Doctors Technology Office: Technical Bulletin

DTO TB - **#15-001**	Recommended Action re: **Malware/ Virus Security Risks**

Brief Description (Non-Technical):

Over the past year, we have been seeing sporadic, but increasing reports around privacy and security risks within the healthcare IT environment. We want to provide some timely practical advice for physicians to manage these risks, especially as it relates to malware risks.

- Some examples of "Malware" -malicious software- are viruses, worms, Trojans, spyware, adware and rootkits.
- Some examples of attacks are "phishing" for patient data and ransomware.

Potential Impact:
Performance degradations and files being locked are only inconveniences, when compared to violations and abuse that can result from PII (Personally Identifiable Information) plus medical records being exposed.

We used to think of a hacker being a lone tech nerd in the basement creating viruses to expose vulnerabilities of software programs. They are now large and organized as the focus has shifted from attacks to making huge profits by stealing PII.

- Personal information for creating credit cards is sold for about $1.00 each.
- PII (name, address, date-of-birth, healthcare information) street values are from $250 to as high as $500 in the US.

Solution
Best practice for IT security depends on the sensitivity of the data and the individual situation; solutions should be scalable to keep up with the ever changing technology. Each physician must determine the applicability of their solutions as they apply to their unique practice.

Doctors of BC has produced a Physician Office IT Security Guide for use by physicians as a general guide but *it is strongly recommended that you retain a knowledgeable and qualified IT professional to assess and maintain your network on a regular basis.* The Canadian Medical Protective Association (CMPA) supports the advice and recommendations contained in this guide and encourages it's consideration by BC's physicians.

Taking appropriate security measures will help ensure doctors derive the benefits technology offers, while protecting patient information and minimizing risk.

Background

The amount of money PII records command on the underground market has drawn large unwanted organized interests. Unlike credit card theft or bank account breaches where victims can cancel their cards or change their bank accounts, personal information with medical records such as diagnostics and prescriptions cannot be changed. In other words, PII with health records has broad utility, thus open to multiple attacks.

Recent examples include:

Author: Ralph Buschner, Daniel Kirkpatrick, Patrick Wong *Original Date Created: 2015-11-18*

- In a recent report by Raytheon/Websense Security Labs, they indicated that the healthcare industry sees 340 percent more security incidents and attacks than the average industry and is more than 200 percent more likely to encounter data theft.
- A PC World article about a ransomware scheme specifically targeting Danish chiropractors with emails with a subject line of "Possible new patient" and Dropbox links containing ransomware.
- Factsheet on Cyber Security and Privacy Protection in Canadian Healthcare outlined that web-borne malware attacks caused security incidents for 78% of healthcare organizations.

Details and Additional Information (Technical):

An effective and planned approach to device security (including in-office and remote access devices) can significantly reduce the risks of virus and malware infection. Some key points to consider include:

- Encryption of all confidential information on desktop or portable devices. Here are some options to consider as there are pros and cons to each:
  - Hardware encryption & Software encryption
  - Entire disk encryption vs file level encryption
- Ensure operating systems and all plug-in software (e.g. Java, Flash and other plug-ins) are up to date.
  - preferably using automatic updates
  - schedule update outside of business hours (computer should be on and not in hibernation)
- Malware detection programs. In addition to protecting the computer from harm, the software should also prevent data theft.
  - Should be up-to-date with auto update on
  - Should be upgraded. (i.e. your version of the software should be less than 2yrs old)
- All removable media devices should also be scanned for viruses and malware before being connected to the corporate system.
- Educate all users within your organization about cyber security; Increase awareness of the risks of phishing e-mails, opening attachments ,and pop-up messages
  - Instead of opening attachments within the email, safe the attachment on the hard drive, then scan for malware before opening or running.

For additional information please review the Doctors of BC Physician Office IT Security Guide

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