Simulation transcript
Protecting your device with Malwarebytes

Task 1: Scan for malware using Malwarebytes

1. Malwarebytes's most well-known product is its antimalware scanning application, known simply as Malwarebytes, which detects and removes malware such as viruses, exploits, and ransomware. Let's explore how to use this too. Select the **Malwarebytes** icon.
2. The Malwarebytes window provides several pieces of information. Select the **Next** arrow to continue.
3. Detection History shows the number of quarantined files. Quarantined files are potentially malicious files that Malwarebytes has moved to a location from which they cannot cause harm. Select the **Next** arrow to continue. (You have zero quarantined items because the software is freshly installed and you have not performed any scans.)
4. **Scanner** lists scheduled scans and includes a button that you can select to start scanning now. Notice that a scan is scheduled for tomorrow at 2:15 AM. Select the **Next** arrow to continue.
5. **Real-Time Protection** includes switches for several real-time antimalware protection services. The services are **On** by default. Select the **Next** arrow to continue.
6. Next, you'll schedule a new scan. First, select the scan's scheduled time.
7. Select **Schedule scan**.
8. In the **Start date** field, type `08/23/2022`, and then press Enter.
9. In the **Start time** field, specify `6:39 PM`, and then press Enter.
10. Next, select **Schedule**.
11. Next, perform a scan. Select **Scan**.
12. Scanning takes a few minutes. You can view the progress in the Scanner pane. This pane shows the time elapsed, the number of files scanned, and the number of harmful files detected. Select the **Next** arrow to continue.
13. Once the scan is complete, the Threat Scan summary appears. Select **View report** to view the complete scan report.
14. The "Scan report" window has two panes. The Summary pane lists information such as potentially malicious files detected and the time of the scan. Select the **Advanced** tab.
15. The Advanced pane lists additional details such as system information and the scan parameters used. To close the scan report, select **Close**.
16. Select **Done** to close the Scanner window.
17. Now assume the scan found potentially malicious files. To view them, select **Detection History**.
18. In the "Quarantined items" pane, you can choose which quarantined files you want to restore or delete. Select the checkbox for each listed file, and then select **Delete**. (Selecting **Delete** deletes the file permanently.)

Task 2: Detect and remove adware and spyware using AdwCleaner

19. Malwarebytes offers three additional products for Windows: Privacy VPN, Browser Guard, and AdwCleaner. Select the **Next** arrow to continue.

20. First you'll explore AdwCleaner. Unlike Malwarebytes, AdwCleaner finds and removes malware, such as adware and spyware, that targets browser activity. Select the **Next** arrow to continue.
21. AdwCleaner also scans for potentially unwanted programs (PUPs), browser hijackers, unwanted browser tools, and unnecessary but hard-to-remove software preinstalled in other software you have installed. Select the **Next** arrow to continue. (Malwarebytes Premium, the non-free version of Malwarebytes, can also find and remove adware, spyware, and other unwanted software that targets browsers.)
22. When you launch AdwCleaner, it opens the Dashboard pane. Select **Scan Now** to start scanning.
23. While scanning, AdwCleaner lists the time elapsed, the number of files scanned, and the number of harmful files detected. Select the **Next** arrow to continue.
24. Once the scan is complete, AdwCleaner lists all potentially malicious files detected. This scan found many malicious files. To quarantine and disable them, select the checkbox for each listed type, and then select **Quarantine**.
25. AdwCleaner quarantines the item and prompts you to restart the device so that the utility can finish cleaning. Select **Restart now**.
26. After restarting the device, AdwCleaner automatically opens and reports that cleanup is complete. Select the **Quarantine** tab to view quarantined items.
27. The Quarantine pane lists quarantined items and information to help you decide whether to restore or delete them. Select the **Next** arrow to continue.
28. Select the **Log Files** tab to view a list of all scans and their results.
29. The Log Files pane contains the plain text log file automatically generated for each clean or scan event. Select `AdwCleaner[S00].txt` to open the log file for that scan.
30. This log file includes extensive information about the scan, such as the version of AdwCleaner used and the types of potentially malicious files found. Select the **Next** arrow to continue.

Task 3: Conceal a device's IP address using Privacy VPN

31. Privacy VPN is a VPN service. With a VPN, you can hide your online data, including your IP address, from malicious actors and other unauthorized parties. Select the **Next** arrow to continue.
32. When you launch Privacy VPN, you can choose the location of the VPN server that you will use. Select **Change server location**.
33. For this simulation, you'll use a USA server. From the list of USA servers, select **Chicago, IL**, and then select **Change**.
34. Now set the VPN to **On**.
35. The application will take a few seconds to connect to the chosen server. Select the **Next** arrow to continue.
36. Now you are connected to Malwarebytes's Chicago, Illinois server and can start browsing anonymously. Select the **Next** arrow to continue.

Task 4: Block online security threats using Browser Guard

37. Next, you'll explore Browser Guard, a browser extension that blocks ads and trackers in addition to websites known for phishing, malware, or other security threats. Select the **Next** arrow to continue.

38. Once you install Browser Guard, a webpage with usage tips opens in your browser. Now you need to enable Browser Guard. On the browser toolbar, select the **Malwarebytes** icon.
39. Select **Let’s go**.
40. The Current Website pane lists the number of potential threats that Browser Guard blocked on the current page. To learn more about Browser Guard’s activity, select the **Statistics** tab.
41. By default, the Statistics pane shows a graph depicting the number of ads or trackers blocked throughout the past week. You can also view statistics on malware, scams, and PUPs blocked. Select **MALWARE**.
42. You can also change the time range displayed in the graph. Select the arrow to display the choices. Next, select **30 Days** from the list.
43. Next, explore Browser Guard’s settings. Select the **gear** icon.
44. The Settings window contains switches you can use to set specific types of protection **On** or **Off**. Select the **Next** arrow to continue.

You successfully scanned for malware, adware, spyware, and other unwanted software using Malwarebytes and AdwCleaner. In addition, you concealed a device’s actual IP address and data using Privacy VPN and blocked other online security threats using Browser Guard.