

TECH TALK

Bob Appleby

They're Coming to Take Memory Away!

Malicious Computer Code¹ has been causing havoc on our computers for years. Their method of delivery has become sneakier and the damage to our systems has become so much greater. Some code keeps making a comeback through more ingenious delivery methods revolving around what has been tagged as social engineered attacks.

The Wikipedia definition of Social Engineering is "the act of manipulating people into performing actions or divulging confidential information." We have seen it on television and read it in books and newspapers; Confidence Men work on our sense of trust to obtain information (personal and financial) or to perform destructive acts. Whether they are doing this to obtain some monetary gain or are just hoodlums, the result is the same. You or your computer system can be compromised if you are not careful.

These new attacks are showing up as news bulletins or special offers that you can't resist and when you click on the site you are either infected by the action of going to the site or tricked into running some executable code. One of the most recent attacks has come from a security attack called ANTIVIRUS2009. Sounds like something you might want to have to prevent infections but it is a program that bundles many different Viruses, Trojans, Spyware and other Malware onto your system. The first rule of thumb to protect yourself from Malware is: If you didn't ask for the information don't trust it!

How do you protect yourself?

1. Make sure that you are running all the current updates for your operating system. Your operating system manufacturer is constantly issuing new software patches to protect against recently discovered vulnerabilities. Because Microsoft Windows has such a large installation base it is the most often attacked system. Be sure to turn on your automatic updates and check your other software products for updates as well.
2. Be sure to have anti-virus software installed on your system and make sure the automatic updates switch is turned on for this as well. Make sure that your anti-virus program has the capability to scan your email and files that are downloaded from the internet. You will also want to make sure that it is capable of scanning floppy disks (if you are still using them) and USB Flash Drives when they are inserted in your machine. Make sure you schedule full system scans periodically.
3. Install a firewall on your system as well. Firewalls can be either hardware or software based, and are used to control inbound and outbound traffic to the internet and notifies you when there is an intrusion attempt on your system. The combination of a firewall and a good anti-virus program will decrease the risk considerably of your being hacked or infected with a virus.
4. Most attacks come through your email so be critical of all that you see hitting your Inbox. Remember, the

malicious code may not be in the actual email that you receive so your computer system's anti-malware applications might not catch the problem. As good as all these antivirus and anti-spyware programs are, they can't protect you from invitations from sites that host malicious code. If you accidentally invite the code to be installed, your computer is going to do what you ask it to do. Once the code is installed many of these programs are smart enough to attack the software on your system that is supposed to protect you and turn off these features or mask their destructive natures. So do not respond to unsolicited (SPAM) email.

5. Be skeptical of individuals representing themselves as officials soliciting personal information via e-mail. Please don't fall for the poor slob in Kenya who can't access the money that their recently deceased parent left them without your help. I know you are a Good Samaritan, but don't become another duped statistic. If the situation is too good to be true, it probably is.

6. Be cautious of email containing files because these files may contain viruses. Only open attachments from known senders.

7. Be sure to validate the legitimacy of the organization by directly accessing the organizations website instead of following the link provided in an email message. A classic subterfuge that is used is an email that appears to be from your bank, credit card company, or PayPal. The email has all of the logos and website links that make it appear as though you are going one of these financial institutions. If you receive an email that you think is real, go to your browser and type in the URL address for that company. Manually make the connection to see if the offer or information request is valid. Most financial institutions makes it a rule not to solicit personal information from you by email; they like the phone. I won't give my SSN over the phone unless I am the one requesting the contact. Be careful.

If you follow these simple rules you will be able to safely navigate through the turbulent waters of the Internet. Remember, with the current state of affairs around the world, we are only going to see more attempts to access our information and resources, not less. Hill Street Blues writers gave us a very well used phrase that is even more important today. So don't forget to... Be Careful Out There!

Bob has been working in the computer field since 1975 and started Computer Connections with his partner Jude Daigle in 1981 at the beginning of the personal computer revolution. Bob grew up in Ligonier and graduated from Ligonier H.S. in 1972. George Washington University is his college alma mater and he is currently living in the Greensburg area. You can see more tech tips and product reviews in Bob's Blog pages at www.bobstechtalk.com.

Most popular Antivirus Software downloads

1. AVG Anti-Virus Free Edition	2,193,618 downloads
2. Avira AntiVir Personal - Free Antivirus	707,900 downloads
3. Avast Home Edition	512,318 downloads
4. Avast Professional Edition	85,945 downloads
5. Norton AntiVirus 2009	56,004 downloads

Figure 1 - CNET Download Ranking

LIGONIER
TAVERN
A Restaurant

"too much fun for such a small town"
check upcoming events and our menu
on line at www.ligoniertavern.com

Sun. 12:00 pm to 8:00 pm
Monday -Thurs. 11:30 am - 9:00 pm
Fri. & Sat 11:30 am - 10:00 pm

724-238-4831
137 West Main Street
Ligonier, PA



No Time Like Now To Learn About Computers

Beginner basic adult computer classes will be taught at Latrobe Senior Center beginning Wednesday March 4, Thursday March 5, and Friday March 6 at 9:30 am to 11:30 am. An evening class will begin Monday, March 9 from 7:00 pm to 9:00 pm. An advanced computer class begins Tuesday, March 10 at 9:30 am to 11:30 am. Classes run for four consecutive weeks. A \$20 non-refundable donation will reserve your seat.

Scholarships are available if needed and a free computer will be given to any student who needs one. Classes are sponsored by Senior Computer Associates through (LAPA) Laurel Area Partnership of Aging. You can sign up at the Senior Center, Avenue C, Latrobe or call 724 539-9288 for more information.

D's Windy Cottage

Specialty Gift Items and Home Decor

745 Lloyd Avenue Extension
(Behind Auto Zone)

724-537-5283
Tues-Sat 10AM-6PM. Closed Sun & Mon

Framed Art, Heirloom Dolls,
Gund Bears, Soy Candles & Warmers
Kites, Spinners & Flags

We have a year-round Christmas Room!
Gift Certificates Available