Lesson 5

Virus and malware overview

Now let's talk about viruses and malware. The word malware comes from malicious software. In general, it is software designed to damage, disrupt or disturb normal operations. The motivation behind malware is sometimes equivalent to a prank or vandalism or sometimes it involves someone trying to commit a crime. There are few different types of malware. The four main types are viruses, worms, Trojans and bots. A few pieces of malware could fall into more than one of these categories, but most things are well contained by one of these definitions. So we're going to talk about each of these four, individually. First is a virus. A virus is malware that is attached to another program. That program is called the host. A virus always must attach itself to something else. Typically, a virus requires human interaction to spread, so when we share the host file maybe by emailing it or putting it on a jump drive, we not only share the file, but we also share the virus. The next type is a

worm. Worms are similar to a virus but they are differentiated by the fact that it is a standalone program that does not require a host. Also it typically does not require human interaction to spread. It can automatically spread itself and often does so by exploiting some weakness in your operating system or other software. Next, is a Trojan. Trojans are named after the wooden horse that was used by Greece to sneak into Troy. And like their namesakes, Trojans are things that appear to be one thing but actually are something else. They are malicious programs that look legitimate. Sometimes they even go so far as to actually provide some legitimate functionality but then also do malicious stuff in the background. For example, you might download a program off the internet that prints out coupons for you and it does in fact print coupons but it also does something malicious in the background. This is a Trojan. Trojans are typically spread by humans and they typically trick humans into performing actions that will help them spread. And the last category is a bot. A bot is basically a shortening of the word robot and a bot performs an action that is usually done by humans, such as sending an email, opening a chat session, browsing the web. Sometimes the bot in and of itself is harmless but when

combined with a virus, it can be very dangerous. Rather than the virus waiting on you to send an email and attach the virus, instead, the bot will automatically send the email and automatically attach the virus. So when combined with something else, bots can be very dangerous.

Exploring anti-malware solutions

In this section, we're going to talk about antivirus software. Antivirus software is software that is designed to detect and remove viruses or other malware from your computer. Most of the products that are called antivirus are actually antimalware, because they remove more types of malware than just viruses. They're usually pretty good at catching worms, and also some of them do a decent job with Trojans and bots. Most antivirus solutions require definition files. Those definition files are a list of all known malware programs. So when the antivirus software runs, it compares a program on your computer against a list of known malware, and if it finds a match, it knows the program to be malicious. These definition files are provided by the vendors and they are updated often, sometimes daily, sometimes even

more than once a day. And it's very important for you to download the updated definition files and use them. Out-of-date malware protection is a big problem. There's a saying that out-of-date malware protection is only marginally better than having no malware protection on your computer. If your computer is going to be infected, it is most likely going to be infected with malware that was just developed recently. All of the older viruses, the viruses that have been out for years, typically don't spread very much, because everyone else's virus protection software has stopped them. So if you're going to get hit with a virus, it's most likely something that was developed recently, and you will only be protected, if you, in fact, have an updated definition file. When choosing a malware solution, and there are several out there for many different vendors to choose from, there's some things you'll want to look for. One is the mechanics of the definition update. Most solutions will have an automatic update. They will download new definition from the vendors periodically. You want to choose a solution that gives you some control over how often definition files are updated. And although you may want it to happen automatically most of the time, sometimes you might want to update them manually. You

need to make sure the software supports an option for manual updates. Most anti-malware products have some mechanism for you to exclude certain types of files from being scanned, and that could prevent false positives. You'll also want to look into what kind of reports are generated from different vendors. If your software is finding viruses on the network, you'll want to be alerted to that or have some sort of report, and if you administer a large number of Windows 11 computers, then you probably don't want to have to go check each and every computer and run the report separately. Some vendors provide a centralized location where you can run reports for multiple PCs from one place. And lastly, you'll want to look into resource usage. Your antivirus solution is always going to use some amount of processor and memory. Hopefully, that will be a low amount of processor and memory, but you may want to do some measurements to see exactly how much CPU and memory your antivirus solution is using, and obviously, the preference would be for it to use less resources.

