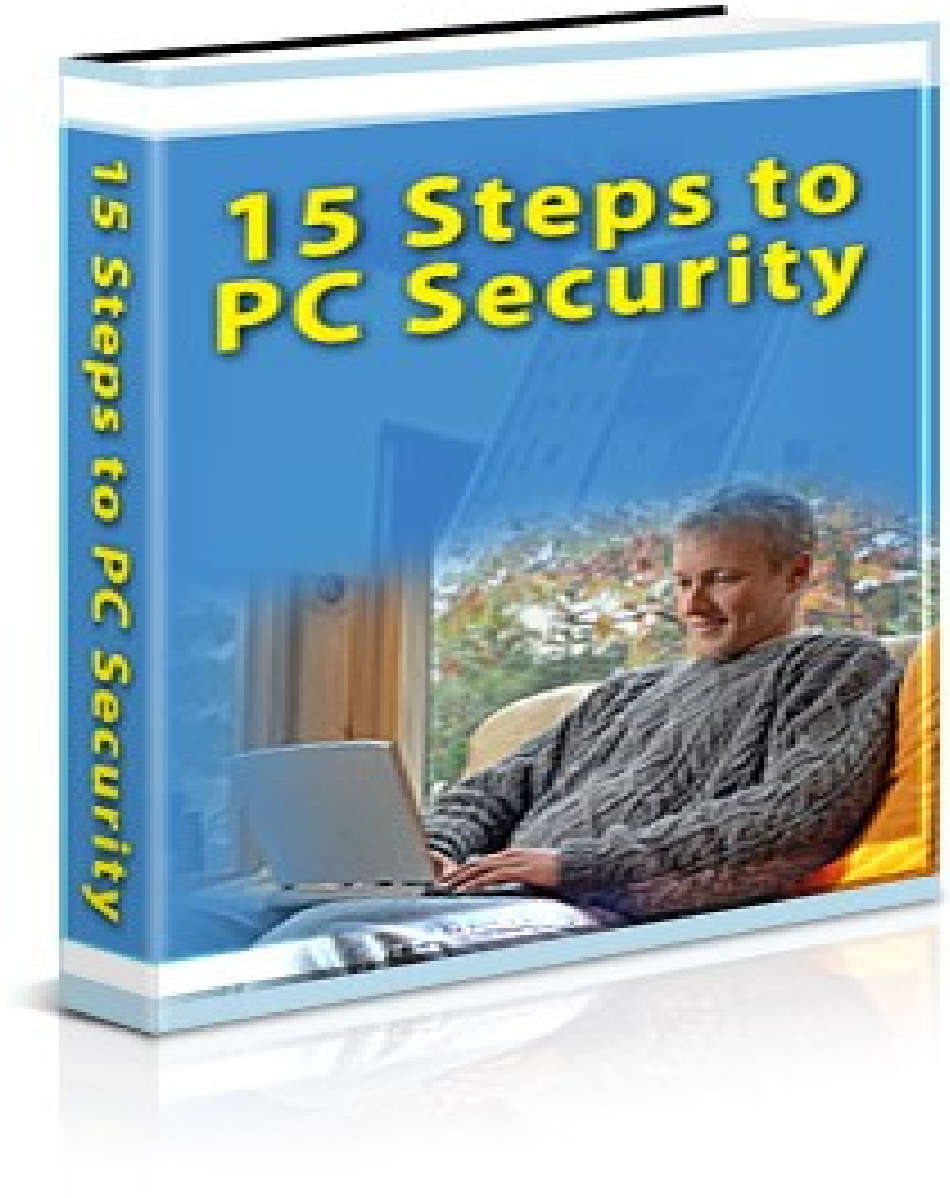

Brought To You By

NoAdware

Remove harmful adware,spyware, trojans, dialers and worms!

15 Steps to PC Security

Table of Contents

CLICK HERE

Step One - How Secure is Your Home Computer

Ensuring the Safety and Security of Your Home Computer

With the popularity of and the reliance on the Internet by almost the entire world population, there are suddenly a lot of things you can do and know with literally one click of the mouse. Making purchases nowadays doesn't require you to go to the shop or store; you can buy items online. Researching for various pieces of information can now be accomplished via the Internet.

