Antivirus Basics
Protecting Your Devices from Threats

A virus is a type of harmful software that spreads between devices, similar to how a biological virus spreads among people. It attaches itself to files or programs and activates when you open them. Consequently, maintaining computer security requires ongoing attention, the right tools, and understanding potential threats. Since the beginning of the Internet, antivirus software has been essential. As the Internet has grown, so has the need to protect against harmful software (malware) that can damage your device or steal your information.

What is the actual function of antivirus software?

Antivirus software protects your system against malware, viruses, spyware, and other harmful programs. It continuously monitors your system to detect and stop threats before they can cause damage. You can set it up to run automatic scans or manually scan your system whenever you prefer.

- **Automatic scans**—Most antivirus software can be configured to scan specific files or folders automatically in real time. It may also remind you to perform complete system scans at scheduled intervals.
- **Manual scans**—If your antivirus software does not automatically scan new files, you can manually check files and media received from external sources before opening them.

Antivirus software is designed to protect your device by constantly monitoring it for potential threats. To do this effectively, it needs full access to your computer or device to thoroughly check all files and programs.

Here's how it helps keep you safe:

File Checking: It looks inside files to see if they match known viruses or behave in suspicious ways.

Full System Scans: It can scan your whole device, not just one file, to find hidden problems. This takes longer but is more complete.

Web Protection: Some viruses hide on websites. Antivirus software checks these sites to help keep you safe while browsing the internet.

Real-Time Scanning: As soon as you open a file or program, the software checks it immediately to catch threats right away.

Removing Threats: If it finds a virus, it either removes it or moves it to a safe place (called quarantine) where it can't do any harm.

Staying Updated: The software uses a list of known threats. Keeping this list updated helps it find and stop new viruses quickly.

In essence, Antivirus software protects your devices by doing the following:

- **Prevention:** This prevents harmful software from being downloaded or run on a device.
- **Detection:** Scans for suspicious activity and known malicious code.
- **Quarantine Isolation:** Isolates identified threats to prevent damage.
- **System Cleaning:** Removes or repairs malicious files to restore the system integrity.
- **Updates:** Threat databases are regularly updated to identify new malware.

One of the most common questions about antivirus software is whether it is still necessary for all devices. While it is true that certain operating systems, such as macOS and Linux, are generally more resistant to malware, the need for antivirus software extends beyond just detecting malware.

For instance:

Windows is a common target for malware. While Windows Defender provides basic protection, a dedicated antivirus program offers enhanced security with features like real-time scanning, improved malware detection, and regular updates for emerging threats.

Apple's security features are robust, but its built-in antivirus, XProtect, may miss some malware that third-party software can detect.

Android devices are often targeted by malware, so it's advisable to use antivirus software for added protection. While Google's Play Protect—Android's built-in security system—provides some defence against harmful apps, malicious applications can still find their way into the Play Store, Google's official app marketplace for Android devices.

Typically, antivirus software is unnecessary for **iPhone or iPad devices**; however, using a VPN can be beneficial in certain situations.

How to Select the Right Antivirus Software?

Selecting the appropriate antivirus software is essential for protecting your device and ensuring it operates efficiently. Therefore, take into account the different types available:

Standalone antivirus software works on its own, separate from your device's built-in security. It checks for and removes viruses, but you need to install it separately.

Cloud-based antivirus software works online, using cloud servers to scan for threats. It stays up to date automatically and doesn't take up much space or slow down your device.

Internet security antivirus software offers more complete protection, including features like firewalls, phishing prevention, identity protection, and real-time monitoring, especially when you're browsing or shopping online.

Machine learning antivirus software uses AI (Artificial Intelligence) to recognize and fight new types of malware by analyzing patterns and behaviors in real-time.

Here are the essential factors to consider when selecting the ideal antivirus software:

- **Identify Key Features:** Look for features like real-time scanning, automatic updates, and strong malware detection.
- **Check Compatibility:** Ensure the software works with your operating system (OS) and does not slow down your device.
- **Evaluate Ease of Use:** Find a user-friendly interface that is simple to set up, especially if you are not tech-savvy.
- **Review Test Results:** Check ratings from independent labs to see how well the software performs and detects threats.
- **Consider Support Options:** Good customer service and technical support are important for quickly handling any issues or concerns.
- **Compare Prices:** Look at subscription costs and available trial versions to find a solution that fits your budget.

[1] Cyber-Seniors does not endorse any specific brand; the examples of antivirus software mentioned below are just a few select options.

Free Antivirus vs. Paid Antivirus

Antivirus brands like Avast, AVG, Avira, Bitdefender, and Norton offer free and paid versions. Free versions offer basic protection, but paid subscriptions usually cost around $50 a year or about $4 a month.

It's worth paying for antivirus software for better security and peace of mind. Paid options provide extra features like identity theft protection, password managers, and virtual private networks (VPNs). Bundling these services in one package often saves you money and offers better value.

