

Protecting devices requires comprehensive, multi-layered approach

As the digital world has evolved and people have become more connected in more ways on mobile devices than ever before, so too has the threat landscape evolved. Cybercrime has become a highly profitable industry around the world, with a multi-faceted approach that includes phishing scams, identity theft, con artists and more.

By [Fred Mitchell](#) 7 Jun 2012

Given the increasing sophistication of the digital threat landscape, the requirement for all-encompassing security is greater than ever. Computer security is no longer just about antivirus solutions. Protecting yourself, your information and your money from cybercriminals and a host of threats requires a comprehensive, multi-layered security solution.

While spam and viruses still exist, and will continue to do so, identity theft has become a more pressing and more prevalent issue. Added to this, the sheer volume of digital data generated in today's world makes adequate back-up and recovery another vital tool. The reality is that the online environment, while it has revolutionised the way we work and play, has also caused the massive evolution of the computer threat landscape. Increased numbers of online users also means increasing numbers of cybercriminals, who make their living by taking advantage of unsuspecting users.

Comprehensive protection vital

In order to remain safe in today's world it is vital to have comprehensive protection that not only detects and eliminates viruses, but also protects your identity online, stops online threats and safeguards your data, files, photographs and more from loss. These layers of antivirus and anti-spyware, Internet security and identity protection help proactively to stop threats before they can infect computers and do irreversible damage.

A firewall is one of the most important features in any security solution, to prevent cybercriminals from hacking into your computer and stealing personal information. However, many users end up switching this feature off because it constantly requires the user to authenticate legitimate installations and system changes. A smart two-way firewall solution solves this problem by remembering decisions you have made in the past and applying these, without constantly requiring user input.

Comprehensive computer security

Other important aspects of comprehensive computer security to look for include vulnerability protection, anti-phishing technology and network threat protection. Vulnerability protection ensures that security loopholes in applications cannot be exploited by cybercriminals to sneak threats onto your computer. Anti-phishing technology blocks fraudulent websites that are commonly used by cybercriminals to steal identities and money from unsuspecting users. Network threat protection detects threats as they travel over a network and eliminates them before they can reach your computer to cause damage.

A comprehensive protection package should also include multiple tools and controls to enhance the user experience and ensure safety across the board. Some tools to look for include safe web-browsing tools that warn you of unsafe websites before you enter them, download checkers to ensure downloaded files are not

harmful or unstable before they are installed, and parental control features so that parents can track their children's online activities to protect them from danger.

Automatic back-up, online storage and bootable recovery

Aside from protecting computers against these and other threats, a truly comprehensive security solution should also include tools for automatic back-up, online storage and bootable recovery. Bootable recovery creates a CD, DVD or USB that enables you to get your computer back up and running, even if it is infected by a virus that prevents start-up. Automatic back-up safely backs up photos, music, documents and other important data to secure online data centres and to USB devices or discs. This ensures that, in the event of something going wrong, computers and information can be quickly and easily restored, minimising the negative impact.

While comprehensive protection is critical, these features and functionality typically impact system performance and can drain bandwidth with constant updates. It is also vital, therefore, to ensure that updates are incremental and can be scheduled for maximum convenience, while minimising the impact on system performance particularly when critical applications are running.

Bandwidth-management tools can ensure that non-critical updates are limited when connected via 3G or scheduled to certain times when bandwidth may be cheaper or uncapped. Smart schedulers can ensure that scans and updates are only run while the computer is not in use so that performance is not impacted, and tune-up tools allow you to fine-tune key system settings, free up memory and remove unnecessary clutter help computers run fast and trouble free.

In today's connected world, keeping your computer, your identity and your personal information safe requires sophisticated protection along with automatic back-up for strong protection without compromising performance. With a comprehensive protection suite you can browse, shop, bank and socialise online while remaining safe, protect your children from Internet dangers, ensure that photos, music, videos and important files are protected from loss, and keep your computer running fast and trouble free.

ABOUT THE AUTHOR

Fred Mitchell is the security business unit manager of Drive Control Corporation.

For more, visit: <https://www.bizcommunity.com>