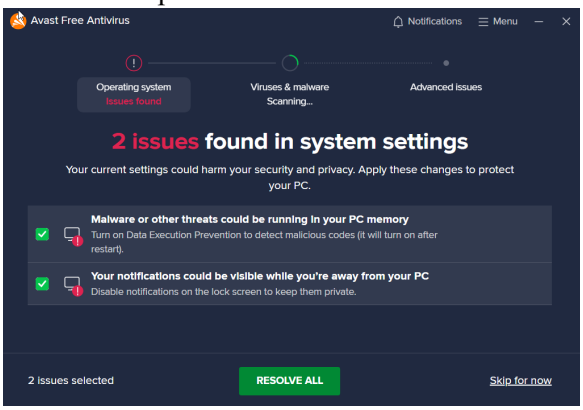



**Figure 18: Avast Operating System Check**

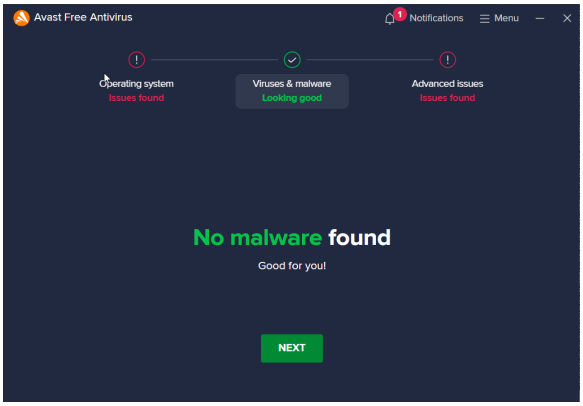



**Figure 19: Avast Virus and Malware Check**

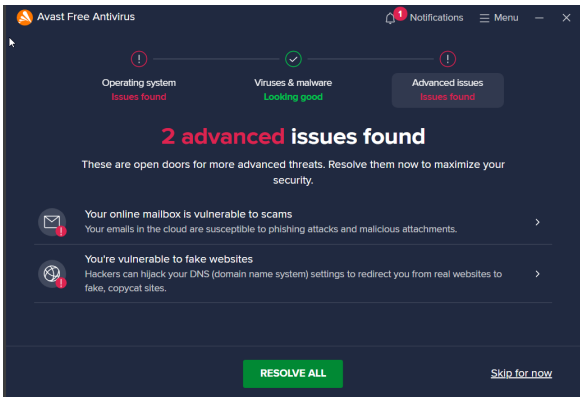



**Figure 20: Avast Advanced Issues Check**

In attempt to try and get the malware to be spotted by Avast Antivirus, I ran a scan for the second time. The results were still the same, this is not a good result. Avast did not detect the any of the five malware samples. I suspect this is because their virus database is out of date. I know that the application version that was downloaded is not out of date due to it being the most recent version with the newest updates.

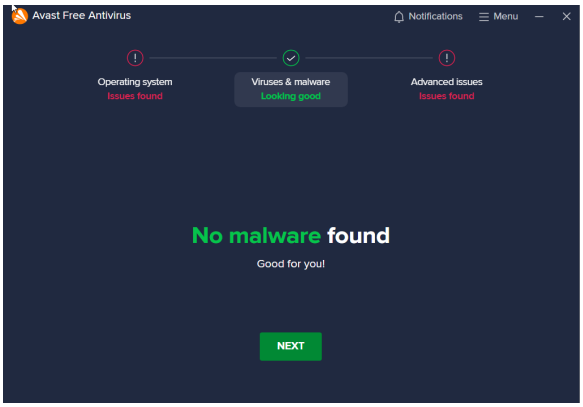



**Figure 21: Avast Second Scan**

### C. *BitDefender Free Antivirus*

BitDefender is also another free anti-virus that makes the same claims as all the other anti-virus softwares. Upon the opening of BitDefender, I was asked to do a scan. This scan did take longer than the others anti-viruses. The results of the scan were disappointing, none of the malware samples were found during the scan. Just as the others, I would infer that the virus database isn't up-to-date.

