CBC

Technology & Science

Email, text message attacks surge during COVID-19 crisis

Cyber fraudsters preying on vulnerabilities spurred by pandemic

Thomas Daigle · CBC News ·
Posted: Mar 30, 2020 4:00 AM ET | Last Updated: March 30

This fraudulent text, purporting to be from the Canada Emergency Response Benefit, is one of several scams related to the COVID-19 crisis. (Thomas Daigle/CBC)

comments

Cybersecurity experts describe it as a perfect storm: employees working from home — away from their firm's IT experts and sometimes without the

protection of a corporate computer network — and hungry for information about a mysterious coronavirus.

With the COVID-19 crisis as the backdrop, fraudsters appear to be redoubling their efforts to steal information or money from unsuspecting users, sending fake emails and text messages as bait, in a scheme known as phishing.

In one scam, fraudsters pretend to be processing EI claims, preying on Canadians who've recently lost their jobs. Users are asked to enter their details, only for the information to be accessed by criminals.

Other schemes come disguised as messages from Shoppers Drug Mart, Public Health Agency of Canada or the World Health Organization. In all cases, the goal is to steal a user's information or money, or infect their devices with malware.

"The tactics are still the same, it's just the subject matter that's changed," said Joe Martin, with North Vancouver-based tech firm Compunet.

"People who do this for a living, they know that they're going to get some clicks, as long as the coronavirus continues to be an issue."

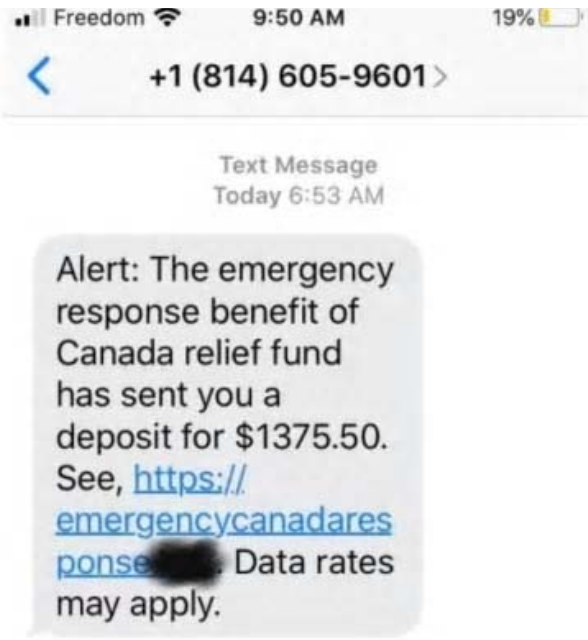
As number of online and telephone scams rises, Shoppers Drug Mart said on its website 'if you receive an unsolicited call, we strongly encourage you to hang up, and call your local store back directly.' (Michael Wilson/CBC)

According to analysis by virtual private network provider Atlas VPN, the number of active websites used for phishing has increased by 350 per cent between January and March, just as the COVID-19 crisis erupted.

What's more, California-based Barracuda Networks said it had observed a 667 per cent spike in phishing emails from the end of February until late March.

- **Canada's cyber spies taking down sites as battle against COVID-19 fraud begins**
- **Trudeau warns of COVID-19 text scam exploiting new emergency benefit program**

The most high-profile scam in this country — highlighted last week by Prime Minister Justin Trudeau in his daily televised address — involves text messages ostensibly offering cash as part of the federal government's Emergency Response Benefit. In reality, the con seeks to get users to click on a link leading them to a fraudulent scheme.



Prime Minister Justin Trudeau issued a warning about texts and other scams that try to lure Canadians using messages about COVID-19 support. CBC has intentionally blurred part of the URL in this message. (Submitted to CBC)

How to prevent phishing

Toronto-based cybersecurity consultant Ritesh Kotak said he had been repeatedly targeted in COVID-19-related scams, receiving "numerous" phishing messages since the start of the pandemic.

"My general advice is 'think twice before you click,'" he said. Kotak also advises using a virtual private network at home for added protection.

Compunet, the B.C.-based firm, sent out an email to clients with the following guidance:

- "Think before you click a link or download an attachment. If you're unsure, don't click or download.
- Don't respond to any requests for sensitive information, even if it's supposedly to update payment information with an account.
- Use well-known websites, such as the CDC or WHO, to stay up-to-date on coronavirus information.
- Hover over the sender's email address to verify whether or not it's a legitimate domain from a familiar organization.
- Remember that legitimate organizations won't ask you to update account information or send personal data via email."
- **Scammers take advantage of COVID-19 fears with calls, texts, emails**

'Can I Be Phished?'

Cybersecurity firm Click Armor, based in Ottawa, even created an online self-assessment tool called "Can I Be Phished?" The platform presents a series of emails and asks users to flag the messages as either safe or suspicious.

The online assessment tool, 'Can I Be Phished?' features animations and emails, asking users to identify whether messages are fraudulent or not. (Click Armor)

"It comes down to people being aware of how they might be targeted and what their vulnerabilities are," Scott Wright, Click Armor's CEO said in an interview.

"We see a lot of attacks happening that try to exploit people's anxieties" related to the pandemic itself and companies' adjustment to it, Wright said.

He warned even consumers who believe they follow best practices can fall victim to scams.