**due Sep 23 at 11:30pm**

Discussion A - Graded - Due Sunday

55 unread replies.55 replies.

Keyboard Monitoring - Privacy Risk?

Research and then post your ideas on the following topic:

Should keyboard monitoring software ever be used? If so, when? You are also responsible to respond to another classmate's posting.

You must follow the Rubric ~

Rubric:

5 - 4pts ~ Discussion posting was the student's original thought based on research and consisting of two to three well developed paragraphs. Student used correct grammar and spelling. The student thoroughly addressed the discussion question; including giving references to backup ideas on the subject matter.  Student responded to another classmates' posting comprised of substantive, which means they responded thoughtfully, adding ideas and extending the conversations.

3 - 2pts ~ Discussion posting was not well thought-out and were only a few sentences. Spelling and grammar errors. Did not include ideas around the reading material or other research on the discussion topic. No references were used to support ideas. Student did not respond to another student's posting thoughtfully - did not post thoughts and ideas on what student posted. *If you agree with the posting indicated why.*

1 - 0pts ~ Discussion posting was not complete: no references were used to back up ideas, grammar and spelling errors, only a few sentences that did not address the discussion topic. Did not respond to another student's posting.

Keyboard monitoring software is a type of computer program which keeps a log of all key presses. The logs can later be accessed, generally by password, and read. The program normally runs in the background, invisible to the user, and ofttimes invisible to anti-virus software! (see Reference 2) The ethical use of this tool is debatable, the primary concern being privacy risk. Despite this and other risks, keyboard monitoring software could, and possibly should, be used in a minority of situations.

Consider the following example: a hospital uses a computer in the X-ray room to adjust the X-ray machine's parameters, such as the wavelength. The computer is loaded with a keyboard monitoring program. The staff is made aware of this fact, and that the computer should only be used for operating the machine. The staff should never access email or use the computer for personal matters. The monitoring program provides a way to guard against improper use of the X-ray machine, providing a log of the operator's proper or improper key strokes. If the machine isn't working properly, the hospital can provide their key logs to the developers to help troubleshoot the issue.

Considering the ethics, there's a distinction between "could" and "should." Keyboard monitoring software could be installed on any computer if it is done with the owner's permission, and if everyone who is licensed to use that computer is made aware of that fact. The topic of "should" extends to a much larger debate. I personally don't believe that public and general office-work related computers should be monitored. Not only is privacy infringed upon, but the keyboard monitor log may provide malicious attackers with sensitive information.

Reference Sources:  
1. https://searchsecurity.techtarget.com/definition/keylogger  
2. <https://www.elitekeyloggers.com/elite-keystroke-recorder-info>

Moses,

Thanks for posting your ideas. A few remarks concerning your statement: “It should be used when you’re working for a company and using their computers...”

I work in a typical office which places its employees into cubicles. My cubicle, though simple, is my own personal space. The company owns the chair I sit on, the desk on which I organize materials, and the computer stationed there. Besides an occasional technician, I am the sole user of the computer. During my down-time I like to visit my favorite sites, check my email, listen to YouTube music, etc.

My company has the authority to install a keyboard monitoring program onto my work computer. If done so, I would at minimum expect to be notified of this fact. While I would probably feel infringed upon, I ultimately recognize that the company owns the computer and is not taking away my personal freedom. I can continue to check my email and risk my personal information, I can start using my phone to check my emails instead, or I can simply refuse to use the computer and possibly quit my job.

With that said, I would alter your statement to use the word “could” instead of “should.” I personally feel that if keyboard monitoring software was used at my workplace that there would be a general upset among all the employees, overall hurting the business. I believe most offices would follow suit.

