

## Internet Security

### Part 1 of 3: Nature of the Threat

Internet access can be an incredible tool in today's business. Being able to access information quickly keeps you at the top of your retailing game.

However, with this accessibility also comes an increased responsibility to protect yourself from the world at large. Just as internet access allows you to connect to the World Wide Web and have all that is available at your fingertips... this also puts your computer out there for anyone in the World Wide Web to connect to **your** system and have all **your** information at their fingertips!

In this month's newsletter, we'll cover part 1 of our 3 part series on Internet Security. You'll find out what some of the most common threats are, and understand some commonly used terms.



#### Malware

This is a broad term that covers any form of malicious software, including:

- Viruses
- Worms
- Trojan Horses

These types of programs are intended to cause data destruction, system malfunctions or crashes, or any other form of unwanted behavior.

Malware can be delivered uninvited by a computer hacker if your system is vulnerable. Or, you could choose to download a seemingly benign program from the internet, and inadvertently bring it into your system.

#### Spyware

Spyware is generally any program that tracks and collects information on your internet activities. This information is often used by companies for marketing purposes. You may read in the fine print of free software (freeware), like screen savers and weather reporting services, that you are installing spyware by downloading those programs.

#### Adware

Most freeware or shareware comes with some type of limited advertising (that's why it's free!). Adware is additional software that may be inadvertently downloaded in the same manner as spyware, and that will continue to generate advertising even when you are not running the originally desired program.

Even if Spyware and Adware do not deliver any malicious code to your system, they bog down your system's resources and cause unwanted behavior. They are also often an indication that other malware may be present.

#### Phishing

This is a form of internet fraud that aims to steal valuable information such as credit cards, social security numbers, user IDs and passwords. A fake website is created that is similar to that of a legitimate organization, typically a financial institution such as a bank or insurance company. An email is sent requesting that the recipient access the fake website (which will usually be a replica of a trusted site) and enter their personal details, including security access codes.

Over the years, the computer industry has become very adept at offering very effective products to combat these threats. A good internet security strategy will deliver peace of mind, so that you can take advantage of all the internet has to offer your business, without compromising your security.

Watch for next month's newsletter, where we will cover part 2 of the Internet Security series: Firewalls.

### Helpful Contacts

#### iCAM Webstore Support has a new number!!

- Phone: **800-949-1470 Option 8**

#### Supplies

- Email: [supplies@camcommerce.com](mailto:supplies@camcommerce.com)
- Phone: 800-CAM-DATA
- Fax: 714-241-0145

#### Training

- Phone: 866-442-1887

#### Installation

- Phone: 800-949-1460