Doctors Technology Office (DTO): Technical Bulletin

Log into Your Computer as a USER - ONLY

DTO TB - #17-005	**Objective:** To help clinics protect themselves from malware (ransomware) attack by preventing anyone from logging in - with full administrator rights.

Brief Description:

One major security vulnerability malware exploits in clinics, with ease, is the fact that most users log in with full administrator rights. Although it is a lot easier to setup and install a new computer system with admin rights, granting all users admin rights ultimately results in greater security risks as well as more unstable computers.

No one should log into their computer with local admin rights under any circumstances.

Potential Impact:

Although damage can occur even without administrator rights, it's generally halted by quality anti-malware, or confined to a single computer. The impact may be severe, but the scope of the damage is contained.

How does infection happen? (When users have full administration rights.)

- While reading email or browsing the Internet, it's very easy for an applet (Flash, JPEG or PDF attachment) to execute and instantly take over the entire computer.
- Users have a tendency to click the OK button, just to continue, and inadvertently install malware.
- Pretend to be a desirable "something", especially a video and claim that a plug-in is needed in order for it to work and users will do anything to bypass security.

More sophisticated malware such as ransomware has taken this to the next level.

What can it do? (When the malware has full administrator control.)

- It can embed so deeply into your system as to make removal virtually impossible, and the system more vulnerable to subsequence attack, reinfection.
- It can control all aspects of information and permission parameters such as files, folders, registry keys.
- It can remove your anti-malware security, rendering it useless.
- It can install keyloggers and remote-access into your network environment.

Author: Patrick Wong

Original Date Created: 2017-10-20

- This will render all userID and passwords, no matter how complex, useless.

In other words, game over.

Note that any decently advanced malware can hide and won't make its presence known while stealing intellectual property.

Solutions to reduce impact:

The solution is relatively easy. Create Least-privileged User accounts (LUA) to be used for each computer system in your clinic.

The same way this method reduces malware attack, such as ransomware automatically installing onto your system and proceeding to attack other systems on your network, is the same way this may impact the occasions when new software and hardware installation are required.

- For clinics where knowing the actual administrator userID and password is not a problem, let the user know.
  - This would allow users control of known software installation with the least efforts.
- For clinics where centralized control is preferred, have the clinic manager or the clinic's security lead assist with any modifications to any computers.

Either method, ensure everyone actually logs in as a "User" rather than as an "Administrator".

Background:

In general, security is based on the principle of least privilege also known as the principle of minimal privilege. In other words, you cannot do "IT" unless you "need" it. Least-privileged user accounts (LUA) are created and given to users to minimize security exposures. Vulnerabilities in one application cannot be used to exploit the rest of the computer; thus, isolating the issue. In addition to better security risk management, clinics that have deployed LUA will experience more stable systems.

Figures from 2013 and 2014 show respectively that 92% of critical vulnerability and 97% of a critical vulnerability in Microsoft software could have been mitigated if users did not have admin rights.

Please do not attempt this on your own, but rather work with your local IT support vendor.

If you have any questions or would like more information contact:

Doctors Technology Office, 604-638-5841, dtotechsupport@doctorsofbc.ca