

Protecting Consumers from Themselves



Presented by the State Information Security
Office & the California Office of Privacy
Protection

September 13, 2007

Keylogging – What is it?

- **Keystroke logging** or **keylogging** records the real time activity of a computer user, including the keys they press.
- Software is readily available on the Internet and free
- It can be used by malicious individuals to obtain passwords, encryption keys, and other personally identifiable information.

How does a user get this software on his PC?

- Keylogging software can be distributed via a trojan horse or a virus.
- It can be either hardware or software. Most common is software.
- Typically, a vulnerable user's PC is not kept up-to-date with fixes, patches, and anti-spyware/anti-virus signatures.

How do users avoid getting it on their PCs?

- Monitor the programs running on PCs.
- Use anti-spyware/anti-virus programs and keep the signatures updated.
- Use a firewall to help prevent transmission of logged material over the Internet.
- Use network monitors to alert them whenever an application attempts to make a network connection.

What's the issue for State government?

- Users, who unknowingly have keylogging software installed on their PCs, access State online applications.
- They enter their PII, such as name, SSN, DL#, home address, password, on the entry screen.
- All keystrokes are captured by keylogging software and obtained by hacker.
- The hacker can now use this PII for identity theft, fraud, and other criminal activities.

How did the SISO determine this was occurring?

- SISO was notified by US-CERT in September 06
 - SISO has continued to receive numerous logs from them.
 - Logs are difficult to decipher, info is layered in a deep multi-folder structure.
 - Spreadsheets were created to capture the information.
- CHP investigated it
 - Determined it to be keylogging events on user PCs (several hundred events).
 - Some anomalies, but majority involved consumers.

Why can't law enforcement capture the bad guys?

- It is almost impossible to capture pertinent evidence, since we do not have access to the consumer's PC.
- Limited investigative information is provided in the logs given by US-CERT.
- Some indication that the hackers are out of the country.

Should we notify affected individuals?

- The State has done nothing to cause the problem.
- Hard to identify individuals found in the logs (very labor intensive).
- It would be an ongoing, never-ending effort.

Therefore, we will not attempt to contact individuals.

What can State government do to protect consumers?

- Establish a “computer security center” Web page for consumers that will provide them important guidance on protecting their home computers.
- Require all State Web-based applications to place a link to the “computer security center” on every initial entry Web page where consumer PII is collected.
- May want to consider requiring it for systems that employees access remotely, too.



Welcome to the General Online Complaint Form

The Department of Consumer Affairs is here to help Californians be careful consumers and to protect them from unscrupulous and unqualified individuals.

- I NEED TO:**
- > [Verify a License](#)
 - > [Search for Forms and Publications](#)
 - > [File a Complaint](#)
 - > [Sign-up for Consumer Updates](#)
 - > [Renew My License Online](#)

[Please read the Information Collection, Use and Access notice below.](#)

Business / Professional You Want To File A Complaint Against:

Fields marked with an asterisk (*) are required.

Business / Professional Name:*

License Number:

Address (Number and Street):*

City:*

State:*

Zip:*

Telephone Number: () -

Person whom you dealt with:

Business / Professional E-mail Address:

Please briefly describe your complaint.*





If the computer you're using now is not protected, identity thieves and other fraudsters may be able to get access and steal your personal information.

Tips from the California Office of Privacy Protection

By using safety measures and good practices to protect your home computer, you can protect your privacy and your family. The following tips are offered to help you lower your risk while you're online.

■ **Install a firewall.**

A firewall is a software program or piece of hardware that blocks hackers from entering and using your computer. Hackers search the Internet the way some telemarketers automatically dial random phone numbers. They send out pings (calls) to thousands of computers and wait for responses. Firewalls prevent your computer from responding to these random calls. A firewall blocks communications to and from sources you don't permit. This is especially important if you have a high-speed Internet connection, like DSL or cable.

Some operating systems have built-in firewalls that may be shipped in the "off" mode.

Next Steps

- Inform ISOs, Webmasters, & IT Council of computer security center.
 - www.privacy.ca.gov/state_gov/secure_computing.html
 - Graphic link button available on State Government page of www.privacy.ca.gov
- Require State agencies to place a link to the computer security center on any Web page collecting PII.
 - Consider also requiring link on any employee online system that is accessed remotely.

Resources

- <http://en.wikipedia.org/wiki/Keylogging>
- <http://compnetworking.about.com/od/networksecurityprivacy/g/keylogger.htm>
- www.chp.ca.gov
- http://www.privacy.ca.gov/state_gov/
- www.infosecurity.ca.gov