48,000 CRA Accounts Might Have Been Hacked

Description

Cyberattacks were rampant in July and August with the acceleration in credential stuffing activities. Cybercriminals targeted more than 48,000 Canada Revenue Agency (CRA) accounts. The Treasury Board of Canada uncovered the suspicious activities in the CRA and GCKey portals.

Investigations by the Royal Canadian Mounted Police are ongoing. Affected departments are also coordinating with the Office of the Privacy Commissioner to give updates and furnish personal information on compromised accounts.

Modus operandi

Online attackers use the credential stuffing method to obtain personal information. People who reuse usernames and passwords across multiple platforms are often the victims of these hackers. The GCKey was not compromised, although the treasury board revoked 9,300 credentials.

If you're one of the users contacted by the treasury, register for new credentials to block subsequent or future attacks. The hackers even sell the stolen credentials to the dark web for other criminals to rip-off. You can make use of the SecureKey Concierge, so you can sign in or access 269 government services.

On the CRA portal, there's evidence of suspicious activities. Chairman and Founder of CyberScout, Adam Levin revealed that COVID-related scams have increased by over 30,000%. Some people give out information to these scammers out of desperation to receive assistance. You're also vulnerable if you overshare personal details on social media.

Defrauding programs

The Canadian Anti-Fraud Centre (CAFC) reports more than 700 cases of CERB fraud. These hackers steal identities, open accounts in their names, and redirect CERB payments. They were also hitting on people who did not apply for CERB. It could be frustrating if you're a victim because you need to clear

your name and prove you didn't receive the money.

Data breaches are becoming prevalent and cybercriminals are getting bolder. They can hack a government website to harvest SIN numbers, addresses, and banking information. The CFAC warns about phishing scams through emails and text messages. Don't respond to these unsolicited emails or text messages.

Cybercrime fighter

Cybersecurity stock **Absolute Software** (TSX:ABT) is gaining popularity among stock market investors. The $645.61 million company from Vancouver, Canada, offers endpoint security and data risk management solutions to governments and enterprises across various industries.

The solutions are in Software as a service (SaaS) business model. They are installed in devices, such as smartphones, laptops, tablets, and computers. Laptops, tablets and smartphones. The Absolute Data and Device Security enable customers to secure endpoints, assess risk and respond to security threats.

Based on a Cybersecurity Ventures Report**,** cybercrimes will exceed $6 trillion by 2021. Losses can be in the form of stolen money, lost productivity, and damaged data. You can add intellectual property theft and breach in personal and financial information.

In the digital environment, cybersecurity is one of the most vital technologies. It prevents cybercrimes as thwart hackers from compromising sensitive information. Absolute Software will be at the forefront of the fight against cybercriminals. The stock is reasonably priced at $15.20 per share and paying a modest 2.26% dividend.

Don't fall prey

Times are dangerous, with fraudsters stalking unsuspecting Canadians. The CRA and other government agencies never send e-mails, texts or call people to gather personal information. Similarly, banks don't inquire about account details.

CATEGORY

1. Dividend Stocks
2. Investing
3. Tech Stocks

TICKERS GLOBAL

1. TSX:ABST (Absolute Software)

PARTNER-FEEDS

1. Business Insider

2. Koyfin
3. Msn
4. Newscred
5. Sharewise
6. Yahoo CA

Category

1. Dividend Stocks
2. Investing
3. Tech Stocks

Date
2025/07/17
Date Created
2020/09/30
Author
cliew