July 4, 2014 Release # 273

-- Begin Transmission --

KEYLOGGING

Keylogging is the process of secretly recording keystrokes by an unauthorized third party.

Keylogging is often used by malware to steal user names, passwords, credit card details and other sensitive data.

Key logging definition

A method used to capture personal information. It activates itself when selecting a link to a website or opening an attachment that secretly installs software on your computer. Once installed, it records everything you type, including any User IDs, Passwords and account or personal information. Thieves know how to retrieve this information, or even set it up to automatically have it sent back to them.

How to prevent Keylogging Attacks

✓Be careful when using the Internet. Do not click on unknown website links, advertisement, and banners.

✓Do not open attachments from unknown email senders. If you got one, forward it immediately to Information Security Department for checking.

✓Make sure your anti-virus software is always updated.

For comments or inquiries email infosec@pjlhuillier.com

-- End of Transmission --

Information Security: It's a Shared Responsibility

REFERENCES:

- Sophos Ltd. (2012). Threatsaurus: The A-Z of computer and data security threats.
- http://www.security4web.org/glossary.php?w=Key%20logging
- http://www.bankinfosecurity.com/how-to-beat-keyloggers-a-2999/op-1
- http://billmullins.wordpress.com
- blog.kaspersky.com
- http://moneebjunior.com/category/techandit/