

Kathleen Advocates Cyber-Terrorism

Source: <http://sci.tech-archive.net/Archive/sci.med.diseases.lyme/2005-07/msg01594.html>

- *From:* "lisasawitch" <lisasawitch@xxxxxxxxxx>
 - *Date:* 26 Jul 2005 15:09:02 -0700
-

Sent to me from kathleen's spinlyme group!

This is a federal crime. A SERIOUS Federal Crime. So do what you think is right! By the way this is almost certainly a violation of her probation/parole.

Remember, she's provided everyone with contact information for the FBI in New Haven: FBI New Haven 203-777-6311

FBI Tips and Public Leads

<https://tips.fbi.gov/>

While the FBI continues to encourage the public to submit information regarding the September 11, 2001, terrorist attacks, this form may also be used to report any suspected criminal activity to the FBI.

FBI Tips and Public Leads

Your First Name

Your Middle Name

Your Last Name

Your Phone

Your Email

Your Street 1

Your Street 2

Your Suite/Apt/Mail Stop

Your City

Kathleen Advocates Cyber-Terrorism

Your State

Your Country

Your Zip Code / Route

Please describe your information:

17607 From: Kathleen <janmusinski@...>
Date: Sun Jul 24, 2005 9:35am
Subject: Countering "counterterrorism"
kmdickson0308
Offline
Send Email

Here's an interesting thought.

If the USDOJ dot gov is in collusion (US Attorney Kevin O'Connor and John G. Rowland) with the NeoCons who believe in belligerence and pre-emptive "Defence," and the USDOJ believes that it is proper to defend the Yale criminals by inventing other people's crimes and slamming them away forever for saying they are innocent, (which was part of the entire plan), then everyone opposed to such abuses of power can become a "terrorist" and jam the DOJ/FBI's email searches with keywords like:

Unibomber
chemist
ammonium nitrate
subversive
bomb
Yale
command
operation
mail

Create several email addresses. Give all of them 950 Pennsylvania Ave NW 20530 as your address.

or, 157 Church Street, New Haven, 06510

I was falsely accused of being "a dangerously intelligent chemist," "like Ted Kaszinski," who

has "command hallucinations to kill."

This was invented for me at my DCF "trial."

Then I was criminally charged with that, and not allowed access to the courts, since a Yale "psychiatrist" determined I was insane to be saying I was innocent.

Tough to figure out.

Silicon Spooks: Government Spying on the Internet

– By Shawn Ewald ©, 2002 (repost here in August, 2004)

NSA's Echelon Surveillance Network In a new novel, *Digital Fortress* by Dan Brown, the National Security Agency (NSA) has built a code–breaking supercomputer called TRANSLTR that can crack any cryptographic cipher in a matter of seconds. Ostensibly, the purpose of this computer is to monitor the encrypted communications of terrorist groups, but the designer of this supercomputer recognizes the danger presented to the privacy of ordinary citizens by his creation and invents an unbreakable code called Digital Fortress. He threatens that, if the NSA does not make the existence of TRANSLTR publicly known, he will distribute Digital Fortress on the Internet.

Unfortunately, only in novels, I suspect, do NSA employees have consciences, much less concern for the privacy of Jane Q. Citizen. Fortunately, only in novels does the NSA have a computer that can crack codes in seconds – even the world's most powerful supercomputer, the Intel Paragon, would take a bit longer than a few seconds to crack a message by brute force that was encrypted with PGP (Pretty Good Privacy, a freely available encryption program that runs on PCs and Macs).

However, the NSA does indeed monitor all Internet communication, just as it monitors all telephone, radio, and satellite communication, and, therefore, our collective right to privacy is routinely violated by the Government without our knowledge.

But what is different about the NSA's activity on the Internet has to do with the Internet itself and the public's understanding of it. The Internet is inherently open and insecure, which makes it incredibly easy to monitor and intercept communication traffic like e–mail messages, for instance. Furthermore, the majority of the American public is largely unaware of how insecure the Internet really is – it is interesting that, thanks largely to the mainstream media's successful manufacturing of Internet paranoia, technophobic or computer illiterate people are more conscious of this aspect of the Internet than many people who use the Internet regularly. Most people have heard about government agencies tapping phone lines or even steaming open

paper mail, but it seems that most people are not aware of the government's routine monitoring of Internet communication traffic, particularly e–mail traffic. This ignorance is dangerous for a society that has become almost wholly dependent on electronic mediums of communication.

The NSA's surveillance of Internet communication began at the early stages of the Internet's development when it was still populated only by government employees, university researchers, and government contractors. Many people involved with the early Internet (known then as ARPANet) were aware of this surveillance. In fact, Richard Stallman, an MIT computer scientist who was then involved with the ARPANet (and later would found the Free Software Foundation), added an optional feature to a text editor/e–mail client that he had created called EMACS; the purpose of this feature was to undermine the NSA's surveillance efforts. The optional feature added randomly selected keywords at the end of an e–mail message composed in EMACS; these keywords (i.e. revolution, terrorist, etc.) he believed would trigger interception by the NSA computers and, hopefully, if enough people made use of this feature, clog the NSA's computers with irrelevant e–mail.

