The Law Society of Manitoba
INCORPORATED 1877 | INCORPORÉ EN 1877

Computer Virus Pandemic

In the past two weeks, two Manitoba firms have called us at The Law Society of Manitoba to say they been hit by viruses – not Covid-19, but computer viruses, specifically a ransomware virus called MAZE.

As a result of the virus attack, they have no access to email, Word, their accounting software, or any of their backups, including cloud backups. Everything is tied up by MAZE and they have been asked to pay an enormous ransom to regain access to any of their work.

The firms are working with IT professionals and cyber insurers and still are not sure how the virus took hold. We suspect that someone clicked on a link or an attachment in an email that was infected with a virus which in turn infected the firms' entire systems. At this point, we do not know when or if they will ever regain complete access to their kidnapped data.

You are vulnerable. A ransomware virus could take over and lockdown everything a lawyer or law firm has ever created electronically - accounting software, client lists, document management systems, financial software, email, everything you ever did in Word, Excel, all the photos taken at firm events, and whatever treasures were kept on personal computers.

Ransomware viruses are often hidden in email attachments. Recently, the infected attachments appear to have been about COVID-19 including:

- Emails with a COVID-19 outbreak maps in an attachment.
- Emails inviting you to a seminar to discuss responses to COVID-19, which includes a link to register for the seminar.
- Emails claiming to be from vendors or associations about COVID-19 that include links to PDFs and Word documents.
- SMS (text) messages, indicating you need to "click here" to find out about modified firm operations.

These emails and attachments can be loaded with malware which can gain control of your remote access into firm computers and encrypt your home and work computers and anything else the malware can reach through your network.

What can **You** do to avoid infection?

- Always think before you click.
- Never click on an email or text message from anyone you don't know.
- If you receive an attachment in an email or text message you were not expecting—even if it is from someone you know—call the person at a known telephone number (not the number listed in the message) to confirm the message is legitimate.
- If you click on something you should have avoided and a box opens that asks you for your password, or to supply some information or click on a link to enable a later version of software: stop, close out, unplug the computer and immediately call your IT support!

Please be careful. Think before you click. And if you notice something suspicious going on with your computer, unplug it and call your IT support right away! Be careful and pass this warning on to staff and lawyers in your office.

Check with the person or firm who provides your IT support and ask if there are additional steps you should be taking at this time.

Hopefully, you have already purchased comprehensive cyber coverage as part of your firm's excess insurance or business policy. If not, now would be a good time to look into extending insurance on your practice to include cyber coverage. A low limits policy the Law Society arranges with CLIA provides initial/first response coverage geared to law firms experiencing a cyberattack. More information about the Law Society/CLIA policy is on the member portal. To report a claim and get some advice, email a description of the circumstances to cyberclaims@clia.ca; or call 1-833-383-1488 (toll free); If you have questions about how to report a cyber claim, you can also call Tana Christianson at The Law Society of Manitoba 204-926-2011.