My Bowling Diary

Strike out with information… don't spare the details!

August 2005

In the June 2005 newsletter, I started a series of articles on protecting yourself on the Internet. It is my hope that it gave you good information and insight. This article deals with viruses, worms and other types of malware that may find their way to a computer near you. Should you have any questions about the content of this article, please feel free to send an email to tsawyer@mybowlingdiary.com.

If you have a subject that you would like to see an article on, please send an email to info@mybowlingdiary.com.

Viruses, worms and other Low-Lying creatures

(By Timothy A. Sawyer, CISSP)

In my June 2005 article, I wrote about protecting yourself on the Internet by being able to deduce fraudulent emails as well as secure vs. non-secure Web sites. This month, I am going to talk about viruses, worms, malware and other dangers that lurk in cyberspace. I will also throw in a little editorial.

Viruses, worms and other forms of malware are programs that are transmitted from one computer to another by various means. Before the Internet explosion, viruses were mainly transmitted on floppy disks and other media. However, viruses are more commonly spread through the Internet, with the more popular forms of transmission being via email and also embedded on downloads from web sites.

Why are viruses spread? Some are spread to try to gain control of a computer. Others are spread for the hope of financial gain. Others are spread simply to wreak havoc. In my opinion, viruses serve no useful purpose. When a virus spreads it simply causes a lot of damage. Companies around the world lose millions of dollars in revenue because they shut their network down when a virus is spread, as well as the extra man hours that they spend to combat the threat. (EDITORIAL) Those who spread viruses, in my opinion, should be found, arrested, tried in a court of law and if convicted, sent to jail for a long time and be permanently banned from working with computers in any form. In addition to that, they should also pay some form of restitution.

With that said, we will always have these low life people on the planet who have nothing else better to do than to wreak havoc. The trick is to reduce the risk of havoc. How do you do this? This you can do rather inexpensively by following these steps:

1) **Anti-Virus software**

Do you have anti virus software? If so, you are on the right path. If you don't, **go buy some**. I'm not going to endorse a specific brand, but the two more popular programs are made by McAfee (http://www.mcafee.com/us/) and Symantec (http://www.symantec.com). I have seen both of these in home use as well as corporate use. Most PCs sold today are sold with one of these two packages installed with a limited subscription. You can also go to any major electronics store and pick up a good package for a reasonable price.

When you purchase anti-virus software from Symantec or McAfee, you purchase a subscription which entitles you to maintain your anti-virus definitions by connecting to their website and downloading their updates. So if you DO have anti-virus software but DO NOT have a current subscription, you may be protected against older viruses but not the newer ones. So if your subscription is NOT current, update it, and keep it updated. For the price that they usually ask for their subscriptions, it is well worth it when you consider the cost of rebuilding a PC operating system and retrieving your files. Been there, done that.

2) **Keep your virus definitions updated and scan regularly**

Always keep your virus definitions updated. The rule of thumb is to update at least weekly and to scan after a new update has been downloaded. Scan on a regular basis, at the very least, weekly.

3) Scan all incoming files and email

If your software has the capability to scan all incoming files and email, turn that capability on and **keep it on**. This is the best way to keep yourself protected against viruses between regular scans.

4) Don't open suspect emails or files

If you get an email that you suspect has a virus, it probably does. Don't open emails that you suspect might be infected, especially if they have attachments. Some infected emails actually said in the body of the email that it was scanned. Don't believe it, scan it yourself.

Generally we say don't open emails from people you don't know. However, most viruses are spread by using the victim's address book, so an email you receive may come from someone you know. Be careful just the same.

5) Be careful what you download

Be careful when you download software from web sites. Some of these programs may contain viruses, malware and Trojan Horses (a Trojan Horse is simply a dormant virus that launches itself when certain conditions are met). If you do download software from the Internet, make sure that you do not run it from the site unless it is a well known publisher such as Microsoft.

6) **Be a good cyberspace citizen**

Be a good cyberspace citizen. If you send attachments, scan the attachment before you send it. When you send email, scan the email before you send it. If you see a suspicious email, report it to your anti-virus software provider. Chances are they know about it, but they (and the rest of the civilized world) appreciate it when you take the time to report a threat.

7) **Keep up on the latest threats**

Most anti-virus software providers maintain a web site that has up to date information on known virus threats, as well as instructions on what to do if you inadvertently catch one. This information is usually free to the public.

So there you are. Seven steps that you can take today to protect yourself, and without spending oodles of money doing it. If we all take these simple steps, we are doing our part to make the Internet a safe place to do business as well as to have fun.