In former New Zealand intelligence agent Nicky Hager's book *Secret Power*, one discovers that the NSA's surveillance capabilities are not hindered by political borders. Under the code–name ECHELON, and with the help of the British, Australian, New Zealand and Canadian Governments, the NSA has established a global communication surveillance network that is capable of monitoring most of the world's electronic communication.

The ECHELON system was created by the NSA as a means to interconnect surveillance systems that had existed in these countries since WWII, and to put these foreign surveillance operations under the control of the NSA. What ECHELON became was an international network of computer systems, each intercepting all fax, telex, e–mail and satellite communications in their region of the world. The intercepted communications are scanned with "dictionary" programs for certain keywords; these dictionaries not only contain keywords of interest to the intercepting agency, but also keywords that are of interest to the other intelligence agencies around the world involved in the ECHELON network. If the intercepted message contains a matching keyword, it is immediately passed on to the headquarters of the agency concerned.

Given this massive technological arsenal, how can citizens protect their privacy on the Internet? There is one method that has proven to be an effective monkey wrench in the Government's efficient surveillance machine, and that is strong encryption. Despite the claims of fiction writers, there is no such thing as an unbreakable code or uncrackable encryption, but what good encryption can ensure is that if someone wants to snoop on your e–mail communications they are going to have to put a good deal of effort into it. Cracking encrypted electronic communications is the labor–intensive equivalent of steaming

Kathleen Advocates Cyber-Terrorism

open envelopes, whereas intercepting and reading unencrypted mail is as easy as reading the back of a postcard. Not surprisingly, the FBI and NSA have asked Congress to outlaw strong encryption. We as citizens should be fighting their efforts every step of the way.

In the documentation for PGP, the program's author, Phil Zimmermann, poses the following to users who may be skeptical about the need for publicly available strong encryption programs:

â??Perhaps you think your E-mail is legitimate enough that encryption is unwarranted. If you really are a law-abiding citizen with nothing to hide, then why don't you always send your paper mail on postcards? Why not submit to drug testing on demand? Why require a warrant for police searches of your house? Are you trying to hide something? You must be a subversive or a drug dealer if you hide your mail inside envelopes. Or maybe a paranoid nut. Do law-abiding citizens have any need to encrypt their E-mail?â??

The answer is obvious, of course they do. In the next issue I'll demonstrate how to use PGP (still the best personal encryption software, and it's free) as well as demonstrate other ways one can enhance one's privacy and security on the Internet.
Silicon Spooks Part 2: Personal Security on the Internet

Last month, I described how the government routinely snoops on our electronic communications and violates our right to privacy.

However, for most people, the government is the least of our troubles when it comes to protecting our privacy when we use computers and the Internet. Other common snoops are our bosses in our workplaces, commercial Internet sites, and criminals. And of those three threats to our privacy, our bosses and commercial Internet sites are the most common threats. In this short article,

I'll try to give some tips on how to protect yourself.

But first, as promised in my last article, here is a brief tutorial on how to obtain and use PGP. I'm going to concentrate on the PC version of PGP because 1) it requires more explanation, 2) it is in much wider use than the Mac version, and 3) the Mac version is easier to use and understand.

What is PGP?

PGP is powerful encryption software. Meaning, it is a piece of software that enables you to encrypt your data (typically documents and e-mail messages).

Where to get PGP?

There really are only two places you can get it. The first is PGP Inc., and the second is at MIT – I recommend the MIT distribution site.
Which version you should get?

There are two commonly used versions of PGP available, PGP 2.6.2 and PGP 5.0. I recommend PGP 2.6.2.

PGP 5.0 is newer and easier to use, but unfortunately it uses an entirely new (though not necessarily better) system for encrypting your data that is not compatible with older versions of PGP. PGP 2.6.2 has a steeper learning curve in terms of usability but it is, hands down, the most widely used version of PGP in the U.S. and, therefore, will enable you to exchange encrypted messages with a much wider number of PGP users.

How to use PGP

Once you've downloaded and installed PGP the first thing you need to do is generate what's called a PGP "key pair". (Installing PGP 2.6.2 is relatively straightforward for people who are moderately familiar with their computer. Print out the setup.doc file in the PGP distribution and follow the instructions for your operating system.)

To generate your PGP key pair, issue the following command at a DOS prompt: `pgp -kg`

After you issue this command, PGP will ask you a few questions and require you to do a few things to generate your key pair. The first thing it will ask is what level of encryption you wish to use – you'll be offered three choices:

1. 512 bits– Low commercial grade, fast but less secure
2. 768 bits– High commercial grade, medium speed, good security
3. 1024 bits– "Military" grade, slow, highest security

I recommend choosing option 3 "Military" grade encryption.

