

SHIELDS ALERT

SURVIVING A HACKER

HELPFUL LINKS ON THE SUBJECT posted by Cindy Buchholz, S.F.C. Editor

Article courtesy: www.myspace.com/testify2love

I would highly recommend reading this one on cyber crime, and the criminal ramifications for key logging that you need to be aware of. Don't do anything that could get you into trouble.

<http://www.crime-research.org/library/Bryan.htm>

And for those of you who have gotten emails from scammers, there is new information out there, (and the technology to support it) that will install a hidden keylogger if you open up an email and read it from someone you don't know). This is why I don't participate in forwarding emails... not even - especially the ones - that talk about God. And these Congressional Signature Pleas for help to petition even for a GOOD cause? Well... the rule of thumb here... if you see it on the internet, and it lines up with something you want to change... forgo the electronic age, and write a letter to Congress yourself. Where do you think these people get their mail lists from? And the innocent are being used to perpetuate this charade... that's what bugs me! But now you know, and you've been warned. You don't know who these people are on your mail list - and by the time you discover it? It's best, if you want to forward, to just cut and paste the body of the message you want to convey to a friend, and forget about the convenience of just pressing "forward". The price is just too high, and it only takes one mistake. Read more about this here:

<http://www.zdnet.co.uk/tsearch/scam+email.htm>

This one deals with identity theft and key logging:

http://news.zdnet.com/2100-1009_22-5954242.html

<http://www.morningstaradvisor.com/articles/doc.asp?docId=4334>

<http://www.securityfocus.com/news/8329>

Detect Key Logger, Identity Theft Spyware

To detect key logger spyware, you need to know what it is and how it works. Key logger is an invisible software program that identity thieves can use to track your online activity.

It is almost impossible to detect key logger on your computer and even if you're careful you'll never know if it is recording information such as bank account passwords and credit card numbers.

You won't even see your machine slow down or see anything unusual. It just silently watches every keystroke you type in as if the identity thieves were standing over your shoulder.

At least on third of all online scams can now be traced to keylogging. ...

For the rest of the article, click here: <http://www.articleblog.cn/946/Detect-Key-Logger-Identity-Theft-Spyware.html>

BUYER BEWARE ! Research the ENTIRE subject. This is why I placed these links here - for people who have no idea what this is, and it is for information only - NOT a recommendation of software - because it can open up the innocent to criminal liability. This is simply a comprehensive review on the subject based on my own personal experience. I know the pros AND the cons, and I am a firm believer in obtaining knowledge that could one day save your own butt. Remember, this "technology" can be used for personal good - (as in protecting your child on the internet), or corrupted for evil in the wrong hands. It all goes to motive.

This link below is the most comprehensive list I have ever seen, (with dozens of links to articles - some quite alarming - both good and bad), but it gives a clear perspective on the age in which we live... how our innocence can be taken advantage of and lead to destruction of our lives as we know it. My suggestion is to educate yourself, STAY informed, and exercise extreme caution. Shocking to know what's out there, so be careful !

<http://legalminds.lp.findlaw.com/list/cyberia-l/msg38238.html>

I realize I've bombarded you with resources, but they are here for your reference. I would suggest you make a note of the links and archive them, should you need them in the future.

COMPUTER SECURITY: ADVICE FROM THE EXPERTS

Please follow these simple steps in order to keep your computer clean and secure: **Use an AntiVirus Software** - It is very important that your computer has an anti-virus software running on your machine. This alone can save you a lot of trouble with malware in the future.

Update your AntiVirus Software - It is imperative that you update your Antivirus software at least once a week (Even more if you wish). If you do not update your antivirus software then it will not be able to catch any of the new variants that may come out.

Use a Firewall - I can not stress how important it is that you use a Firewall on your computer. Without a firewall your computer is susceptible to being hacked and taken over. I am very serious about this. Simply using a Firewall in its default configuration can lower your risk greatly.

Visit Microsoft's Windows Update Site Frequently - It is important that you visit regularly. This will ensure your computer has always the latest security updates available installed on your computer. If there are new updates to install, install them immediately, reboot your computer, and revisit the site until there are no more critical updates.

Install Spybot - Search and Destroy - Install and download Spybot - Search and Destroy with its TeaTimer option. This will provide realtime spyware & hijacker protection on your computer alongside your virus protection. You should also scan your computer with program on a regular basis just as you would an antivirus software.

Install Ad-Aware - Install and download Ad-Aware. ou should also scan your computer with program on a regular basis just as you would an antivirus software in conjunction with Spybot.

Install SpywareBlaster - SpywareBlaster will added a large list of programs and sites into your Internet Explorer settings that will protect you from running and downloading known malicious programs.

Update all these programs regularly - Make sure you update all the programs I have listed regularly. Without regular updates you WILL NOT be protected when new malicious programs are released.

Follow this list and your potential for being infected again will reduce dramatically.

You will want to **finish cleaning now by removing your restore points and starting fresh** with them.

Please do this:

Turn off System Restore.

On the Desktop, right-click My Computer.

Click Properties.

Click the System Restore tab.

Check Turn off System Restore.

Click Apply, and then click OK.

Reboot.

Turn ON System Restore.

On the Desktop, right-click My Computer.

Click Properties.

Click the System Restore tab.

UN-Check *Turn off System Restore*.

Click Apply, and then click OK.