However, there is an unfortunate reality that goes along with the wonders of the Internet. It also thanks to the Internet that computer security is always an issue. With the continued growth of the dependency of people (including businessmen, offices, government officials, and more) on computers and the Internet, this is a more important issue than what most believe.

If you are a home computer user, you still need to make sure that your computer is safe from any form of malicious online attack, including hacking. You might have important data (including any identification) in your computer which intruders can have access to.

That being said, it is important for you to find out just how safe your computer is from these potential attacks.

The very first step before actually tinkering with your computer is finding out the motive of intruders and why they target home computer users. They do this because (1) home computer users typically don't have security measures installed to counter them, which makes them easy targets; and (2) they often have valuable information stored that is enough to entice these intruders, such as credit card information. Think about it – you might potentially be a target.

Following that, you have to know what types of attack to expect – it is usually via email or clicking an ad-banner on a website. Opening an unknown, seemingly innocent email or clicking on an ad-banner will sometimes put you at unwanted risk and open the door for intruders. Once they're in, they're sometimes hard to get rid of, so your home computer security should start with you being careful about the things you do while connected to the Internet.

Being careful doesn't mean just choosing which emails to open or not, and which ad-banners to click to or not. This also includes sending

valuable information over the Internet, which is at risk for interception by a third party. It would be better to transmit really important information the old-fashioned way, unless you are very much confident in your security measures.

Next would be trying to place security measures in your computer itself. If your operating system is Microsoft Windows, they offer security updates and malicious software removal tools every month which are be extremely helpful to you – the same goes for other operating systems such as Apple OS and LINUX. There are monthly updates because the intruders always try to find a way to get around these security measures.

After getting the free security updates of your operating system, you need to get an anti-virus program, preferably one that has the greatest number of virus definitions (you might need to purchase this). Viruses, aside from causing chaos to your computer, can also be used to retrieve information from you and spread out to attack other computers. By obtaining a high-quality anti-virus program, viruses would not be as much of a problem.

Since intruders know the capabilities of anti-virus programs, they

sometimes choose to use what is known as spyware, which are little bits of data that can either be annoying or potentially dangerous. Aside from being able to slow down your computer processes, it can also be used to retrieve data from you. To combat this, there are anti-spyware programs available, both freeware and via purchase.

We will discuss spyware in depth further on.

The final security measure is a firewall. Normally, anti-virus programs offer firewalls; so acquiring one should not be much of a problem. A firewall acts like a security guard – it disallows outright entry to anything trying to access your computer (even if it is a program), without asking for your confirmation.

If you do not have these as your PC security and safety measures, you might be highly susceptible to an attack from intruders, if they haven't done so already. These measures ensure you that your computer and the data inside of it are safe and secure.

Step Two - All About Viruses

Computer Viruses and Guarding Against Them

In this modern Information Age, computers are necessities in life. Whether we use them for simple functions such as typing our homework and business reports, up to more important acts like online business meetings and transactions, one cannot deny that computers are a big part in our daily lives. Using a computer, particularly the Internet, is one task that even a ten year old can do at this particular period in time.

With the growing increase of popularity and reliance on computers, as well as the demand for it, security risks have also gone up, which is a reality that cannot be ignored. With the billions of information bits being spread across the World Wide Web, hackers and computer intruders (criminals) see the value in focusing their attention to computers and the Internet. The information they would retrieve here is (more often than not) more useful than when doing it the old-fashioned way.

As such, these intruders have devised methods to get information out

of computer users, with or without these people knowing that they've been hacked. As is the case in real life, there are some computer programs that are disguised to be innocent, but actually act as spies, providing information to the intruders. These malicious programs, which are security threats, are called computer viruses.

Computer viruses should not be taken lightly. They work in many different ways; one of them may be to provide data to the one who planted the virus. Other viruses can simply be annoying - slowing down your computer, building unwanted files, etc. – while some can be very disruptive, such as deleting your hard drive, compromising your operating system, etc.

As such, there are different types of viruses, which normally differ in how they function and how they are spread. Examples of these include Trojan horses, worms, email viruses, and logic bombs. It would be important for you to know these kinds of viruses in order to better protect you from them, as well as to have the proper programs to get rid of them.

Thank You For Reading

15 Steps To PC Security Preview

CLICK HERE FOR MORE