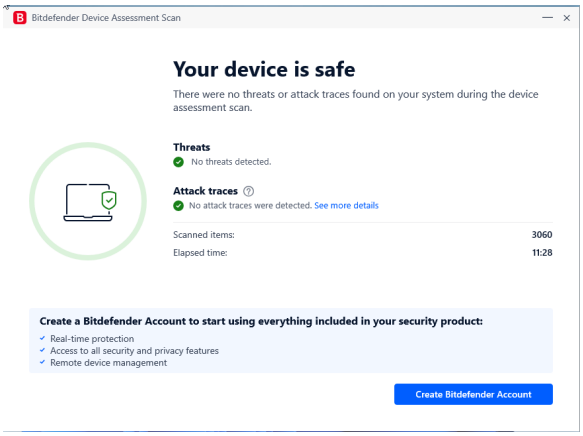



**Figure 22: BitDefender Scan Results**

### D. *AVG*

AVG claims to be a top rated anti-virus software with 6 layers of protection. When the application opens you are greeted with a home screen detailing their claims.

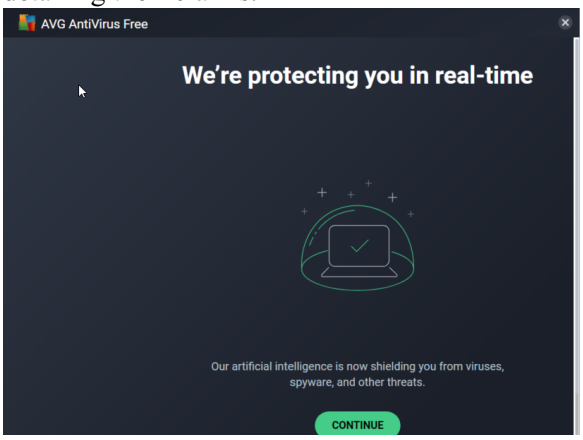



**Figure 23: AVG Home Screen**

Next the screens that are shown are similar to those that Avast has. Again, there were threats found in the operating system and advanced issues, but no viruses and malware.

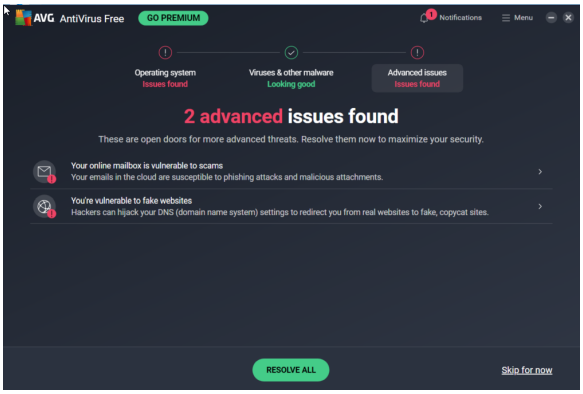



**Figure 24: Avast First Scan**

Hoping for a different outcome, I ran the scan again, but still none of the malware was found on the system. Again, this has to be because of an outdated virus database.

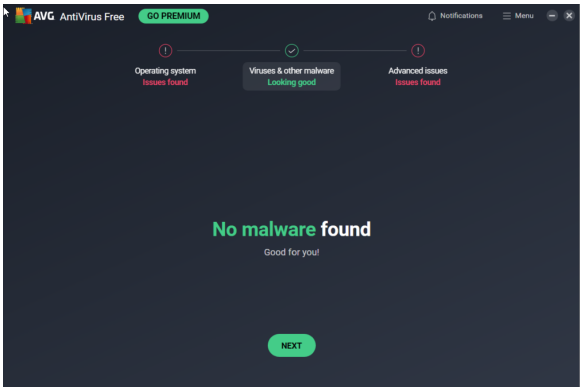



**Figure 25: Avast Second Scan**

### E. *Microsoft Defender*

Microsoft Defender is the built-in anti-virus software on all Windows systems. Windows Defender is backed by all that use it and say that there is no need for an anti-virus while on a Windows operating system. I had high hopes for this anti-virus due to all the good reputation it has. After doing a quick scan of the whole computer, like the other anti-viruses did, none of the five malware samples were found.