Using Microsoft Defender Antivirus

In this section, we're going to talk about virus and threat protection. So off the start menu, I'll type in virus and that'll pull up an option for virus and threat protection, I'll click on that. The top part of this interface shows that there are no threats currently detected on my windows 11 PC, and also shows when the last scan was conducted. From here I can conduct a quick scan or with the option below that I can go to scan options, which will give me four different types of scans. So the first option is a quick scan, which will check folders in your system where threats are commonly found. So for example your web browser's downloads folder is a place that's most likely to get a virus or malware, we can also do a full scan, which will check every file in every folder, this takes a long time to complete, we can do a custom scan where we choose which files and folders we would like to scan, and then the last option is a Microsoft defender offline scan. There are some files that are hard to check while the computer is running, so an offline scan will cause the computer to reboot, and during the reboot cycle, it can access some files it normally couldn't access while it was running. So those are our four types of scans. Going back to virus and threat protection, we see the next section called virus and threat

protection settings, where we have the option to manage settings, I'll click on that. It's asking me a few questions, and most of these are just options I can turn on or off, the first one is real time protection, and this is turned on by default and probably should be on all computers, what this does is every time we access a file as we are accessing the file, the file is scanned for viruses and malware, so this provides an additional layer of protection on top of the scans. Then the next two options are for cloud delivery protection and automatic sample submission, these are similar settings, both of them involved the fact that Microsoft maintains a database of malicious files, and by having both of these on the files on our computer, can be compared to Microsoft's database of malicious files, and that helps Microsoft defender antivirus do a better job of identifying viruses on your computer, and then the bottom one is tamper protection that we can turn on or off, and it prevents others from tampering with important security features. So in other words it limits who can turn off antivirus scanning, who can change the schedule of how often scans are run, it limits that to just administrators, so that should be turned on on most computers. Going back to virus and threat protection, the last section I want

to talk about is virus and threat protection updates, it shows when my last update was, which was about two hours ago, below that we can click on protection updates, and it basically allows me to check for updates immediately. So I'll click on that. Microsoft defender antivirus is going to update the signature files on a regular basis no matter what, but if you want to force it to update immediately, you can do that by clicking here.

Manage ransomware protection

In this section, we're going to talk about ransomware protection in Windows 11. Off the Start menu, I'll type in ransomware. And I'll click on the option for a ransomware protection. This feature limits the application that can access the files in certain folders. The hope is that it would block a ransomware attack by preventing the ransomware software from accessing your most important files. I highly recommend that you have this turned on just by clicking on the simple slider here. And if you're presented with user account control dialogue, click, Yes. So now I've turned on ransomware protection, and three links have appeared below the slider. The first one is block history. As the

name implies, this is a history of all of the applications that have been blocked by this feature. And I have none, which is good news. Going back, we'll look at protected folders. And again, user account control dialogue may appear for you. Click, Yes. And it shows which folders are currently protected. I didn't add any of these. All of these came by default. The first one is the Documents folder under my user account. And having that one is very important because I keep the majority of my documents in my Documents folder. It also is protecting Pictures, Videos, Music. I don't necessarily use all of those folders, but it's fine that they're in here. One that's not in here is Desktop. And I do have the bad habit of leaving a lot of files on my desktop sometimes. So I'm going to add that by clicking add a protected folder. And I'll just select my Desktop, then select folder. And now, the Desktop folder under my user account is also protected. Going back to the main interface, the last of the three options is allow an app through controlled folder access. When I click on that, it shows me an interface where I can choose a particular app that would be allowed. So again, Microsoft is trying to block ransomware applications. If there's an application running on your computer that it misidentifies as malicious, you may

have to come in here and manually add that application so that it would no longer be blocked. The ransomware protection is something I highly recommend that you turn on. I also highly recommend that you look at the folders that are being protected because it may not be exactly the folders that you want to protect. You'll likely want to come in and add one or two more folders to this service.