Antivirus Software Guide

Term	Definition
Antivirus	Software used to prevent, scan, detect and delete viruses from a device
Firewall	Part of a computer system or network which is designed to block unauthorized access while permitting outward communication
Malware	Combination of the words "**mal**icious soft**ware**". It is software that is designed to damage and destroy devices and/or devices' systems
Phishing	Any attempt to gather private personal information by masquerading as a trustworthy entity
Ransomware	A type of malware that restricts access to a device and demands a ransom be paid to the malware's developers
Virtual Private Network (VPN)	A "tunnel" that connects your device to another by filtering it through private networks, potentially protecting it from attacks from outside your network
Virus	Software that piggybacks on real programs – each time a program runs, the virus runs, too, giving it the chance to reproduce (by attaching to other programs) or wreak havoc

Introduction to antivirus software

Whether you have years of experience with devices or you're learning how to use one for the first time, it's important to know how to keep your information and device safe. A good way to protect your device is by using antivirus software. **Antivirus software** can prevent malware from entering your device's system or remove malware in the system if it finds it.

Malware is an umbrella category of "**mal**icious soft**ware**" that can damage or destroy data on your device. **Viruses** are an example of malware - software that can reproduce and cause issues each time a program runs. All viruses fall into the category of malware, but malware encompasses more than just viruses – other types of malware includes *Trojan horses*, *worms*, *ransomware*, and *scareware*. Malware can cause ongoing issues to your devices if it is not properly handled and removed.

The good news? Most devices now have antivirus software built-in, meaning you do not need to buy or download additional protection. In general terms, if you have purchased a device within the last three to five years, it will have antivirus software pre-installed. If your device is more than five years old, consider downloading an antivirus program to ensure your machine is regularly checked and running properly.

Antivirus Software Guide

To make sure you're taking advantage of your device's antivirus software, **complete or schedule updates when prompted by your device**. These updates will ensure your device is operating at peak performance. The most commonly owned devices are usually either Apple or Microsoft brand. Both systems run differently, so check out the information in the next section to learn more about the pre-installed antivirus program on each system.

Mac devices:

What is Apple's antivirus software called? XProtect. There is also a pre-downloaded application called Malware Removal Tool (MRT).

When was it was released? XProtect is included on all Apple devices that have come out since 2009.

What does it do? XProtect scans applications and files for viruses and malware using a database of threats that Apple updates regularly. If XProtect detects malware, it notifies the user and blocks the download. Since threats are always changing, the Malware Removal Tool (MRT) also scans your computer regularly to check that nothing sneaks past XProtect. If the tool identifies malware, it will notify you and remove the dangerous files.

Windows devices:

What is Microsoft's antivirus software called? Microsoft Defender Antivirus.

When was it released? Microsoft Defender comes pre-installed on all Windows devices released after 2015.

What does it do? Microsoft Defender Antivirus provides protection on your device and in the cloud. It scans files and applications, resolves threats, and lists detected threats in security reports on the Windows Security app.

Introduction to VPNs
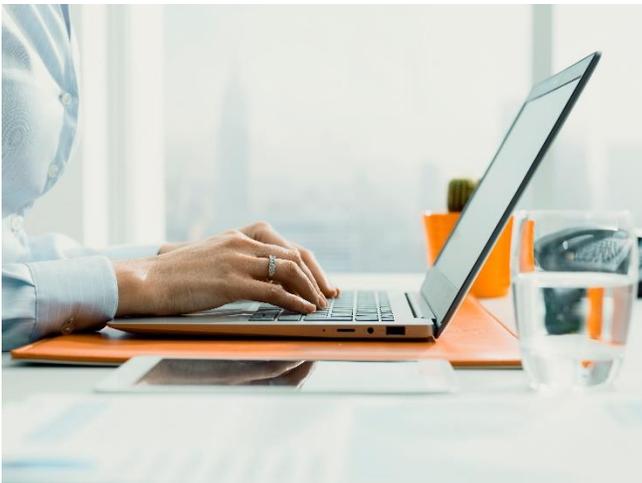
There are many stigmas and concerns around online safety, and seniors are often targeted because bad actors assume they are not digitally literate. If you want to take an extra step to protect your privacy online, consider setting up a **virtual private network** (**VPN**). VPNs provide a secure private connection between networks that can connect users even if they are far away from each other. Paying for a VPN allows you to create secure and encrypted pathways that protect your private information online. For more information, check out the resources below.

Resources:
https://computer.howstuffworks.com/virus.htm
https://computer.howstuffworks.com/vpn.htm
https://computer.howstuffworks.com/buy-antivirus-software-considerations.htm

Antivirus Software Guide

List of antivirus programs:

Many antivirus software programs have a free option with basic features, with the ability to upgrade to a paid service. Below are a few antivirus programs with the pros, cons, and specs (**spec**ification**s**) of each service.

Avast One Essential	Kapersky Security Cloud Free	AVG Antivirus Free
Pros: • VPN bandwidth limit • Includes privacy and performance features	Pros: • Ransomware protection • Phishing protection	Pros: • Boot-up scan removes persistent malware • Browser extension that keeps you safe while online.
Cons: • Limited malware protection on iOS • Many features require upgrade	Cons: • No direct tech support • Features for iPhone and iPad are limited	Cons: • Fixing device performance issues requires upgrade
Specs: ✓ On-demand malware scan ✓ Malicious URL blocking ✓ Phishing protection	Specs: ✓ On-demand malware scan ✓ Malicious URL blocking ✓ Phishing protection	Specs: ✓ On-demand malware scan ✓ Malicious URL blocking ✓ Phishing protection
Avira Free Security	Adaware Antivirus Free	
Pros: • Many features beyond basic antivirus protection • Also acts as password manager	Pros: • Completely free	
Cons: • Many useful features require upgrade	Cons: • No protection against malicious or fraudulent URLs • Lacks features found in competing free products	
Specs: ✓ On-demand malware scan ✓ Malicious URL blocking ✓ Phishing protection ✓ Firewall	Specs: ✓ On-demand malware scan	