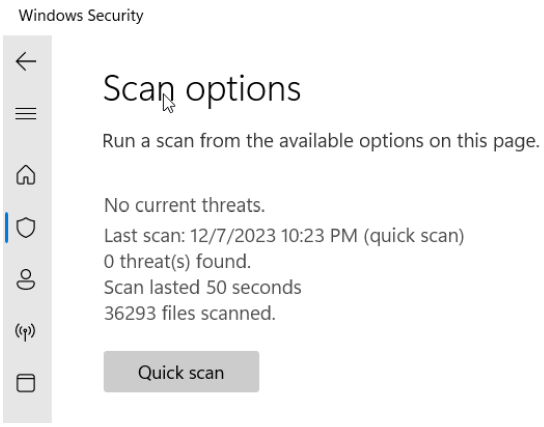



**Figure 26: Microsoft Defender First Quick Scan**

I tested it again by running another quick scan to hopefully get at least one sample. But the results led me to nothing.

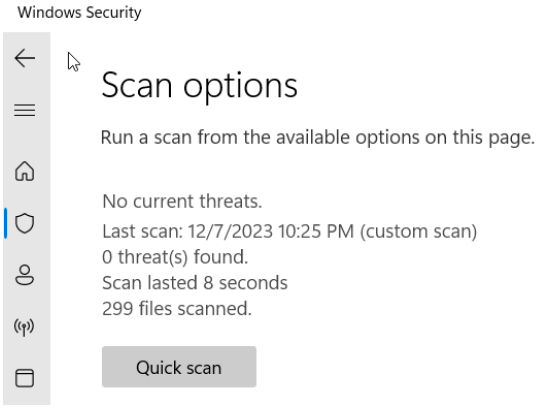



**Figure 27: Microsoft Defender Second Quick Scan**

After this I tried running each individual malware sample into the Microsoft Defender and it still did not identify any of them as a threat. This shocked me due to all the times that Microsoft Defender has blocked downloads. I don't know why Microsoft Defender didn't pick up any of the files as threats. For this one, I don't think the issue is an out of date virus database.

### *F. Question 1*

After analyzing the results from the first survey question, it shows good results that a majority of the respodents know what Anti-Virus is and the purpose of using it. With 88.6% (179 respondents) saying yes it can reveal that people from all backgrounds are informed on Anti-Virus software. Considering that my survey was not aimed at a specific target audience can safely infer that the awareness of proper computer safety is known across the grid. But just because 88.6% of the respondents know what it is, doesn't mean that they think highly of it.

With the 11.4% (23 respondents) of individuals that responded with no reveals that more people need to be informed on basic computer protection. This also reveals that they are potentially at a higher risk for coming in contact with malware that can cause damage to their system. This could also mean that they have strayed away from the topic of Anti-Virus Software because it has been made into something that is complicated and only people that are well versed in the area of computers and computer protection should know about.

### *G. Question 2*

The results for the second question asking if they use an Anti-Virus Software has a percentage of 56.4% (114 respondents) saying that they do use one. This can definitely be seen as a good thing because it means that 114 respondents care about protecting their systems. And it can be inferred that this percentage is either all or most of the respondents that answered yes in the previous question.

But on the counterpart, 43.6% (88 respondents) responded with no. This is a huge amount considering that the question deals with protecting your information and systems from dangerous malware. If I could reach out to those that responded with no, I would let them know that this is a big risk and let them know the dangers that they are potentially facing.

### *H. Question 2a*

The sub-question to question two, asks the respondents that answered with yes, what Anti-Virus they are using. The survey received a wide array of answers, some being very common and some that were not. This reveals that the respondents likely choose the anti-virus of their choice due to what the anti-virus offered and if that lined up to their expectations.

### *I. Question 3*

The third question then goes on to ask the respondent if the anti-virus that they choose was free and those that didn't have an anti-virus answered accordingly. With the results saying that 29.2% (59 respondents) of individuals use a free anti-virus software, 33.7% (68 respondents) use a paid anti-virus software, and 37.1% (75 respondents) don't use an anti-virus software. Even though the difference is small, it tells that if people are going to pick an anti-virus, they are going to pick one that is paid. This is a common assumption, mainly because paid anti-virus softwares tend to have better ratings from their customers.