Antivirus Software Extras

- **Identity Theft Protection:** Software solutions can help safeguard your identity by scanning various sources, such as criminal and financial records, for personal information. These services monitor for signs of misuse and may include insurance coverage for identity theft costs.
- **Password managers** are now part of antivirus software. They securely store usernames and passwords in an encrypted vault, assess password strength, and generate strong, unique passwords.
- **VPNS (virtual private networks)** are included in many antivirus programs to hide your IP address and encrypt online activities, enhancing security and protecting your data and browsing privacy.

How to Install Antivirus Software

Here are the basic steps for installing antivirus software on any device:

1. **Choose an antivirus:** Select a reputable antivirus program that meets your needs.
2. **Download the software** from the official website or your device's app store.
3. **Run the installer:** Open the downloaded file and follow the setup instructions.
4. **Accept terms and conditions:** Read and agree to the license agreement.
5. **Customize settings:** Adjust your security preferences, such as enabling automatic scans or real-time protection.

Conclusion

Antivirus software is essential for protecting electronic devices from malware, but can also cause issues. It may incorrectly flag safe files as threats (false positives) and often fails to detect new, undocumented threats.

Since antivirus programs require full access to devices, they can become targets for cyber attackers. Recent research has revealed security flaws in various antivirus solutions that could allow attackers to execute harmful code remotely, gain control over systems, or steal sensitive data.

Additionally, antivirus software can consume significant system resources, slowing down computers. It can be challenging to install and configure for non-tech-savvy users.


Connecting Generations
Cyber-Seniors™


be well
ILLINOIS


aetna®


BEYOND
FORCE


trail
TOTAL RETIREE ADVANTAGE ILLINOIS

Definitions

- **Adware** is a program that inundates you with unwanted advertisements and can sometimes lead to malware infections.
- **Browsing privacy** means keeping your online activities and personal information safe while using the Internet. It includes tools and practices that prevent websites, advertisers, and hackers from tracking or collecting your data.
- **Built-in security** is a tool already included in a device, software, or operating system. You don't need to install it separately. It protects your computer, phone, or network from viruses, hackers, and malware.
- **Cloud computing** is an environment where resources and services are delivered over the Internet, accessible through a web browser or client software.
- **Cloud servers** are virtual, not physical, run in a cloud computing environment, and can be accessed on demand by unlimited users.
- **Encrypted vault for passwords** is a safe place to store your login information. Password managers use it to keep your passwords secure. They scramble your passwords through encryption, so only someone with the master password can read them.
- **False positive** in cybersecurity occurs when a security tool incorrectly flags a legitimate activity, file, or user behavior as malicious.

- **Firewall** is a security tool that protects your computer or network from threats. It blocks harmful or unauthorized internet traffic while allowing safe connections.
- **Identity theft** happens when someone steals your personal information, such as your name, Social Security number, or bank details, to commit fraud.
- **Infected downloads** are files or programs that contain harmful software. These downloads can damage your device, steal your personal information, or compromise the functioning of your system.
- **IP address** is a unique number for each device that connects to the internet. It acts like a home address, helping computers find and communicate with each other online.
- **Linux** is an open-source operating system. It is known for being flexible, secure, and stable.
- **macOS** is the operating system created by Apple for its Mac computers.
- **Malware,** or "malicious software," is harmful software that can damage your electronic device or steal your information. It can infect your device through infected downloads, phishing emails, or unsafe websites.
- **Master password** is the main, highly secure password used to unlock a password manager or an encrypted vault.

- **Open-source operating systems (OS)** are systems where anyone can see, change, and share the source code. This means developers and users can customize the OS to fit their needs, enhance security, and add new features.
- **Phishing** is an online scam in which cybercriminals trick people into giving away sensitive information, such as passwords or credit card details. They often appear to come from trusted sources, such as banks, government agencies, or familiar companies.
- **Ransomware** is malware that locks users out of their files and demands payment to regain access.
- **Spyware** is software that secretly collects your personal information without your permission. It can track what you type and the websites you visit, and even steal sensitive data, such as passwords or credit card details. Spyware often comes with free downloads, fake apps, or phishing scams.
- **Trojans** are malicious software disguised as legitimate programs, tricking you into installing them.
- **Unsafe websites** can harm your device, steal your personal information, or trick you into downloading harmful software. They often lack proper security measures, like encryption, so you'll see "http://" instead of "https://" in the URL.
- **URL (Uniform Resource Locator)** is an address for something on the internet. Just as your home has an address to help people find it, a URL helps web browsers locate specific web pages, images, or files online.

- **User-friendly interface** is a design that makes it easy for people to use a website, app, or software without confusion. It's intuitive, simple to navigate, and visually clear, so users can accomplish tasks quickly without frustration.
- **Web browser** is a program that lets you use the internet and view web pages. It helps you browse websites, watch videos, and shop online. Some popular web browsers are Google Chrome, Microsoft Edge, Safari, and Mozilla Firefox.
- **Web page** is a single document on the internet that can be viewed in a web browser. It resembles a digital page in a book, containing text, images, links, videos, and other multimedia elements.
- **Worms** are self-replicating malware that spreads across networks and can slow down systems.