

Computer security newsletter

Secure your computer

Step 1—Secure Firewall

- Step 2—Virus protection
- Step 3—Spyware/adware
- Step 4—Data backup
- Step 5—System updates
- Step 6—Acceptable use policies/Safe Email usage
- Step 7—Digital certificates and encryption

Each issue of our newsletter addresses a new step in securing your computer.

Special points of interest:

- Is your computer secure?
- If you had a computer crash or were hacked into, would you be able to recover?
- AWC Consulting provides comprehensive computer support to secure your valuable computer data.
- Be sure to check out our Security Audit special on page 3.

Inside this issue:

Secure your computer with a firewall	2
Understanding firewalls	2
Beware common attacks	2
AWC Consulting company profile	3
Security Audit: Small Office Special offer	3

How secure are you?

The data your computer holds is invaluable. Should you be the victim of data loss, the amount of time required to rebuild (if possible) your company's files would be incredible. Given the value of the data to your business, it is extremely important to take steps to protect it. Data loss can occur from a variety of different problems.

This issue reviews Internet security and the steps you should take to protect your company from online attacks.

AWC Consulting offers a broad variety of services to protect your information, including:

Firewall: Keep hackers out of your computer. The number of online threats grows every day....

Antivirus gateway: Prevent viral infections before they reach your internal network. Your first line of defense from infection...

Antivirus software: Virus attacks are a frequent and ever changing threat. Should you or an employee open a dangerous file your data can be destroyed...

Digital certificates and encryption: Sending email is akin to yelling all your secrets out in a room full of people. Find out how to secure your email messages....

Acceptable use policy: Employees need clear direction on what is considered acceptable uses of a company computer. Minimize



Is your data secure from computer hackers?

your exposures...

Safe email practices: Email is now the most common virus attack method. By implementing some simple steps you can protect yourself from becoming a victim....

Operating system and program updates: Security holes are found in Windows and other popular applications on a regular basis. If you do not update your machine consistently, you are vulnerable...

Data backup: Sometimes the worst happens. If your computer fails, will you be able to recover?

Contact AWC Consulting to help you secure your company's information.

The danger of being online

When your computer is connected to the Internet, it is exposed to a variety of potential threats.

When you browse the Internet, other computers on the Internet can communicate with your computer. This leaves you extremely vulnerable to a variety of common attacks. This is especially troubling as several popular programs (such as Kazaa) open up services on your computer that allow others to view your files.

Security flaws are discovered on a regular basis and allow hackers to attack your computer with

the potential to view or destroy the sensitive data stored there.

With the advent of high speed Internet connections, people are putting their computers at great risk. Being constantly online means leaving yourself open to attack at any time.

Several virus outbreaks have been spread by attacking vulnerable computers connected to the Internet. Is your computer safe?

Beware common attacks

Many people believe that online attacks are the domain of computer experts. Unfortunately, this is far from the truth. Even an inexperienced computer user can easily attack your computer. These hackers (often referred to as “script kiddies” as they are typically teenage boys), download scanner programs that automatically search for computers with common security flaws. These programs scan thousands of computers per minute and then flag the computers that have security flaws.

The scanners enable the hacker to, for example, attack and exploit vulnerable computers. These attacks can be orchestrated simply by downloading and installing the offending program onto a computer.

This form of attack is extremely common and most new firewall users are shocked at the number of probes and attacks their computer receives from the Internet.



A firewall protects you from online hackers attacking your computer.

Secure your computer with a REAL firewall

To secure your computer from attacks you need to “teach” your computer to ignore or resist external connection attempts and probes. The generic term for such a program is a Firewall. There are two common firewall types:

- 1) **Software firewall:** This installs directly onto your computer. These programs monitor your Internet connection and attempt to block unwanted external attacks. While your computer has a direct connection to the Internet, the software attempts to control and protect the connection.
- 2) **Hardware Firewall:** This is a piece of equipment that is connected to the Internet. The hardware firewall is the only piece of hardware that is directly connected to the Internet. Your computer is protected as it requests information from the Internet through the firewall.