### *J. Question 4*

The fourth question from the survey asks if the respondent regularly updates their anti-virus software, the results say that 42.1% (85 respondents) do and 57.9% (117 respondents) do not. This is alarming because more than half do not update their anti-virus on a regular basis. Keeping it up-to-date is how the anti-virus can keep you best protected from malware and have a current version of the program. The reason for this result could be because anti-virus software companies advertise their software as having automatic virus updates, this is not to be confused with automatic program updates. Automatic virus updates are updating the database within the anti-virus software application on your system with a more up-to-date version. And automatic program updates involve the application security, adding new features, as well as fixing any bugs, and this also includes updating the virus database.

### *K. Question 5*

The fifth question asks how the respondent found out about their current anti-virus, 32.7% (66 respondents) found theirs online, 30.7% (62 respondents) from a friend or family member, and 36.6% (74 respondents) don't use an anti-virus. A majority of the respondents found their anti-virus online, this reveals that they have done some research of their own into anti-viruses and their benefits.

Those that found out about their current anti-virus from a friend or family member reveals that the friend or family member could possibly be knowledgeable in the field of technology and that led them to trusting their opinion.

### *L. Question 6*

The sixth question asks if the respondent will continue to use their current anti-virus, the results revealed that 43.1% (87 respondents) will continue to use, 5% (10 respondents) will not continue to use, 16.3% (33 respondents) might continue to use, and 35.6% (72 respondents) don't have an anti-virus.

It's good that a good majority has found an anti-virus that either works, suits their needs, or both. This shows that anti-virus companies have a pretty decent retention rate of customers and provide a good quality software.

The amount of respondents that responded with no is quite small, this reveals that there is a small percentage of anti-virus companies that aren't making products up to the consumer standard.

For those that choose maybe reveal that their current anti-virus is either working but they want something different or it reveals that their anti-virus isn't working but they aren't sure which anti-virus to go to next.

The second largest section is those that don't use an anti-virus software, again this is alarming. Modern day viruses are getting smarter and they are programmed to look like regular files. But just as viruses are getting smarter, so are anti-virus softwares. This is all the reason to get an anti-virus to better help protect yourself.

### *M. Question 7*

The seventh question on the surveys asks the respondents what features stood out to them about the current anti-virus, this question received a lot of different responses. But here are the some of the noteworthy responses: automatic virus updates, real-time scanner, scheduled scans, automatic program updates, pre-installed, and price/free.

Automatic virus updates being a favorite feature for 16.29% (29 respondents) of the individuals reveals that people like the virus database being

automatically updated for them versus having to go in and update the virus database themselves. This is a good thing because it ensures that you always have the current version of the virus database. The virus database is how the anti-virus knows what could potentially be a virus and what is probably not a virus. Keeping this up-to-date ensures that you are protected.

Real-time scanner being a favorite feature for 13.48% (24 respondents) of the individuals reveals that people like the idea that they can go and browse the web, check emails, etc. and the anti-virus is constantly checking the websites and links that they are opening to see if they are safe. Having an anti-virus with this feature is a must, it's nice having that piece of mind knowing that your computer is being protected as you're using it.

Scheduled scans being a favorite feature for 12.92% (23 respondents) of the individuals shows that they like having scans occur on a regular basis that they can control. Usually when there is a scheduled scan option, there is a scan now option or an option along those lines. Scans come in two different types, full and custom. Full scans scan the entirety of the computer and all disks, while custom scans can scan the most commonly used folder or any folder(s) that you would like to be scanned. Usually, custom scans don't take as long as the full scans because they aren't scanning the entirety of the computer.

Automatic program updates being a favorite feature for 8.99% (16 respondents) of individuals like that their anti-virus application has the ability to update itself. This is also a good feature because it ensures that the application is up-to-date with any security updates, performance issues, virus database updates, and bug fixes. And this also is good because it occurs in the background with any user interaction and it don't force the user to stop what they are doing to initiate the update.

