



Saskatchewan  
Financial Services  
Commission

---

## Ransomware: To pay or not to pay

Picture yourself at your computer, innocently conducting your personal business when your screen displays a logo of your local police force and advises you that your computer has been used for an illegal purpose. At this point, your computer is locked and you no longer have access to any programs. Don't panic, there is a simple solution, as soon as you pay your fine you will be able to access your computer again. Should you pay your fine?

It's surprising how many people pay the fine. What is perhaps more surprising is the fact that some people, being well aware that the above scenario is a scam, still pay the fine hoping to gain access to their computer programs again, which is unfortunately not the case. It's astonishing that although the percentage of people who pay the fine is estimated at only approximately 2.9% of those who are targeted by this scam, the scammers are profiting at least \$5 million dollars a year.

This type of scam is called Ransomware. It has evolved from the Microsoft anti-virus scam and was first detected in Russia in 2009. Canada and the USA started seeing this in the third quarter of 2012. It is a type of crime which is growing exponentially due to its high profitability. Because of the high profitability, various organized crime groups are hiring programmers to develop increasingly complicated malicious software. Since all the groups work independently and create their own software, it becomes increasingly difficult to protect the public as it is nearly impossible to know what variation will hit the public next.

There are different ways for the culprit to get onto your computer, but the most common one is referred to as drive-by downloads. This is as simple as visiting a site which has been compromised and the software is automatically installed on your computer without your knowledge. Voila, your computer is now held ransom and you're made to believe you owe a fine.

Since using a computer has almost become a necessity for the average Canadian, it is impossible to be completely protected against these issues. However, certain steps can be taken to lower your risk. The main one is to avoid advertisements on adult websites. Most Ransomware is located on these sites. The idea behind this is to play on the fact that people who go to these sites usually want to keep it private. Also, never pay someone over the Internet if you don't know who they are and if you're unsure about the need to pay a fine, call the originating agency to clarify. Please do not use the number the suspicious page provides - get the correct number from the phone book or 411. If you think your computer has been compromised, you may want to have a professional computer technician look at it.

For further information on this topic see:

<http://www.antifraudcentre-centreantifraude.ca/english/ransomware.html>

Contact Person: Cpl. Janie Perreault, RCMP Regina Commercial Crime Section.

Phone: 306-537-6259

E-mail: [Janie.Perreault@rcmp-grc.gc.ca](mailto:Janie.Perreault@rcmp-grc.gc.ca)