There are a multitude of “firewall routers” being offered to consumers to “secure” your connection to the Internet. Unfortunately, these routers mainly provide a way to share an Internet connection with little or no true security. It is critical to know if your connection is secure.

“Many people believe that online attacks are the domain of computer experts. Unfortunately, this is far from the truth”

Understanding firewalls

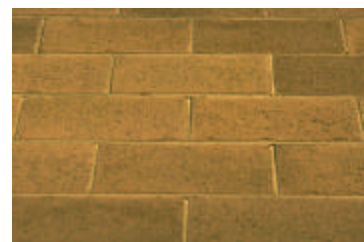
Software firewalls are best used on individual home computers. Hardware firewalls are best used in multi-computer environments to secure all computers in an office. Software and hardware firewalls can be used together, but great care must be taken to ensure proper setup and operation.

A well configured hardware firewall offers more protection than a software firewall as it is not susceptible to direct virus attacks (a virus can disable or circumvent the software firewall). A hardware firewall can not be circumvented by users, and manages/maintains all security policies in one location. A hardware firewall allows for effective

enforcement of the firewall configuration in an office can protect multiple workstations.

As with Antivirus software, a software firewall, if not utilized and updated properly, can provide a false sense of security. Software firewall options are critical, and changing the configuration of the software (for example to allow a game to work) can create significant risk of unintended security breaches.

Setting up an effective firewall requires careful planning. AWC Consulting can help you create an effective security plan to protect your computer(s) from attack.



A firewall is one part of a complete security plan. AWC Consulting can create an effective security foundation for your company.

PO BOX 45070 RPO Mid-Yonge
Toronto, Ontario M4P 3E3

Phone: 416.783.7951
Fax: 416.783.8829
Email: sales@awcconsulting.com

Your complete computer consulting supplier

Secure your computer



Step 1—Secure Firewall

- Step 2—Virus protection
- Step 3— Spyware/adware
- Step 4—Data backup
- Step 5—System updates
- Step 6—Acceptable use policies/Safe Email usage
- Step 7—Digital certificates and encryption

Please contact us if you require additional newsletters or back-issues.

Company profile

AWC Consulting has provided effective solutions to clients for over six years in the Greater Toronto Area. We support a wide variety of companies ranging in size from one person to over one hundred.

Consulting services

Computers are a fact of life in business. You want your computer to perform its function easily and efficiently. AWC Consulting allows you to focus where you add the greatest value... doing your job. Don't waste your valuable time trying to keep your computer running in tiptop shape. Let AWC Consulting help you.

As your partner, AWC Consulting takes the time to learn *your business and your computing requirements*. With this information we can develop a custom solution to meet your business needs in the most effective manner possible. Our goal is to help you succeed in your business by letting you *focus on doing your job*. You do not need to fight with your computers or waste valuable time trying to get your computer equipment to perform the way you want. We offer a wide variety of training, Internet/network, maintenance, and troubleshooting services to help you leverage your computer investment.

Learn more online

To learn more about AWC Consulting, please visit our web site: www.awcconsulting.com



Security Audit: Small Office – Special Offer

AWC Consulting can secure your office network. For a limited time we are offering our **Security Audit Service** for half the regular price.

This special offer includes the following:

- Scan up to 10 workstations for vulnerabilities and document steps required to secure workstations.
- Scan up to 10 workstations for Virus and Spyware infections. Remove (if possible) any detected Virus and Spyware infections.
- Scan 1 server for vulnerabilities and document steps to secure server.
- Assess current firewall (if present) with external and internal port probes.
- Scan entire internal network and note all connected devices requiring investigation.
- Scan for open file shares.
- Provide a printed assessment listing major vulnerabilities.

COST: Only \$750. LIMITED TIME OFFER. Price subject to change without notice.

Limitations: 10 hour limit. For offices with severe security problems, not all problems will be documented within this time limit.

All taxes are extra.

AWC Consulting can prepare a custom Security Audit to meet your needs. Please contact us for additional information.



We also offer detailed audits following the Open Source Security Testing Methodology Manual. Call for further details.