CYBERSECURITY COMMUNICATION
Please circulate

May 23, 2017

To: University Cybersecurity Communication Recipients
From: University Systems
RE: Hardware Keyloggers

In the past year, a number of universities across Canada have been targeted by USB key-logging devices. Keystroke-loggers are designed to capture keyboard inputs typed into a computer and are designed to capture usernames and passphrases. Carleton University recently discovered a number of these devices present on shared workstations in their classrooms. More information on this attack can be found in the following article on thestar.com:

https://www.thestar.com/news/canada/2017/03/28/potential-hacking-devices-found-on-carleton-university-computers.html

In University Systems, we inspect the computers in our shared computing facilities each day as part of our closing routine for suspicious USB devices. If you have workstations in your department that are in public spaces, we recommend routinely inspecting these computers for key-loggers or other suspicious hardware devices.

If you have any questions about these issues or recommendations, please reply to this message.

Regards,

Marcus

Marcus Greenshields
Cybersecurity Working Group
University Systems
University of Victoria

University of Victoria

To verify the authenticity of this message, visit:
www.uvic.ca/systems/verify