Canadian Transit System Hit By Ransomware Attack

What You Need to Know

What Happened?

Vancouver's transit system, TransLink, confirmed on December 3, 2020 their system was targeted with ransomware. The attack is believed to have started with a successful phishing email.

To help mitigate the attack, TransLink shut down several of its IT services, including tap and pay, and commuters were unable to use credit or debit cards in the TransLink fare machines.

The ransomware note went on to threaten to release certain information in three days if TransLink did not meet its demands, which were unspecified in this letter.

Protecting Your Business from Ransomware

As a trusted IT Support provider, we can play a critical role in helping your business stay ahead of ransomware risks and better safeguard your company. Here's a quick overview of a comprehensive ransomware protection strategy:

- **Employee education:** Teach your team about the ways that criminals can gain access to information and why they must adhere to security guidelines.
- **Antivirus:** A necessary piece of the puzzle to help detect attacks, but certainly not the be-all and end-all for ransomware protection.
- **Business continuity and disaster recovery (BCDR):** You can restore systems to the state they were in immediately before the attack, ensuring minimal data loss.

Contact us today to learn how we can arm you with the best solutions to combat cyber attacks.

For more information please contact:

Ian Evans, President & CEO

Phone: 647-361-8191 x 105

Email: contact@etechcomputing

www.etechcloud.ca

Did You Know...

Ransomware can easily bypass antivirus, pop-up blockers, email/spam filters.

The average ransom demanded is $5,600.

However downtime costs are nearly 50X greater than the ransom requested.

Source: Datto's Global State of the Channel Ransomware Report

E-TECH