Ransomware:
Stick'Em Up

by LYNNE ARCHIBALD,
NOTTAWAGA BEACH

Image by Michael Geiger on Unsplash

We used to worry about shadowy figures lurking in dark alleys, but we're quickly learning that the online world is full of thieves who wield ransomware as their weapon of choice. Ransomware is malicious software that locks you out of your own data unless you pay hackers a ransom. According to *Maclean's*, ransomware has become "the greatest threat to the digital networks on which the modern world depends. Hospitals, corporate giants, small businesses, cities and regular individuals have fallen victim to this expanding sub-genre of cybercrime."

Two characteristics make municipalities ideal victims for hackers: public data that need to be carefully guarded, and access to funds. This is what brought cybercrime to southern Georgian Bay.

In April 2018, the Town of Wasaga Beach's computer systems were hacked and held for ransom. According to a report by the town's treasurer, it took nearly seven weeks to recover from the attack. Town staff worked with computer experts to negotiate the return of the data, ultimately paying $34,950. Then they had to build a new network, scrub the released data to ensure they were clean, reconfigure existing software programs, and install new software and hardware for enhanced security. An additional $37,000 was paid to the computer consultants. The total cost, including staff overtime and productivity losses: $250,000.

A few months later, the Town of Midland paid $76,000 (eight bitcoins) to unknown hackers who had encrypted its servers and backups. Fortunately, following the Wasaga Beach attack Midland had purchased insurance for the rest of 2018 for just under $7,500, with coverage for up to $2 million. The insurer brought in expert negotiators who advised paying the initial ransom demand of six bitcoins. In the end, Midland had to pay two more bitcoins in order to get all the encryption keys. Before the attack, the town had already been increasing security and was working on a plan to migrate their servers to the County of Simcoe. This has since become a priority.

In each case, the attack occurred on a weekend and the towns later went public with what had happened. Many businesses and individuals don't from embarrassment, but also because the transactions are untraceable — ransoms are paid in cryptocurrency, usually Bitcoin. Even when victims go public, the chances of catching the hacker are essentially zero. To date, the OPP has never laid a ransomware charge.

Here in Tiny, IT/Health and Safety Administrator Brenda Biggs reassured residents that "the township has over the past few years strengthened the security of township data and network systems due to the increase in ransomware and phishing scams by implementing the following measures: higher levels of email virus detection; strong virus protection for all devices located on the township's network; implementation of a full managed service strategy to provide IT expertise in the field of network management, strong backup procedures and protocols, security on all devices, and best practices and policies for all users to adhere to; and the purchase of cyber-insurance in the event of a ransomware attack."

Biggs confirmed that the township is confident with the above systems in place and that their number one focus is to ensure that the information belonging to the public and Tiny residents is kept secure and free from malicious predators.
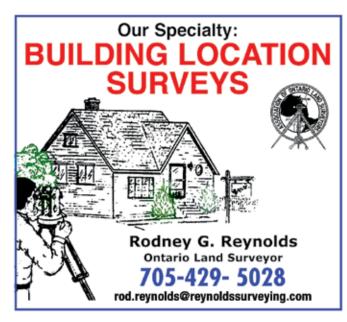
How we can protect ourselves

The anti-virus software company Norton reports that 10 million Canadians were affected by cybercrime in 2017, which cost them a whopping $1.8 billion. Each person lost an average of 10 hours of time dealing with the crime. The consumers most prone to cybercrime were Millennials, representing 42% of all victims.*

Ransomware is usually delivered via phishing emails: a fake alert that tries to get you to click on a link or open an attachment immediately, or an imposter email crafted to resemble correspondence sent out by banks, credit card companies and other organizations that seek confidential information, such as credit card numbers, account numbers, and passwords. Hackers also look for security holes in software that has not been updated using what they call "exploit kits."

Most experts recommend multiple layers of protection:

- **Back up your information regularly**, protect your backups with security software, store them on different servers, and/or store them offline. Consider using a cloud service. Backing up data removes a hacker's leverage over you. If you can afford to lose what is on your computer, you don't have to pay the ransom.

- **Always keep your security software, operating system and other software up to date**. Software updates will frequently include patches for newly discovered security vulnerabilities before they can be exploited.

- **Never open links or attachments unless you are 100% certain** about what they are and where they came from.

- **Use strong passwords**, and don't use the same password on more than one site.

2017 Norton Cyber Security Insights Report:
https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-comparison-canada-en.pdf