RANSOMWARE

Government Employees Can be Targets

We don't typically give much thought to whether we could be potential targets for hackers simply because of the work we do. No matter where we work, we handle information every day. That makes us targets for hackers.

Why Me?

Ransomware, a form of malware that locks and encrypts files on a victim's computer, is on the rise. According to a report by EmsiSoft, "In 2019, the U.S. was hit by an unprecedented and unrelenting barrage of ransomware attacks that impacted at least 966 government agencies, educational establishments and healthcare providers at a potential cost in excess of $7.5 billion".

> *Ransomware is an increasingly popular form of malware aimed at government employees. It is our responsibility to continue to defend against these threats. We all have a significant role to play in the security of information as the majority of successful cyber attacks have been a result of user error. Educating users on cyber security best practices is the first step in tackling the ransomware issue.*
>
> **John Roberts**
> Chief Information Security Officer,
> Ministry of Government and Consumer Services

The Financial Post recently reported ransomware attacks have occurred that were aimed at employees in an unnamed Canadian government health agency and an university actively engaged in COVID-19 research. In these attacks, hackers deployed phishing emails with infected file attachments. If the recipient were to click on the attachment, their files would be encrypted until a ransom was paid. In both instances the attacks were unsuccessful.

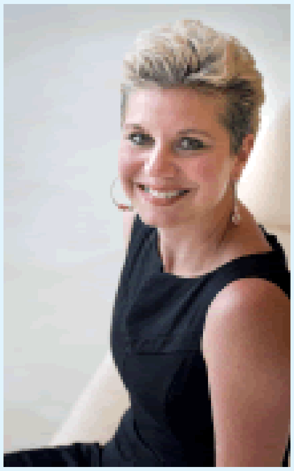
Over the past few years, there has been a number of high-profile ransomware incidents that have impacted all types of organizations. Aside from costing millions or billions of dollars in lost revenue, these attacks also resulted in damage to public trust. They have also led to sensitive information being exposed. In many instances, only once the hackers' demands for payment were met, was control of the ransomed computer systems released.

> *Government employees can be targets for ransomware and other types of cybercrime, because they may be providing services that communities rely upon, and that makes information in their care a valuable commodity to cyber criminals.*
>
> **Jenny Alfandary**
> Chief Information Officer, Metrolinx

Organizations attacked by ransomware in recent years include Garmin, LifeLabs, A. P. Moller-Maersk, Sony Pictures, and San Francisco Municipal Transportation Agency. Some of these attacks were so severe that the affected organizations were forced to cease normal operations and resort to non-computer-based transactions and communications, as in the case of the Sony Pictures attack, where they had to communicate with their employees using paper-based methods.

How do ransomware attacks typically play out, and what do hackers hope to gain? The goal of hackers is to profit financially. Hackers will hold computer systems hostage, forcing businesses and individuals to pay a ransom before files and information are released. Hackers' demands for payment are usually in the form of cryptocurrencies like Bitcoin to help avoid detection. In return for payment, hackers typically provide a decryption key so the affected organization or individual is able to recover their information and resume operations. In many instances, the decryption key does not restore all the data, and sometimes the decryption key does not work at all.

Similarly, in the case of private individuals, hackers look to exploit opportunities by threatening to expose personal information in return for payment. Cyber security experts caution against giving into hackers' ransom demands because there are no guarantees that victims will get their information back. Even in cases where people do, there is no guarantee these hackers won't target them again in the future. What can you do to protect yourself and the information you handle every day?



> *"Cyber Security Awareness Month is an internationally recognized campaign held each October to raise public awareness of online safety, privacy and cyber security. This month-long event, coupled with cyber security awareness training programs in workplaces across Canada, should remind us how important it is to always safeguard our information, whether it's on a personal or work device."*
>
> **Christine Beauchamp**
> Acting Director, Contact Centre & Incident Detection,
> Canadian Centre for Cyber Security

For more tips and information on ransomware, please refer to the What is Ransomware and How to Prevent Ransomware Attacks article.

As public service employees we all have a responsibility to safeguard information placed in our care. By everyone doing their part, we all help to keep our workplaces and homes safe and secure

This article was produced in collaboration with the Ministry of Government and Consumer Services, cyber security risk management staff at Metrolinx, and the Canadian Centre for Cyber Security as part of raising cyber awareness during Cyber Security Awareness Month.

GETCYBERSAFE.CA

METROLINX

Communications Security Establishment
Centre de la sécurité des télécommunications

Ontario

CYBER SECURITY AWARENESS MONTH