Ledgard Consulting

FACT SHEET

No 052/ Ver: 1.0
Topic: PC & Windows

Anti-Virus Protection

Introduction

You must maintain your protection on your computer by using antivirus software. There are several options available, some free and some at a cost. It is purely a personal choice, but this fact sheet may help you decide which option is best for your situation.

Windows Defender:

This is built into Windows 10 and 11 and is adequate for most needs. It is updated and scans for threats.

Certainly! Windows Defender, sometimes known as just 'Defender', is an antivirus and anti-malware software that's built into Windows operating systems. It's designed to help protect your computer from viruses, spyware, and other malicious software. Here's an overview of its key features and functionalities:

Real-Time Protection:

Constantly monitors your system for any threats and takes immediate action when malicious software is detected.

Comprehensive Scanning:

1. Provides various scanning options, including quick scans, full system scans, and custom scans to check specific files or folders.

Automatic Updates:

2. Regularly updates its virus and threat definitions to protect against the latest threats. These updates are automatically downloaded and installed.

Firewall & Network Protection:

3. Helps protect your device by monitoring network activities and blocking potential threats. It includes a firewall to prevent unauthorised access.

Ransomware Protection:

4. Offers controlled folder access to help protect files from unauthorised changes by ransomware. You can specify which folders to protect and which applications are allowed to access them.

Parental Controls:

5. Includes family safety features that allow you to monitor and control your family's online activities. This can consist of setting screen time limits, content filters, and activity reports.

Device Performance & Health:

6. Monitors your device's performance and provides recommendations to improve system health. This includes checking for Windows updates, battery life, and storage capacity.

Integration with Microsoft 365:

7. Enhanced protection and features when integrated with Microsoft 365, providing additional tools and security measures.

How It Works

8. **Scanning:** When you initiate a scan, Microsoft Defender searches your computer for known threats using a database of virus definitions and heuristics to identify suspicious behaviour.
9. **Quarantine and Removal:** If a threat is detected, it can be quarantined (isolated) to prevent it from affecting your system or removed entirely.
10. **Real-Time Monitoring:** Runs in the background, constantly checking files, emails, apps, and websites for potential threats.

Benefits of Microsoft Defender

11. **Built-In Protection:** Since it's integrated into Windows, there's no need to install additional software, making it convenient for users.
12. **Cost-Effective:** Free for Windows users, providing basic protection without the need for a separate antivirus subscription.
13. **Regular Updates:** Automatically receives updates to ensure your system is protected against the latest threats.
14. **User-Friendly:** Simple and intuitive interface, making it accessible for users of all technical levels.

Potential Limitations

15. **Basic Features:** While it provides robust protection, some users may prefer additional features offered by third-party antivirus programs.
16. **Performance Impact:** Although generally lightweight, scans and real-time protection can occasionally cause slight performance slowdowns on older or less powerful systems.
17. Overall, Microsoft Defender is a reliable and convenient solution for protecting your Windows devices from various cyber threats.
18. You can access Windows Defender by going to:

Settings> Update & Security> Windows Security>

Now Defender is also available for both Android and iPhone

Microsoft's Malicious Software Removal Tool (MRT)

What is MRT

Microsoft Removal Tool (MRT) is a versatile utility designed to help Windows users detect and remove specific types of malware from their systems. Running MRT is a straightforward process, and this guide will walk you through the steps.

> ***Note:*** *MRT is not an App, it is a piece of software which is not accessible from the Start Menu or Apps list*

Step 1: Accessing the MRT Program:

- Press the Windows key on your keyboard or click the Start menu.
- In the search bar, type mrt.

- Click on the result labelled mrt or Microsoft Windows Malicious Software Removal Tool.

Step 2: Launch the Tool:

- If prompted by the User Account Control (UAC), click Yes to allow the program to run.
- The MRT program window will open, displaying an introduction and basic information about the tool.

Step 3: Choosing the Scan Type:

- On the main screen, you'll see three scan options:
- Quick Scan: Scans commonly infected areas of your system. Recommended for routine checks.
- Full Scan: Thoroughly scans your entire system. This option may take more time but ensures comprehensive malware detection.
- Custom Scan: Allows you to select specific folders or drives to scan.

Choose the appropriate scan type based on your needs and click Next.

Step 4: Running the Scan:

- The tool will begin scanning your system. The duration of the scan depends on the scan type and the size of the data being processed.
- During the scan, you can monitor the progress displayed on the screen.

Step 5: Reviewing the Results:

- Once the scan is complete, MRT will display the results:
- If no malware is detected, you'll receive a confirmation message.
- If malware is found, MRT will provide options for removal. Follow the on-screen instructions to delete or quarantine the infected files.

Step 6: Close the Tool:

- After reviewing and addressing the scan results, click Finish to exit the program.
- It is recommended to restart your computer if prompted, especially after removing malware.

It is essential to run MRT regularly to ensure your system remains clean and secure, as there is no automatic process. Consider supplementing MRT with a dedicated antivirus program for comprehensive protection.

Malwarebytes:

Malwarebytes is a well-known anti-malware software designed to detect and remove various types of malicious software, including viruses, spyware, adware, and ransomware - Here are some key points about Malwarebytes:

Features

19. **Anti-Malware:** Scans and removes malware from your system - Anti-Exploit: Protects vulnerable applications from being exploited by malware.
20. **Anti-Ransomware:** Detects and blocks ransomware attacks.
21. **Adw Cleaner:** A separate tool included with Malwarebytes that removes adware and potentially unwanted programs (PUPs).
22. **Privacy Dashboard:** Provides insights into how your data is being used and offers privacy protection tools.

How It Works

23. **Scanning:** Malwarebytes scans your system for malicious software and provides a detailed report of any threats found
24. **Removal:** Once threats are detected, Malwarebytes attempts to remove them from your system.
25. **Real-Time Protection:** The paid version offers real-time protection to prevent malware from infecting your system in the first place

Benefits

26. Malwarebytes is effective at detecting and removing a wide range of malware types
27. User-Friendly: Easy to install and use, even for those with limited technical knowledge.
28. Regularly updated to protect against the latest threats.

Considerations

There could be some performance impact when used on older Subscription Cost: The paid version requires a subscription, but the basic configuration is free. (There is a free trial of the paid version) Malwarebytes is a reliable tool for keeping your devices safe from various types of malware

Alternative Anti-Virus Software:

Which you are able to subscribe to. They all give a FREE option which is much the same as Windows Defender, however, within the paid-for version they do give access to other tools, such as performance-enhancing and VPN's, such as: AVG, Avast, Norton, Kaspersky, Sophos, to name a few….. Additionally, there are versions of all these anti-virus programmes available for smartphone via the App Store

It is a personal choice as to which options you want to use; the author's personal choice is Windows Defender and the free version of Malwarebytes.

The information on this fact sheet is also part of the wider Cyber Security book, which is available from the tech web site within the pdf downloads section.

www.tech-insights.uk