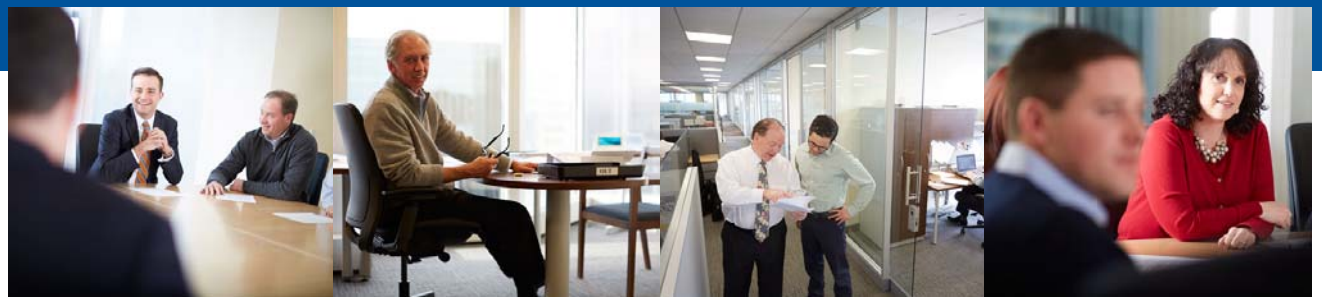
SCHNEIDER DOWNS

INFORMATION SECURITY RISK ADVISORY SERVICES

NEW WIRELESS KEYBOARD RISKS EXPOSED



7/28/2016

Big Thinking. Personal Focus.

Schneider Downs Information Security Risk Advisory Services

In July, security researchers published a new hacking technique that has allowed Hackers to take control - and more importantly - monitor certain types of wireless keyboards. New Hackware, dubbed "*KeySniffer,*"has demonstrated the ability to monitor non-Bluetooth wireless keyboards from as far away as 100 yards (all dependent on location/building/environment) when paired with a computer radio receiver. Here is a list of some of the vulnerable keyboards: http://www.keysniffer.net/affected-devices/

Schneider Downs Information Security Risk Advisory Services

Schneider Downs recommendations:

- Do not utilize non-Bluetooth wireless computer devices in business sensitive areas
- When utilizing Bluetooth devices insure that encryption setting is turned on
- Train employees to routinely sweep (look around) office area for unfamiliar electronic devices and unplug any suspicious devices then alert security. (Reference FBI Key Sweeper Advisory: https://info.publicintelligence.net/FBI-KeySweeper.pdf