



Personal Security on the Internet

By

Shad Mortazavi

Nexus Global Technical Manager

Nexus Management Inc

Personal Security on the Internet - Dangers and Solutions

Published in: <http://newsviews.info/techbytes.html>

NOTE: The information contained in this document is the property of Nexus Management and is disclosed to you on the condition that you maintain the information strictly confidential. You are hereby warned that the information disclosed is subject to change without notice or the assumption of any liability on the part of Nexus Management.

Personal Security on the Internet - Dangers and Solutions

Welcome to Tech-Bytes and to the topic of personal security on the Internet. Over the next three issues I will be covering personal, corporate and enterprise security.

If you are reading this article on the Internet and using your personal computer without any security, you may be interested to know that there is high possibility that your system has been attacked or compromised in some way.

You may think that this is unfair or that this sort of thing will not happen to you. Think again, most hackers are indiscriminate and utilize whatever resources are available to them. Whether you are aware of it or not, as a user of the world's largest network you are inevitably exposed to all types of dangers and all types of people.

Hackers have a variety of motives and agendas and undertake lots of different types of hacking. One that you may be surprised about is the hacker that uses your system to unlawfully hack someone else's computer, so in fact it looks like you are doing the hacking. They may do this for pleasure or if you are very unfortunate they may have a different agenda. Some motives for hacking include showing off to other hackers, gaining information such as compromising a college network, or challenging their ability to compromise other systems. Hackers may engage in activities that effect your PC's performance and/or stability or may revisit your system time and time again to exploit other systems.

If you are unfortunate enough not to have installed any anti-virus software on your personal computer, then a hacker at this very moment could be looking at the same screen as you and they could be chuckling to themselves as you both read this article. Worse still, if you have a web cam that you leave on there is even a possibility that this person has picture and a recording of your voice.

A small time hacker such as this may show some interest in you, he/she may capture the packets emanating from your system and access information about you. Through this they may gain your name or pick up on your hobbies, or at worst they may discover your credit card details as you shop online.

On the other hand, you may have been compromised by a professional hacker. This person will have no interest in your computer system as it offers no resistance to his/her skills, but will use your system as a base to compromise a corporate system. In some cases this can solely be for the sheer mental exercise

Personal Security on the Internet - Dangers and Solutions

Published in: <http://newsviews.info/techbytes.html>

NOTE: The information contained in this document is the property of Nexus Management and is disclosed to you on the condition that you maintain the information strictly confidential. You are hereby warned that the information disclosed is subject to change without notice or the assumption of any liability on the part of Nexus Management.

of outsmarting a corporation who has taken their system seriously and invested heavily in security. Or more sinisterly, the professional hacker may be after information that can directly or indirectly lead to them making a financial gain. If this professional is to tell anyone about your system, it will be to a select few people. This highly skilled individual will not need to show off and in fact if they excel at what they do, like a good criminal they will not leave any clues as to their activity.

This all may sound like a clip out of the movie Hacker or Swordfish, but hacking is a real threat & is taken seriously by the IT world. Some of the individuals, like the hackers in these movies, are extremely talented people with a deep insight into the working of your operating system and the protocol that facilitates the communication of the information between the different components of the Internet.

However unlike in the movies, information about computers and hacking is not a state secret. This is where the fantasy of these films diverges from the reality. In fact, nearly every exploit of operating systems and piece of equipment used on the Internet is fully documented and this information is readily available to the public by means of the Internet. The tools used by hackers, are also easily available for download and are in most cases free. There is now a whole volume of books that explain the exploits of hackers, how they are performed and how they can be prevented, from the simplest to the most sophisticated hack.

After reading all of the above you should now have a better understanding of the dangers of being online. As a security consultant, I wish to further reiterate the possible hazards of working on the Internet but also offer you some simple tools that you can use to combat this threat. There is no need to spend a fortune, and in most cases the tools can be found on the Internet and are downloadable.

There are 3 tools that will help minimize your exposure and vulnerability. I recommend at least the first two and advise the third if you have sensitive data. Please remember that no one technology is guaranteed to keep your system secure.

Before investing in any security tools, it is a good idea to scan your PC to check for existing viruses and security risks. Symantec's Security Check will undertake this service free of charge. Norton also provide a good suite of professional products for the home user, which are easy to update. Information on such products can be found at [Norton's website](#)

Personal Security on the Internet - Dangers and Solutions

Published in: <http://newsviews.info/techbytes.html>

NOTE: The information contained in this document is the property of Nexus Management and is disclosed to you on the condition that you maintain the information strictly confidential. You are hereby warned that the information disclosed is subject to change without notice or the assumption of any liability on the part of Nexus Management.

The first tool I would recommend is

1. A Good Personal Firewall

A firewall is a hardware or software device which looks at the conversation between your system and the Internet. They will permit and deny access to and from your system based on rules specified by you. They are available in three flavors:

- A hardware ADS/DLS router, a hardware device that sits between you and the Internet. These are fairly inexpensive devices that are easy to configure and provide you with a good degree of security. Two that immediately come to mind are Syslink and D-Link's devices.
- A software personal firewall; one of my absolute favorites is ZoneAlarm. The basic version of their software is free for download, and is very intuitive, easy to use and stable.
- I have also had very good experience with the Symantec product, Norton Personal Firewall.

Personal firewalls in most cases are not very sophisticated; one product that attempts to apply some of the security principles encompassed in industry strength corporate firewalls into the personal firewall product is one found at PC VIPER.

For those of you considering Linux, SuSE is shipped with a good personal firewall.

If you are well versed and have the equipment, you may consider configuring a Linux box as your firewall. This will be the object of one the future Tech-Bytes articles.

2. Anti-Virus software

This is equally as important as a Personal Firewall and is available from a variety of sources, such as for download from certain websites, or through free software from a computer magazine.

Without anti-virus software a hacker may gain access to your system using software known as a Trojan. Most Trojans are well documented and can be detected using an anti-virus engine. Again Symantec's Norton product is amongst one of the best, very well documented, and stable, with a good update engine.

Personal Security on the Internet - Dangers and Solutions

Published in: <http://newsviews.info/techbytes.html>

NOTE: The information contained in this document is the property of Nexus Management and is disclosed to you on the condition that you maintain the information strictly confidential. You are hereby warned that the information disclosed is subject to change without notice or the assumption of any liability on the part of Nexus Management.

Another good free product (for personal use) is AntiVir. Plus there is a Linux/FreeBSD and Microsoft Windows.

3. Intrusion Detection

Finally there are pieces of software that look at known attack patterns. One of the best known is BlackICE. Black ice is unique, in that it tries to detect intruders based on known exploits and then informs the user about these.

When using any of the above systems, please remember to update the definition files on a regular basis. In most cases the program can be scheduled for a regular daily update and will often tell you or remind you as it is updating itself. This is vital otherwise, you may spend hours and dollars reviewing and protecting your system, but by not updating these products on a regular basis you are giving the opportunist a chance to exploit your system.

Last but not least, be vigilant.

Shad Mortazavi