

## Protecting Your Computer in the Face of Cyber Warfare



Any computer that is not properly protected is a cyber weapon waiting to be loaded and used! There are over 1 million pieces of malware in circulation today. Numerous studies suggest an unprotected computer connected to the internet can be compromised in less than 1 hour – some say in less than 10 minutes.

Managing computer security within the confines of any organization is a difficult job. Worms, viruses, spam, malware, port scans and perimeter defense probes are constant threats. Your mobile workforce is an additional challenge because they are at the mercy of their surroundings. You need a strategy to ensure your systems and data is as safe on the road as they are in your corporate offices.

Every individual needs to:

1. Make sure all software has the latest patches, service packs and updates. To do this, go to the software vendors' web site and search for updates.
2. Install, use and maintain anti-virus software. There are an estimated 200 new software viruses released on the internet every month. Scan your computer at least weekly to make sure it is not harboring viruses or worms.
3. Install, use and maintain anti-spyware software.
4. Install, use and maintain anti-spam software. Do not respond or click on any links included in Spam emails. Do not even use the "unsubscribe" link in their email.
5. Avoid running attachments, particularly .EXE files that may come in your e-mail, even if they come from individuals you know.
6. Install and use a firewall. Firewall software is mandatory to restrict dangerous network traffic from compromising your computer. Make sure the settings are in the medium to tight range and not the lower level protection settings.
7. Protect your passwords. Use a combination of number and upper as well as lower case letters. Never give out your password to anyone.
8. If you have a laptop, encrypt the hard drive.
9. Backup your data regularly. If the computer is used for business, back it up at least monthly.
10. Don't install unfamiliar programs, bootleg copies of programs, or freeware from web sites other than main players like yahoo and others.
11. Lock the screen or logout when away from the computer even for a few minutes.
12. Turn your computer off when you are not using it. The downside is that being "always on" renders computers more susceptible.

**CONTACT**  
**technolytics**

4017 Washington Road  
Mail Stop #348  
McMurray, PA 15317  
P 888-650-0800  
I [www.technolytics.com](http://www.technolytics.com)

About the Author: Kevin G. Coleman is an international security and intelligence consultant with Technolytics and has regularly featured articles in DefenseTech.org and International Intelligence Magazine covering homeland security, terrorism, security and intelligence worldwide. For six years he served as a science and technology advisor to the nation's leading research and development center that service the U.S. Department of Defense, Department of Homeland Security and the Intelligence Community. Additionally, he testified before Congress on Cyber Security and Privacy.