

April 1, 2009 Newsletter

1. The Internet is Infected
2. Security Doesn't Have to be Expensive
3. Don't back up? You might be outta luck
4. About me and this newsletter

#####

1. The Internet is Infected

The March 29, 2009, broadcast of '60 Minutes' featured a story about the security risks that constantly threaten Internet users. One specifically, the Conficker virus, is estimated to be currently infecting 10 million computers world wide. As of the broadcast, it was still dormant and had not yet detonated its payload (i.e. delivered the intended results) but researchers are concerned that it may become active on April 1.

The piece also talked about the most common motivator for virus authors, money. Don Jackson, Director of Threat Intelligence at SecureWorks in Atlants, was interviewed and discussed a gang of Russian teenagers who steal tens of thousands of dollars a week by gaining control of computers infected with viruses they wrote. An Internet fraud victim was also interviewed, saying that she had several thousand dollars stolen from her bank account, literally right before her eyes (in a virtual way), despite her computer having antivirus and firewall protections.

But here's the footnote that CBS just only brushed on. The victim interviewed admitted that her sons had been downloading games and music from websites. There's the smoking gun. Websites that feature downloadable movies, music, games, ringtones, or anything else that appeals to teenagers or young adults, are known to be ripe with Internet STDs.

While I know the facts presented by CBS to be true, I think their presentation of them was overly dramatic and sensationalized. In addition to effective and updated antivirus software and a firewall, it is critical for a user to employ common sense when on the Internet. Without it, maintaining the computer's security is an uphill battle.

Related reading:

[http://www.cbsnews.com/stories/2009/03/27/60minutes/main4897053.shtml?](http://www.cbsnews.com/stories/2009/03/27/60minutes/main4897053.shtml?source=mostpop_story)

[source=mostpop_story](http://www.cbsnews.com/stories/2009/03/27/60minutes/main4897053.shtml?source=mostpop_story)

<http://support.microsoft.com/kb/962007>

http://www.symantec.com/norton/theme.jsp?themeid=conficker_worm

#####

2. Security Doesn't Have to be Expensive

By now, you may be wondering what you should be doing to protect yourself. Well, there's a short checklist of items that can make a big difference.

1) Dump Internet Explorer

Since July 2007, W3Schools.com says Mozilla's Firefox is the most commonly used web browser. Of course, there is no single authoritative entity to declare Firefox the most popular, but www.w3schools.com is a respected Internet resource for all things web. So why use Firefox? It is less vulnerable to Internet threats than Internet Explorer is. Many people say it's also faster and better to use. Best of all, it's free.

2) Make sure you have updated, effective antivirus software

Good antivirus protection doesn't have to be costly. Sure, Symantec/Norton and McAfee are the big dogs in this pack, but there are some others to be aware of. Grisoft's AVG is a free, easy to use and effective antivirus package. Avast is also very highly regarded.

But be careful not to trust your security to untrustworthy hands. There are malicious programs circulating the 'Net, masquerading as good guys, such as WinAntivirus 2007/2008/2009. These are tornados looking for a place to touch down.

3) Put a firewall between you and the 'Net

Firewalls come in two main forms, software and hardware. A software firewall is a program you install in an individual computer that provides protection from prowlers on the Internet, trying to creep in to your computer through an unlocked door. A hardware firewall does the same, except it is a tangible device and it protects all computers connected to it. For example, any broadband router used with high-speed Internet service, is also a firewall. Technology has advanced so speedily that routers can be had for less than \$50, and they also allow other computers in your home to share your high-speed connection.

4) Think before you click

The vast majority of computer infections are results of the user opening an unexpected email attachment, clicking a unknown link or visiting a untrusted website. I'm certainly not telling you to never do any of these things, you wouldn't make it very far down the Information Superhighway. But a suspicious eye will keep you safer.

Related reading:

http://www.w3schools.com/browsers/browsers_stats.asp

<http://www.mozilla.com/en-US/firefox/personal.html>

<http://free.avg.com>

http://www.avast.com/eng/avast_4_home.html

<http://compnetworking.about.com/od/wirelessrouters80211g/tp/80211ghome.htm>

#####

3. Don't back up? Don't push your luck

Computers have become so easy and convenient on which to store our digital lives. Pictures of the family, your budget spreadsheet that will help you to afford that awesome vacation this summer, the hours of extra work you do at home because there's not enough time at work; these are all things that are important possessions. So why do you only have one copy of them? Would you dream of only having one key to your house or your car? No, you have backups. One with the neighbor, at work, or with the folks.

Backing up your computer is just as important. I think that many people are intimidated by the concept and don't know where to begin. So they don't. But it's not as difficult as one might think. All it takes is one catastrophic event, and years of work and memories could be gone.

Your backup routine's complexity depends on your individual situation, but a typical home user can get away with backing up irreplaceable data files to an external harddrive or burning CDs/DVDs (make sure to have copies of software CDs as well). Another way is to sign up with an online backup service. Not all are created equal, but I like Mozy. Once it's set up on your computer, you don't have to do anything. It's so easy, my mom uses it! Sorry Mom. But the point is, get something in place and stick to it. It's like insurance: you have it so you'll never need it.

Related reading:

<http://www.mozy.com/?ref=3f9a896b&kbid=39462&m=5>

#####

4. About me and this newsletter

Lee Abrams is an IT professional from the Philadelphia area, and has over 8 years experience helping computer users and bringing valuable services to small businesses. People have come to rely on his experience, integrity and speedy service in a variety of situations, including computer, network and server installation and repairs (Windows and Apple OS X computers), website design and maintenance, consulting and coaching, PC disinfection

and clean-up, and general technology services.

I write this newsletter as a value-added service to my clients as a way to help keep computer users abreast of the rapidly changing landscape. Please feel free to pass this on to anyone who you may feel this will be useful, but only as a whole like the way in which you received it.

I would never lead you astray, so every website link in this newsletter has been visited by me and has been verified to be non-malicious at the time of writing.

Please note that all content within it does not carry any warranty or guarantee, neither written nor implied. However, I am happy to work with you on a customized plan of action.

If you would like to read past newsletters, please visit <http://www.digitallee.net/archives.html>

I hate spam; everyone hates spam. I hope you don't consider this email spam. I respect your privacy and your wishes, so if you wish to not receive this newsletter any more, please reply to this email and indicate so. I promise you won't receive any more.

--

Computer and technology consulting
with a personal touch
www.DigitalLee.net