HSB BI&I

Munich RE

Risk Solutions

Home Cyber Protection

Loss Bulletin

The Boiler Inspection and Insurance Company of Canada (BI&I)

390 Bay Street
Suite 2000
Toronto, Ontario M5H 2Y2
Tel: (416) 363-5491
biico.com

Connect with us

Home Cyber Protection

Homeowners' digital information and computer systems can be damaged, exploited or destroyed by a virus or hacker. As the number of connected devices used and services depended upon increase daily, homeowners have become more exposed to cyber criminals looking for ways to defraud them. Even with antivirus software installed on computers, homeowners are still vulnerable to computer attacks and new viruses continue to emerge that can bypass known defenses.

Typical homeowner policies do not cover losses caused by these types of cyber threats.

Coverage is now available through BI&I Home Cyber Protection, in which homeowners and tenants can receive coverage for attacks to computers and connected home devices, as well as online fraud and cyber extortion.

Cyber Attack on Computer

An unsuspecting click on a malicious link or email attachment can cause widespread damage to a home computer's operating system.

An individual opened an electronic file attached to an email which looked like it was from UPS. It unleashed a nasty virus called Virus XP that was making its rounds. The virus corrupted data and

reconfigured the existing computer setup. In order to restore the system, a "start from scratch" alternative was pursued, which required reformatting the hard disk, erasing everything on it, and reinstalling the operating system and all software applications. This option was only possible because a back-up was available.

Cyber Attack on Connected Home Device

A homeowner may believe he or she is the only person able to access and control their own smart home devices. But they may not be.

One evening, the insured's internet wasn't working. After the usual attempts, the homeowner contacted the internet provider who explained that there was not a known outage in the area, but did notice some strange activity on the account. Someone had gained access to the wireless router and added new services to the account including adding a new phone line. A smart thermostat and security system were also connected providing additional information for this hacker.

The insured ended up having to call and pay for service technicians from the internet and security providers to have both systems reinstalled.

Cyber Extortion

Cyber criminals may demand money under the threat of deleting a homeowner's computer files or stealing personal information.

A ransom note was received on the Tuesday before Thanksgiving. It popped up on the homeowner's computer screen soon after she discovered that all of her files had been locked. "Your files are encrypted," it announced.

"To get the key to decrypt files you must pay $1,000 USD." If payment was not received within a week, the price would increase to $2,000.

The threat included destruction of her decryption key, and any chance of accessing the thousands of files on her PC — all of her data — would be lost forever. The homeowner paid the $1,000 extortion demand and had to pay an information technology firm to investigate the ransom and ensure that there were no viruses left behind on her computer.

Online Fraud

Criminals continue to find creative ways to bait unsuspecting people in deception schemes through the internet.

One morning, a homeowner received an email from her grandson Tommy, who was in trouble. Tommy's email read that he had been in a car accident the night before, was facing possible criminal charges and needed money for a lawyer. Within 20 minutes another email was received. This one was from a man who identified himself as Tommy's attorney, who provided a brusque, professional rundown of the situation. Apparently, the driver in the other car, a foreign diplomat, was injured. The diplomat had agreed to accept $1,950 to cover her costs. She was ready to sign a release just as soon as the homeowner wired the funds and provided the lawyer with the wire transmission registration number. The homeowner called Tommy, yet got no answer.

Fearing for her grandson, she paid cash for the MoneyGram, sent it off, and emailed the lawyer the registration number.

The next morning, another email arrived from the lawyer looking for more money. The warning lights flashed brighter. The homeowner called her grandson again, only to find out Tommy had never been in an accident.

Data Breach

Most individuals do not realize that they may be holding sensitive information of others and would be responsible for notifying affected individuals if that information was lost or stolen.

A mom regularly volunteers at her kids' schools, helping teachers track students' birthdays and their lunch account numbers. She uses a spreadsheet on her personal tablet. The tablet is not secured with a password and the data contained in the spreadsheet is not encrypted. During a field trip, she leaves the tablet on the bus and it is never recovered. The loss of this personal information is considered a data breach. Fearing that families at the school might become victims of identity theft, the woman called her lawyer who advised her to notify the affected families and provide them with fraud alert and case management services.

© 2018 The Boiler Inspection and Insurance Company of Canada (BI&I).
All rights reserved.