# Partner News

**May 2009**

*For over 25 years Software To Go has been offering superior products, service and support to small and medium sized businesses.*

*Software To Go is a full-service Technology Solution Provider specializing in computer and software pre-sales knowledge and post-sales support!*

*The Staff of Software To Go*

*We belong to Business Networking International, a group of businesses referring business to each other.*

*If you are looking for new customer or clients we invite you to come as our guest to a networking event. Meet seventeen local business professionals who will refer your business to their customers.*

*For more information:*
*Our Web Site*

## Beware 'Swine Flu' Internet Scams

Thieves are eager to take advantage of the panic. U.S. CERT warned of scams in which purveyors of malware attempt to get victims to click on infected attachments by using social engineering techniques (new name for a con-job). As always, the advice is to not trust alarming messages from senders you don't know.

The scam as reported by McAfee's Avert Labs appears to be very similar to traditional pharmaceutical spam, modified to take advantage of the concerns of the day.

As InternetNews.com has noted, thieves and spammers tend to take advantage of breaking news and trends. Every year, there's a spam outbreak for Valentine's Day and specially targeted malware for tax time. Scammers even tried to take advantage of the September 11th terrorist attacks.

## What types of files can hackers corrupt?

A hacker may be able to insert malicious code into **any file**, including common file types that you would normally consider safe. These files may include documents created with word processing software, spreadsheets, or image files. After corrupting the file, an attacker may distribute it through email or post it to a web site. Depending on the type of malicious

www.software-to-go.com

*Contact Us*
*636-441-3420*
*314-727-3420*

*Visit our retail location*
*1385 Triad Center Dr.*
*St. Peters, MO 63376*

code, you may infect your computer by just opening the file.

When corrupting files, attackers often take advantage of vulnerabilities that they discover in the software that is used to create or open the file. These vulnerabilities may allow attackers to insert and execute malicious scripts or code and they are not always detected. Sometimes the vulnerability involves a combination of certain files such as a particular piece of software running on a particular operating system or only affects certain versions of a software program.

**What problems can malicious files cause?**

There are various types of malicious code, including viruses, worms, and Trojan horses. However, the range of consequences varies even within these categories. The malicious code may be designed to perform one or more functions, including:

- Interfering with your computer's ability to process information by consuming memory or bandwidth (causing your computer to become significantly slower or even "freeze")
- Installing, altering, or deleting files on your computer
- Giving the attacker access to your computer
- Using your computer to attack other computers

**How can you protect yourself?**

- **Use and maintain anti-virus software** - Anti-virus software recognizes and protects your computer against most known viruses, so you may be able to detect and remove the virus before it can do any damage. Attackers are continually writing new viruses, it is important to keep your definitions up to date.
- **Use caution with email attachments** - Do not open email attachments that you were not expecting, especially if they are from people you do not know. If you decide to open an email attachment, scan it for viruses first. Not only is it possible for attackers to "spoof" the source of an email message, but your legitimate contacts may unknowingly send you an infected file.
- **Be wary of downloadable files on web sites** - Avoid downloading files from sites that you do not trust. If you are getting the files from a supposedly secure site, look for a web site certificate. If you do download a file from a web site, consider saving it to your computer and manually scanning it for viruses before opening it.
- **Keep software up to date** - Install software patches so that attackers cannot take advantage of known problems or

vulnerabilities.

- **Take advantage of security settings** - Check the security settings of your email client and your web browser. Apply the highest level of security available that still gives you the functionality you need.

***Software To Go Provides a Number of Maintenance and Support Programs Designed to Fit the Needs of Almost any Business!***

**We still sell XP Pro loaded on all of our computers**

Starting at$599, our computer come loaded with XP Professional, two spyware removal applications and configured for security. All you have to do is turn it on and start using it!

**Did you know?**

**Do you want to keep your information safe for free?**

There are many sophisticated ways to protect your information, but one of the most powerful ways is to **make it unavailable** to prying eyes. The easiest way to do that is to **turn off the equipment**. It doesn't matter how good a hacker is. If your computer is off and they don't have physical access to it, then they can't get your data.

Turning your computer off also **saves electricity and cash**. Some companies disconnect their network from the Internet each night by

*We belong to Business Networking International, a group of businesses referring business to each other.*

*If you are looking for new customer or clients we invite you to come as our guest to a networking event. Meet seventeen local business professionals who will refer your business to their customers.*

*For more information, contact us*
*636-441-3420*
*314-727-3420*

throwing a power switch.

In a business, you can also increase your security by allowing computers to power down after a period of inactivity. You can set your computers to lock after a few minutes of inactivity as well so someone needs to log in to see your valuable data.

In the various versions of Windows, you can do this by right clicking on blank space on the desktop, selecting properties, and configuring the screen saver. Banking web sites and other security conscious sites, network devices and other devices have inactivity lockouts offering protection with little effort.