The next three things you'll be asked will be 1) choose a user ID 2) choose a passphrase and 3) entering random keystrokes to generate your key pair.

Your user ID should be your full name and e-mail address, for example:

Shawn Ewald shawn@...

Your passphrase can be as long as you like – it should literally be a phrase or sentence or a long string of characters – just make sure you can remember it. Next, you will be asked to type random keystrokes – this helps PGP generate a truly random key pair. When prompted to do this, just hit random keys at random intervals until PGP tells you to stop.

Now PGP will generate a key pair that will be stored in two files: `secring.pgp` and `pubring.pgp`. The first file `secring.pgp` contains your PGP secret key, it is very important that you never let anyone see this

Kathleen Advocates Cyber-Terrorism

file, it is also very important that you make a backup copy of this file on a floppy disk and store it in a safe place. The second file `pubring.pgp` contains your PGP public key, this key can be freely distributed once you have extracted it from `pubring.pgp`. To extract your public key from your public key ring (`pubring.pgp`) issue the following command at a dos prompt:

```
pgp -kx Shawn shawn pubring.pgp
```

NOTE: replace Shawn and shawn with the beginning of your own user name.

In this case, PGP will store my public key in a file called "shawn.asc"; I can open this file with any text editor to view it. Once you've extracted your public key, you can send it to friends so that they can use their copy of PGP to send you encrypted messages. You can even make it available to strangers by putting it on your web page. I, for example, have made my PGP public key available on the web at:

<http://www.radio4all.org/pgp/>

How to encrypt and decrypt files

To encrypt a file, issue the following command at a DOS prompt:

```
pgp -es textfile -u your_userid
```

To decrypt a file, issue the following command:

```
pgp encrypted_file -o filename
```

NOTE: replace the words "textfile" and "encrypted_file" with the actual names of the files you wish to encrypt/decrypt, replace "your_userid" with your actual user ID, and replace "filename" with the name your wish to call the decrypted file.

In both of the above examples PGP will ask you to enter your passphrase. If your passphrase is correct it will immediately go to work.

Add-ons for PGP

Obviously, typing commands at a DOS prompt is not an enjoyable experience for most people. Fortunately, there are many add-ons (mostly for e-mail programs) available for free on the Internet that provide a nice graphical interface and make PGP much easier to use. The best place to look for these add-ons is at the yahoo PGP directory. Go here and select the "PGP - Pretty Good Privacy" link.

Other features of PGP

There are many other features to PGP that I'm unable to describe in such a brief article. So, I strongly suggest that you print out and read the file "pgpdoc1.txt" that comes with the PGP distribution.

Other personal security measures you can take

Kathleen Advocates Cyber-Terrorism

In addition to learning about and using encryption software like PGP, there are other aspects to using the Internet where your personal security can be improved. The following is a list of simple things you can do to protect yourself when using the internet.

1.
Avoid making credit card purchases on-line

Despite the hype, secure online transactions are not nearly as secure as many businesses would like you to believe. Furthermore, it is not likely that online transactions will ever be as secure as real world transactions. Be aware that you are taking a risk whenever you submit your credit card number online.

2.
Scan downloaded files for viruses before opening them

This is a no-brainer, but it can't be repeated enough. Get a good virus program (like McAfee Anti-virus, IBM Anti-Virus, or Dr. Solomon's Anti-Virus) and scan the files you download before opening them.

3.
Never give out your password

No one needs to know your password, except you; never give it out. If you are signing up for a service on the web that requires a password, make a new and unique password for that service, never use your ISP password for any service on the Internet.

4.
Disable the "cookies" feature in your web browser

This can be done in most modern browsers. For example, to disable cookies in Netscape Communicator:

Click the Edit menu, then select "Preferences." In the Preferences Dialog box, select the "Advanced" category. In the "Cookies" section select "Disable Cookies". Then click the "OK" button.

Happy surfing!
Suggested Reading and Websites:

- * Secret Power: New Zealand's Role in the International Spy Network, by Nicky Hager
- * The Puzzle Palace: A Report on America's Most Secret Agency, by James Bamford; Viking
- * The Crypt Newsletter
- * Secrecy & Government Bulletin
- * PGP: Pretty Good Privacy, by Simson Garfinkel; O'Reilly & Associates
- * Bandits on the Information Superhighway, by Daniel J. Barrett; O'Reilly & Associates

CSS printer friendly enabled
mail to a friend Send this to

- *Follow-Ups:*
 - ◆ *Re: Kathleen Advocates Cyber-Terrorism*
 - ◇ *From:* Chuck
 - ◆ *Re: Kathleen Advocates Cyber-Terrorism*
 - ◇ *From:* derdrittemann2003
- Prev by Date: *Re: Mad. Angry. Elisa test!*
- Next by Date: *JillF you are right!*
- Previous by thread: *A National Security Risk*
- Next by thread: *Re: Kathleen Advocates Cyber-Terrorism*
- Index(es):
 - ◆ *Date*
 - ◆ *Thread*