

# Canadians have lost more than \$1.2 million to COVID-19 scams

Con artists from all around the world are preying on the anxious

[Elizabeth Thompson](#), [Katie Nicholson](#), [Jason Ho](#) · CBC News · Posted: May 01, 2020 4:00 AM ET | Last Updated: May 1



Hundreds of Canadians have received text messages and emails from scammers trying to cash in on the COVID-19 pandemic. (Martin Diotte/CBC)

Canadians have lost more than \$1.2 million in recent weeks to scammers taking advantage of the COVID-19 pandemic, CBC News has learned.

Jeff Thomson of the Canadian Anti-Fraud Centre said the centre has received 739 reports since March 6 of attempts to defraud Canadians with scams related to the pandemic. He said 178 of those attempts succeeded.

The centre is also seeing attempts to use the pandemic as cover to infect computers with malware.

The victims of one such scheme receive messages telling them they've been exposed to someone who has tested positive for COVID-19 and asking them to fill out what looks like an Excel form. When users click to enable the content and view the form, it infects their computers with a Trojan downloader that installs malicious files, said Thomson.

He said it's not the first time scammers have adapted their tactics to try to cash in on an emergency.

"It's the heightened sense of anxiety, of fear ... The isolation that people are in right now is also a key factor," Thomson told CBC News.

"Essentially, frauds are designed to get people to not think straight. So if, you know, people are already in that state ... they may not be thinking straight. So it's prime time for scammers and fraudsters to solicit for scams."

**Any direct communication Canadians receive about applying for the CERB is a scam.-**

*Etienne Biram, CRA spokesperson*

The Canadian Centre for Cyber Security is also seeing attempts to scam Canadians over COVID-19.

"COVID-19 has presented cybercriminals and fraudsters with an effective lure to encourage victims to visit fake web sites, open email attachments and click on text message links," said Ryan Foreman, spokesman for the Communications Security Establishment and the Centre for Cyber Security.

"These email typically impersonate health organizations and can even pretend to be from the Government of Canada. Canadians need to be aware that this type of threat is real, is happening, and that these types of COVID-19 email and websites are really fraud."

Foreman said the centre has worked with industry to take down 2,000 websites that were trying to defraud Canadians — including some that pretended to belong to government organizations like the Public Health Agency of Canada, the Canada Revenue Agency (CRA) and the Canada Border Services Agency.

## **Scammers impersonating government agencies**

Those government agencies are involved in one way or another with the federal government's pandemic response; the CRA, for instance, is charged with getting Canada Emergency Response Benefit (CERB) payments out the door. Online con artists are making that work more challenging.

"Scams purporting to be connected to the CERB may have many variations, but all appear to have the goal of duping Canadians into providing personal information under the guise of helping them claim the benefit," said CRA spokesperson Etienne Biram.

"To be clear, the CRA is not contacting Canadians to claim CERB. Canadians must apply for the credit themselves. Simply put, any direct communication Canadians receive about applying for the CERB is a scam."

Toronto-area resident Joanna Giannakopoulos almost fell for that scam. She received a text a few days after she was laid off from her job in a restaurant.

"I clicked the link because I thought it was a text from the government," she said.

## Phishing swindles, merchandise scams

Following the instructions in the text, Giannakopoulos filled out and submitted personal information — her full name, her social insurance number, her bank, her bank account number and password — before she suddenly realized there was something wrong with the text's website address.

She had to scramble to notify her bank and credit agencies that her information could have been breached.

"I think that can be an easy trap, especially at a vulnerable time like right now," she said.



Jeff Thomson is a senior RCMP intelligence analyst with the Canadian Anti-Fraud Centre who says scammers are taking advantage of the pandemic. (Jean Delisle/CBC) Thomson said the phishing scam asking victims to click on a link to collect a benefit is one of the "hot scams" — but it's not the only one the centre is seeing.

"We continue to see a variety of merchandise scams, including offers for free masks or test kits ... text messages or email that ask you to click on links to complete a survey which, again, will harvest your credit card, your personal information."

## Con artists are upping their game

Other countries, such as the United Kingdom and the United States, are also getting hit with COVID-19 scams.

U.S. Federal Communications Commission Chairman Ajit Pai said he has seen the form of the scams evolve over the course of the pandemic.

"Unfortunately, we have seen that some of the fraudsters have adapted their business plans in the midst of a pandemic," Pai said. "Earlier on, they were focusing more on spam, text messages and robocalls relating to, for example, testing kits and fake cures and the like.

"Now, recently, we've seen an uptick in trends relating to more work-related offers. So, for example, Amazon is looking for people to work from home as an associate. Give us some of your personal information. Here's a free subscription to Netflix for five months."



U.S. Federal Communications Commission Chairman Ajit Pai. (Evan Vucci/The Associated Press)

Pai said the FCC is finding that the vast majority of the scam calls are coming from overseas into the North American market.

"They're all over the world," he said. "It could be Philippines, India, China, Brazil. Unfortunately, this is a worldwide phenomenon."

Pai said scammers often target small gateway telecom providers who pass the call or text on to larger providers. He said the FCC and the Federal Trade Commission issued a notice to those gateway providers regarding international robocalls and robotexts.

"We showed them the sources that we were seeing," said Pai. "They cracked down the next day, within 24 hours. And that's helped us combat this problem in some cases very, very quickly."

Canadian telecom companies and the association that represents them, meanwhile, say they take the problem seriously but offered few examples of concrete action.

The Canadian Radio-television and Telecommunications Commission (CRTC) said it doesn't comment on possible investigations. It said Canadians should be vigilant about scams and report them to the Canadian Anti-Fraud Centre.

*Elizabeth Thompson can be reached at [elizabeth.thompson@cbc.ca](mailto:elizabeth.thompson@cbc.ca)*