



This article may be syndicated in whole or part. Simply provide a link back to the original article or <http://www.guardianprotection.com>. Please note that we usually update articles over time and the date last modified on article pages is usually referring to a navigational change.

Security in Today's World

There are many things in life that are worth protecting. Our children, our valuables, our resources and of course, ourselves. Only twenty years ago, if security was mentioned, you were speaking of protecting your home. And you were most likely discussing a security system, monitoring, watchdogs, firearms and cameras.

With the explosion of the personal computer, and the Internet's ease of access to information, security has now taken on additional roles. With over 605 million people online at any given moment worldwide, criminals are no longer bound by geographic location. Today's cyber criminal can hack from the comfort of his home just by getting online.

There are software programs that do nothing but scan the Internet for un-secure ports and open networks so that they can enter into those unprotected machines to access critical information. There are many users who know little about Internet security and rely on their ISP to provide it for them.

To look deeper into this topic, let's examine the qualities that make security both similar and different. With your home, you have a physical area that you can protect with fire and motion sensors, cameras, glass-break detectors and decals strategically placed to deter would-be thieves. For your computer, you protect a virtual space usually containing sensitive information relevant to your personal finances or key identity theft items such as family names and social security numbers. To protect these resources, one must install software (anti-virus, port scanners, Trojan hunting software, firewalls) as one level of protection. You can also add another layer of security through a hardware firewall of connectivity to and from the internet or network.

Both home security and computer security have maintenance costs associated with them. Reliable home security will usually consist of a one-time fee to install the hardware in your home, and then an agreement to have 24-hour monitoring service for a given length of time. Computer security will consist of buying the software and then either a monthly or yearly subscription fee to receive the latest information and protection from Internet threats.

One difference between the two is the methods of monitoring. While computer security is only responsive while the computer is active or online, home security monitoring is

responsive at all times provided the system is properly armed.

Another distinction is the method of response. In home security, a human will respond by dispatching police, fire or EMS directly to your home or business site. On a computer, the response is when the software vendor becomes aware of the problem, creates a solution, and has an update available for download.

With the advances of technology, monthly fees for home security monitoring are reasonable for the service they provide. Be warned: not all monitoring companies have the same capabilities when it comes to quick response. That's one reason why it's a good idea to make sure that any security company you choose has a UL certification. This can be critical as it indicates that the security company has met stringent standards for management system compliance (such as a back up source of power). The same methodology should apply for a security software provider. Just because they say they're the best, doesn't mean that they are. Due diligence is the user's responsibility. Your information is too valuable to be taken lightly.

Both home security and cyber security are similar to having insurance. You have it, but you hope you never need it. And if you do need it, you want a company or vendor that has a history of excellent customer service.

There are those people who think that having a firearm is all they need for protection. While that may hold true in some form, a firearm won't let you know if someone is trying to enter your home through the back door while you are sleeping and notify you or the authorities. Another common perception is that a watchdog will alert a homeowner to intrusion, but again, man's best friend sleeps 10 to 12 hours a day and can't notify the police.

There are some computer users who claim that they can detect a virus by the email that is sent with some obvious taglines meant for the user to open and infect the machine. Not all viruses are in emails, although that is the most common form. They can also be uploaded to a website, or embedded in Java Applets or Active X controls.

Trojans, which can log all of the users keystrokes and sites visited, are secretly downloaded in the form of free games or free software, and are undetectable by anti-virus software. This is the preferred method of attack by a hacker on a machine. By not altering the performance of a machine (like a virus or worm does), the user blissfully continues to use their machine to make online purchases, and enter sensitive information, thinking they are secure, while the Trojan secretly records all of the information and will simply send all of the user's information at designated intervals to the hacker.

Many times a decision about security measures for your home or computer is based on budgetary constraints. But always consider what it is that you are protecting and how much you would pay to get back whatever was stolen, lost or destroyed if an unfortunate event occurred in your life.

Article by Paul Bliss