You have been Keylogged!

- ***Someone has access to your accounts?***

Jan invested in a new software that allowed her to access her clients' records from any computer, anywhere. As a matter of fact, the ability to login from any device was the deciding feature in selecting her software- the flexibility to work from home, vacation or while at conference. Several months later, and much to her disbelief, someone has been accessing her client records, without her knowledge.

How could this be possible? Jan has never shared her login credentials with anyone.

This scenario is not only possible but occurs more frequently than most people are aware of. Jan may have unknowingly shared her login credentials at a conference when she used the hotel's computer to access her PMS system. Jan may have been 'Keylogged".

What is a Keylogger?

A software-based **Keylogger** records the activities of the computer it is installed on, including each keystroke, all in real time. It records what was typed, when it was typed, what program it was typed in, including email and messaging programs. The more sophisticated **Keyloggers** may also copy and transmit screenshots to a remote computer or web server, or allow remote access to data stored locally. Some programs work in a hidden mode making itself invisible to the average user (hardware based Keylogger are not discussed here).

Keyloggers are used in many applications, some good and others not good. A few examples include:

- Parents install and use Keyloggers to monitor their children's use of computers and the internet.
- IT organizations use Keyloggers for technical support.
- Research organizations use Keyloggers in research studies.
- Companies use Keyloggers to monitor their employees.
- People use Keyloggers to monitor the activities of love ones, close associates, persons of interest, etc.
- Malicious individuals use Keyloggers to steal information - credit cards, bank accounts and passwords, etc.

It is not surprising that security experts consider Keylogging as one of the most dangerous computer threats. It allows cyber criminals to capture and receive private and confidential information without the knowledge of the user for weeks, months or even years.

How can you be Keylogged?

1. If you use a public, semi-public or another person's computer that has a Keylogger program installed. Keyloggers works the same for remote desktop or log-in programs. Experts believe public and semi-public computers account for the lion share of Keylogging.
2. Someone with access to your computer could install a Keylogger on your computer, in an effort to track you.
3. Keyloggers are sometimes bundled with a malware (virus), which installs itself on your computer after you have clicked on it, for instance.

What proactive steps can you take?

1. Change your password frequently.
2. Do not use public, semi-public or another person's computer to log into your programs.
3. Password protect your computer. Avoid sharing your computer with others.
4. Avoid logging in as an Administrator for everyday usage. Setup a user account to do so.

5. Install and maintain an updated Anti-Keylogger on your computer. Implement and maintain a good computer security policy.
6. Be wary of any software (including PMS and Remote Desktop software) that allows you to login from any computer. Logging in from any computer is a disaster waiting to happen. A proactive approach is to block access from any unregistered computers.

Checking your computer for a Keylogger

The best way to check your computer for a Keylogger is to download and run an anti-Keylogger program, much like your antivirus program. You can also do a quick check without installing a program.

1. Press *Ctrl+Alt+Delete* on your keyboard
2. Click the *Task Manager*
3. Click on *Processes*
4. Scroll all the way down to *winlogon.exe*. If you see two instances of winlogon.exe, you have been Keylogged. Don't delete any of these files until you are absolutely sure which of the two the Keylogger program is.

Why is this important in Healthcare?

In the context of a Health Care Facility (HCF) or a Health Custodian, such infringement could be tantamount to a breach of Personal Health Information (PHI). Even worse, you could potentially wake up one day and find your clients' information posted on social media. A breach of this magnitude could destroy your credibility as a business or therapist.

I note that the above examples are extreme cases. Nonetheless, I am guided by the approach advocated by the Privacy Commissioner of Ontario, Dr. Ann Cavoukian, who promotes *"Privacy by Design"*, a proactive approach to PHI protection. "A few preventative steps can save a lifetime of headaches."

Logging in from any device and from any locations are nice to have. However, security considerations are must haves.

About the Author

Danny Doobay has been a Business and IT consultant to industry and government for more than 25 years. He has held executive positions in both public and private sectors. He has also project managed software development, implementation and data migration.

He is currently the CEO of Baylaan Technologies, a software solutions developer based in Markham, Ontario. Baylaan develops both custom and packaged software solutions for several sectors, including the increasingly popular SkeduleX Practice and Case Management System.

Danny Doobay, MBA
Chief Executive Officer
Baylaan Technologies Inc.
Tel: 905-202-4716
Email: ddoobay@baylaan.com
http://www.baylaan.com/

Follow Danny on: