



Indian Computer Emergency Response Team

Department of Information Technology
Ministry of Communications & Information Technology
(Government of India)



CCAOI

Representing the ecosystem of Internet - Bharat Model

Security Newsletter

15th December, 2010

As internet is becoming an integral part of our lives, it is important that we are aware of the threats we face in the Cyberspace. The need of the hour is to be aware and adequately equipped to protect ourselves online.

Symantec in their **2010 State of Enterprise Security** study released on 20th Dec 2010 reveals that **75% organizations experienced cyber attacks** and **42% organizations rate security as their top issue**, more than natural disasters, terrorism, and traditional crime combined. Cyber attacks cost enterprise businesses an average of \$2 million per year, and are often very effective, according to the report.

Gartner has forecasted that by 2015, online sabotages will become multi-modal and very damaging and that even a G-20 nation's critical infrastructure will be disrupted and damaged by such cyber attacks.

Keeping this in view, with the support of **Indian Computer Emergency Response Team (Certin)**, **Department of Information Technology**, **VeriSign India** and **Sify Technologies Ltd.** we are releasing the next edition of our fortnightly Security Newsletter where we try **Debunking Some Common Myths**.

Debunking Some Common Myth

There are some common myths that may influence your online security practices. Knowing the truth will allow you to make better decisions about how to protect yourself.

While believing these myths may not present a direct threat, they may cause you to be more lax about your security habits. If you are not diligent about protecting yourself, you may be more likely to become a victim of an attack.

What are some common myths, and what is the truth behind them?

- **Myth: Anti-virus software and firewalls are 100% effective.**

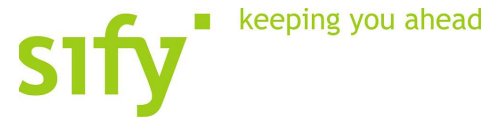
Truth: Anti-virus software and firewalls are important elements to protecting your information. However, neither of these elements is guaranteed to protect you from an attack. Combining these technologies with good security habits is the best way to reduce your risk.

- **Myth: Once software is installed on your computer, you do not have to worry about it anymore.**

Truth: Vendors may release patches or updated versions of software to address problems or fix vulnerabilities. You should install the patches as soon as possible; some software even offers the option to obtain updates automatically. Making sure that you have the latest virus definitions for your anti-virus software is especially important.

- **Myth: There is nothing important on your machine, so you do not need to protect it.**

Truth: Your opinion about what is important may differ from an attacker's opinion. If you have personal or financial data on your computer, attackers may be able to collect it and use it for their own financial gain. Even if you do not store that kind of information on your computer, an attacker who can gain control of your computer may be able to use it in attacks against other people.



- **Myth: Attackers only target people with money.**

Truth: Anyone can become a victim of identity theft. Attackers look for the biggest reward for the least amount of effort, so they typically target databases that store information about many people. If your information happens to be in the database, it could be collected and used for malicious purposes. It is important to pay attention to your credit information so that you can minimize any potential damage

- **Myth: When computers slow down, it means that they are old and should be replaced.**

Truth: It is possible that running newer or larger software programs on an older computer could lead to slow performance, but you may just need to replace or upgrade a particular component (memory, operating system, CD or DVD drive, etc.). Another possibility is that there are other processes or programs running in the background. If your computer has suddenly become slower, you may be experiencing a denial-of-service attack or have spyware on your machine.

- Author: Mindi McDowell. Produced 2006 by US-CERT