



Consumer Affairs Tabloid



Keeping you in the “KNOW”

287- CITY

Army Community Service Financial Readiness Branch

November 2007



Excerpt from: Federal Trade Commission

Botnets and Hackers and Spam (Oh, My!) www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt132.pdf

Hackers and spammers may be using your computer right now. They invade secretly and hide software to get access to the information on your computer, including your email program. Once on your computer, they can spy on your Internet surfing, steal your personal information, and use your computer to send spam — potentially offensive or illegal — to other computers without your knowledge.

Computers that are taken over this way often become part of a robot network, known as a “botnet” for short. A botnet, also known as a “zombie army,” usually is made up of tens or hundreds of thousands of home computers sending emails by the millions. Computer security experts estimate that most spam is sent by home computers that are controlled remotely, and that millions of these home computers are part of botnets.

Spammers can install hidden software on your computer in several ways. First, they scan the Internet to find computers that are unprotected, and then install software through those “open doors.” Spammers may send you an email with attachments, links or images which, if you click on or open them, install hidden software. Sometimes just visiting a website or downloading files may cause a “drive-by download,” which installs malicious software that could turn your computer into a “bot.” The consequences can be more than just annoying: your Internet Service Provider (ISP) may shut down your account.

Excerpt from: Onguardonline.gov

Stop – Think - Click <http://onguardonline.gov/index.html>

You can minimize the chance of an Internet mishap by adopting these practices:

1. Protect your personal information. It's valuable.
2. Know who you're dealing with.
3. Use anti-virus and anti-spyware software, as well as a firewall, and update them all regularly.
4. Make sure your operating system and Web browser are set up properly and update them regularly.
5. Protect your passwords.
6. Back up important files.
7. Learn who to contact if something goes wrong online





Excerpt from: Get NetWise
www.ftc.gov/bcp/edu/pubs/consumer/homes/rea04.shtm

File-sharing Tips

The best tip for file-sharing is to stop and think before downloading files through these networks. It's best to keep your and your kids' file-sharing safe, secure and legal. Here are more tips:

- **Don't download files from people you don't trust** -- Just like you shouldn't open e-mail attachments from people you don't trust, you should be wary about downloading files from them as well.
- **Keep your file-sharing legal** -- Downloading copyrighted music, movies and software using these file-sharing programs without the copyright owner's permission could put you in serious legal trouble. Peer-to-peer users should be aware that they may not be anonymous while using these networks. Copyright holders have located peer-to-peer copyright infringers and have sued them. There are a growing number of online music and movie services where you can stream, download or purchase digital files with the copyright owners' permission. Using these services is one way to ensure that you will avoid unwanted lawsuits.
- **Watch out for spy-ware** -- Some file-sharing programs embed spy-ware programs when you install them on your computer. These programs can run in the background and create unwanted pop-up advertisements and some even monitor your online behavior.
- **Use and update your anti-virus software** -- Computer experts are starting to see viruses being spread through file-sharing networks. Be careful what you download and always make sure your anti-virus software is running and frequently updated.
- **Secure your sensitive computer information** -- If you keep sensitive information on your computer like your tax return information and online bank account data, check to make sure that you are not inadvertently making this available to thousands of strangers on the Internet.
- **Parents, talk to your kids** -- Parents should be aware that file-sharing networks contain inappropriate audio and video clips -- many of a sexually explicit nature.



From the Files of Fort Hood's Consumer Affairs Office

After a hard day at work one of the first things I do is check my email on my home computer. Well that is after I feed the cats, prepare supper, clean up, etc. A couple of hours later I'm finally ready to relax and check my inbox. Yes! I have 10 new messages. How irritating, it turns out to be just a bunch of junk mail and spam. I guess I need to reread the above articles in this Tabloid and follow my own advice.

The next step is to report the spam by forwarding it to spam@uce.gov which is part of the Federal Trade Commission. Any Phishing mails should be sent to reportphishing@antiphishing.org. The Anti-Phishing Working Group, a consortium of ISPs, security vendors, financial institutions and law enforcement agencies, uses these reports to fight phishing. For more information about phishing go to www.phishinginfo.org;

Another tip - I will set up a separate email address to use when making online transactions. Such as: booking reservations for airline tickets; Christmas shopping over the internet; or when signing up for an online newsletter. This will cut back on the amount of junk mail my main account will receive.

Back issues of the Consumer Affairs Tabloid are available on the Financial Readiness section of the ACS website at www.hoodmwr.com/acs.

Have questions? Contact: melody.squires@us.army.mil 287-CITY (2489)