Pre-installed being a favorite feature for 10.11% (18 respondents) of the individuals reveals that they like the fact that it is already installed on their system. This is a relief for some because not everyone is well versed in anti-virus protection and don't know what to look for. Some examples of the most commonly pre-installed anti-virus softwares are Microsoft Defender on Windows systems and XProtect on MacOS systems. And to the belief that they would leave the pre-installed anti-virus if it didn't work, it might be acceptable to say that the pre-installed anti-virus is effective and works.

The best part of the respondent's anti-virus is the price/free for 5.06% (9 respondents) reveals that people like an anti-virus that isn't too damaging on their bank accounts. This isn't a bad thing because there are anti-viruses out there that don't cost a lot that meet people's needs and that are effective.

### *N. Question 8*

The eighth question asks the respondents if they have ever had a computer get infected by a virus, the results say that 35.6% (72 respondents) have, 50% (101 respondents) have not, and 14.4% (29 respondents) don't have an anti-virus. This question has three different responses because the goal was to filter who had an anti-virus and still had a computer infected, who had an anti-virus and hasn't had a computer get infected, and those that don't have an anti-virus.

For the 35.6% of respondents that have gotten a virus while using an anti-virus, I would have to ask if automatic virus updates and real-time scanner were turned on. This is because those are the two features that would likely catch the virus. Automatic virus updates because the exact virus or similar entries into the database would have been on the system and alerted the user of a potential match. Then the real-time scanner would be effective here because it could scan downloads, websites, emails, etc. and alerted the user if anything they had come in contact with or about to come in contact with was a virus.

### *O. Question 8a*

The sub-question to question eight asks the respondents that had a virus, what steps did the anti-virus take, this question had a lot of different responses. But here are some of the interesting responses: didn't work/did nothing,

quarantined the virus and let the user deal, quarantined the virus and asked to delete, deleted the virus, and alerted the user.

For 4.95% (10 respondents) of the individuals to say that their anti-virus didn't work/did nothing is alarming. This is due to how effective anti-virus software generally is. Whatever anti-virus that they had provided them a false sense of security and I hope that this doesn't deter them from using an anti-virus again in the future. I would recommend finding another or if you don't have the means to go and find another, tweak the settings in the application to see if that provides better protection.

Quarantined the virus and let the user deal is how 3.47% (7 respondents) of the individuals responded to the question. I believe that this is probably the most predicted action for an anti-virus to take. This is because the anti-virus could have falsely marked a file as a virus and it isn't, this isn't uncommon action. There's many reasons that it could happen, one being that the signature of the file has been malicious before or a similar signature was found that was malicious.

For 1.49% (3 respondents) of the individuals to say that the anti-virus quarantined the virus and asked to delete is another common action too. This is similar to the other response of quarantining and letting the user deal but it is slightly different. Being that the anti-virus is highly certain that the file in question is a virus but the anti-virus wants to let you know about it before deleting.

Deleted the virus is how 2.48% (5 respondents) of the individuals responded, this response is also similar to the two before. But this response assumes that the anti-virus just deleted the file that it believed was a virus and told the user after the action was done. This is common too, if the anti-virus is very certain that the file is malicious, it will just go ahead and delete the file.

Alerted the user is how 1.49% (3 respondents) of the individuals responded. It is safe to say that this response means that the anti-virus just found the file and told the user but did not delete nor quarantine it. This is uncommon, usually anti-viruses will quarantine the file even if they aren't sure. This is just a precaution so that it can't infect the rest of your files if it actually is malicious.

### *P. Question 9*

The ninth question asks the user what operating system that they use with the options being MacOS, Windows, and other. MacOS had 39.1% (79 respondents), Windows had 57.4% (116 respondents), and other had 3.5% (7 respondents). This question doesn't really have anything that has to be analyzed. You can simply infer that the respondents had a preference of an operating system and choose that one. There isn't really anything to say that any operating system is better than any other one.

### *Q. Question 10*

The last question on the survey asks the respondents if they are familiar with the dangers of not having an anti-virus, 90.1% (182 respondents) saying yes they are and 9.9% (20 respondents) say that no they aren't.

