Title:
Does Internet security software really work?

Word Count:
802

Summary:
In the recent years there has been many Internet securtity tools to hit the consumer market that claim to be providing excellent protection against online threats such as phishing sites, Trojan horses and viruses. Amongst Internet security packages there are Norton Internet Security, Webroot Spy Sweeper, McAfee Antivirus and many more. Are those products really so efficient in fighting threats and safeguarding our personal information from being stolen?

Keywords:
internet, security, software, malware, spyware, antivirus

Article Body:
In the recent years there has been many Internet securtity tools to hit the consumer market that claim to be providing excellent protection against online threats such as phishing sites, Trojan horses and viruses. Amongst Internet security packages there are Norton Internet Security, Webroot Spy Sweeper, McAfee Antivirus and many more. Are those products really so efficient in fighting threats and safeguarding our personal information from being stolen?

With the introduction of the Norton Internet Security 2007 that comes with a new interface and a lower price the private user may expect they get a comprehensive online protection and personal information safety whilst banking or shopping online.

These Internet security tools, and Norton Internet Security in particular, come with a bunch of smart features that can give you an additional protection against even unknown, or unrecognized threats by using behavior monitoring algorithms. But, many average users who never stray far from mainstream Web sites will find most of features of the internet security software available today unnecessary - it's like purchasing a BMW to drive it only to church on Sundays.

For example McAfee internet security tools still feel heavy and clumsy even if its new version, failing to find the happy medium between features, ease-of-use and performance.

On top of that, many applications do not play well with other security software you might already have installed on your PC. These are third-party anti-virus, antispyware and anti-adware software you purchased from other vendors that apps that may have been serving you well so far and there's no reason why you should stop using them.

Therefore, I recommend to have a look at the features first, before any purchasing decision is made – if you decide you don't need a BMW to drive to church once a week, a lighter, much more user friendly internet security software, such as ZoneAlarm Internet Security 7, may be a better choice.

Today, there are a few types of risks that may affect your PC's security while you surf the Web and install downloaded software: viruses, Trojan horses, spyware, worms and rootkits. Thes programs can install on your computer when you download software from untrusted sources or visit booby-trapped websites often referred as to phishing sites.

On top of that, malware often spreads itself by sending bogus e-mails to everyone in your address book. But not only pirate copies of software can contain dangerous code - viruses often come from unsuspecting sources; even some Sony music CDs inadvertently inflicted viruses.

All antivirus software packages available today is especially to deal with these threats by scanning downloaded files, running applications, scanning incoming e-mails, attachments and some of them can even scan instant messages blocking and deleting incoming malware. Security researchers say antivirus software has become essential, but it's no longer enough because you come across dangerous sites every day you surf the Web that can use smart techniques to launch an attack on your PC.

Some of the malicious software is designed to steal sensitive information such as login credentials, passwords, personal information and even credit card numbers. Hackers keep inventing new ways of stealing information penetrating your computer or hijacking keystrokes you type while you shop or bank online.

While online identity theft has become a growing problem, protecting your computer from these kind of threats is essential. Any chunk of information you keep on your computer or send over the Internet may be to cybercriminals. This is why you need strong Internet security protection – an anti virus, a firewall and an anti-spyware software.

Research show, that most security and privacy threats come from adware, spyware

and phishing. Security engineers admit these types of threats are amongst the fastest-growing threats to PC and personal security on the Web today. The major problem is that these applications are tiny programs that can be transported over the Internet and installed on the victim's computer in seconds and can not be detected without a proper anti malware program working in the background.

Some spyware and adware can be moderately not harmful, gathering information about what sites you visit or what you do while you work on the PC, however, there are still very dangerous spyware out there that can be used for example to connect your computer to a world-wide network of infected machines – a botnet – that cybercriminals often use to launch DDoS (Distributed Denial of Service) attacks.

An article called "State of the net 2006," issued in the September 2006 by Consumer Reports cites alarming statistics showing the damage caused by viruses, spywae and advare to computers owned by individuals and businesses. The magazine reports that nearly a million people replaced their computers in the past six months because of spyware infections.

Charles Brooker is IT security advisor and software tester at Norton-Soft – Information Source about Norton Software