

### Get Helpful Information:



## Viruses, Malware & Spyware...Oh My!!!!

*News article posted 9-9-09*

### Let's see...

in the months of July and August 2009, **Small Business Technologies (SBT)** has had at least one computer support call to... Wooster, Ashland, Akron, Medina and Cleveland Ohio all for the same basic reason – virus, spyware or malware removal. In fact, in our 9 years of service in the Northeast Ohio area, I would venture to guess that resolving Spyware and Malware related problems accounts for at least 25% of our troubleshooting service calls.

Perhaps the top two questions I receive from customers when we visit them to address virus related issues is "Why do people do these things?" and "What should we be doing to stop acquiring or remove unwanted pests?"

I do my best to help both small businesses and home users understand that the type of people who create and proliferate these pests has changed over the years. A mere 10 years ago, the "bad guys" simply wanted to wreak havoc on else's computer to brag to their peers about the creative code they developed to make someone else's life difficult. In a word, I would broadly categorize these individuals as vandals.

Today's malware creators are much more sophisticated and purposeful in their strategies. Sometimes their aim is to expose sensitive information entered or stored on a user's computer for their own misuse or to sell to a 3rd party for criminal purposes. A good example of this is

Are you or your business currently dealing with technical issues stemming from viruses, malware, or spyware. SBT is happy to offer our help. You are welcome to contact us at your convenience.



Email SBT:  
[help@sbtechs.com](mailto:help@sbtechs.com)



Call SBT:  
**330.335.7278**



Tell SBT:  
**Information Form**

a software keystroke logger that captures the website, username and password of a banking site that a user visits. **Read this article for an in-depth discussion of the topic.**

More frequently we see malware installed on pc's that has silently rendered the user's system to the role of a "zombie" computer. As far as the creator of this software is concerned, their eventual intent for your now infected computer is often times to use it in a Denial of Service (DOS) attack on a 3rd party website. In this unfortunate scenario your pc, along with millions of other infected pc's, will flood a particular website with meaningless traffic to bring the website to a crawl. This was the exact type of attack that happened to the Twitter.com site in August. **Read the Time Magazine article.**

If your pc has been infected in this manner, you may experience general slowness due to the fact that there is extra software running on your pc taking away valuable clock cycles from the processor which would otherwise be used for word processing, email or web browsing.

So this leads to the next question I am asked by our customers.... "How can we prevent malware, spyware and viruses from infecting our network and remove them once we're infected?" As I discussed in this **Connecetions Newsletter article** for Palitto Consulting in February 2009, most companies are best served by taking a multi-faceted approach including a proper firewall, anti-virus software and internet usage policies. Intrusion detection systems like those provided by **Protectus** are also invaluable tools.

Other methods small businesses can adopt center around preventing users from being exposed to areas where they might become infected in the first place. Proper spam filters like those provided by **AppRiver** help prevent potentially infected emails from reaching user inboxes.

Businesses can also adopt technologies to help prevent users from visiting malicious websites as well. These are typically referred to as web-content filtering solutions. Basic versions will simply block the user from visiting an inappropriate site. More robust versions will also report the activities of users to the network administrator as well as allow users to request exceptions to visit specific sites. Ask your computer professional for advice on what type of solution would best fit your company's needs.

Finally, if your pc has been infected already, a business needs to have a strategy in place to restore the infected pc's back to their original condition. Tools like HijackThis from **www.majorgeeks.com** or **Spybot Search and Destroy** can help remove viruses, spyware and malware after they have infected a pc. Deeper infections might need to be addressed with a tool like **IceSword** which, though effective, might require the assistance of a computer professional to employ.

The most important method of protecting your pc's is to ensure you have proper backups in place. In this way, no matter how bad the malware may get, any data on the computer and

the operating system and applications can be reinstalled or restored. The former can be a time consuming and expensive process. At SBT, we sell and implement devices that can take nightly images of multiple pc's on your network. This strategy protects in the most thorough way possible because you can just restore everything (operating system, updates, drivers, apps and data) back to the hard drive with the last good clean image before infection. This solution has the added bonus of restoring a pc even if the physical hard drive itself fails.

So where will our next malware removal visit take us to? Beachwood or Wadsworth? Lorain or Canton?

If you have are concerned about the risks of malware exposure and would like to find out what prevention strategies are best suited for your business, drop me a line or contact your local service provider.

**Dan Allen NET+**

***Small Business Technologies, Inc***

Wadsworth, OH

**[www.sbtechs.com](http://www.sbtechs.com)**

**[responddodan@sbtechs.com](mailto:responddodan@sbtechs.com)**



**Did you find this article helpful?**

*Visit the SBT News page for other helpful articles and information*