For the individuals that responded yes, it is a safe assumption that they at least know the basics of not having an active anti-virus. And for those that are more advanced and have more knowledge, they definitely know the dangers of modern day viruses and their potential impact on an unprotected system.

For the small number of individuals that are unfamiliar, it's okay to say that they might not be technology savvy and don't understand viruses and anti-virus softwares. But I would hope that after taking my survey and doing some research on their own that they would find an anti-virus that best fits all their needs so they can stay protected from the dangers in the computer world.

## V. Conclusion

In conclusion, while the Internet is still a good resource for getting information, we must still remain aware of all the dangers that it could

pose. Malware is getting smarter and more advanced each day and this definitely a big risk to everyone. Worms, ransomware, Trojan Horses, and all the other types of malware all have one main objective, to damage as many systems as possible and do it as quickly as possible.

To help reduce the risk, a good solution is to use an anti-virus software protect yourself. Anti-virus softwares help protect yourself online by having features such as automatic virus updates, automatic program updates, real-time scanning, scheduled scans, and a plethora of other features. The combination of all of those features makes an anti-virus software that is able to protect your device from attacks.

Anti-virus software has the ability to protect you when browsing the Internet, opening email attachments, and downloading files. But you shouldn't rely on it to protect you while you are being careless, you should get into the habit of being cautious while you are browsing the Internet, opening email attachments, and downloading files. Anti-virus should be used in conjunction with being cautious.

The findings from the experiments that were conducted shows that anti-virus might not be able to protect you from everything. So, it's in your hands to carefully examine what you are coming in contact with on the Internet and use your best judgment of what is safe and what isn't.

## VI. References


*[1].* Blackthorne, J., Bulazel, A., Fasano, A., Biernat, P., & Yener, B. (2016). {AVLeak}: Fingerprinting Antivirus Emulators through {Black-Box} Testing. *10th USENIX Workshop on Offensive Technologies (WOOT 16)*. Retrieved from https://www.usenix.org/conference/woot16/workshop-program/presentation/blackthorne

*[2].* Haffejee, J., & Irwin, B. (2014). Testing antivirus engines to determine their effectiveness as a security layer. *2014 Information Security for South Africa*, 1–6. https://doi.org/10.1109/ISSA.2014.6950496

*[3].* Hsu, F., Wu, M., Tso, C., Hsu, C., & Chen, C. (2012). Antivirus software shield against antivirus terminators. *IEEE Transactions on Information Forensics and Security*, *7*(5), 1439–1447. https://doi.org/10.1109/tifs.2012.2206028

*[4].* King, C. (2019). Does Anti-Virus Software Do All That It Promises? Probably Not. https://www.cs.tufts.edu/comp/116/archive/fall2019/cking.pdf

*[5].* Lockett, A. (2021). Assessing the effectiveness of YARA Rules for Signature-Based Malware Detection and Classification. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2111.13910

*[6].* Min, B., Varadharajan, V., Tupakula, U., & Hitchens, M. (2013). Antivirus security: naked during updates. *Software - Practice and Experience*, *44*(10), 1201–1222. https://doi.org/10.1002/spe.2197

*[7].* Rasool, M. A., & Jamal, A. (2011). Quality of freeware antivirus software. *DiVA*, 150. Retrieved from https://urn.kb.se/resolve?urn=urn%3Anbn%3Ase%3Aliu%3Adiva-74438

*[8].* Samociuk, D. (2023). Antivirus evasion methods in modern operating systems. *Applied Sciences*, *13*(8), 5083. https://doi.org/10.3390/app13085083

*[9].* Sukwong, O., Kim, H., & Hoe, J. (2011). Commercial Antivirus Software Effectiveness: An Empirical Study. *Computer*, *44*(3), 63–70. https://doi.org/10.1109/MC.2010.187

*[10].* Zheng, M., Lee, P. P. C., & Lui, J. C. S. (2013). ADAM: An Automatic and Extensible Platform to Stress Test Android Anti-virus Systems. *Lecture Notes in Computer Science*, *7591*, 82–101. https://doi.org/10.1007/978-3-642-37300-8_5



ACKNOWLEDGEMENTS

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