

## How to avoid common coronavirus phishing scams

The latest phishing campaigns include emails, texts and social media posts related to COVID-19 that try to put malicious software on your devices or persuade you to give up your personal information.

### What are the coronavirus phishing scams?

The coronavirus phishing scams are the latest version of a common scheme. Cybercriminals send an unsolicited email or text to potential victims. These messages are made to look like legitimate communications from health care providers, government offices, retailers, employers and other trusted sources.

The emails offer information and advice about the virus to get you to unknowingly download malicious software or give your personal information. So far, versions of these phishing emails have been made to look like official communications from:

- The World Health Organization (WHO)
- The Centers for Disease Control and Prevention (CDC)
- University and college health services

If you receive any emails or text messages about COVID-19, especially ones that direct you to click a link or download an attachment, exercise extreme caution.

### Current COVID-19 phishing scams to watch out for

**Updates from employers:** Scammers send emails that appear to come from your employer, with updates about their COVID-19 policies. These emails link to malicious content.

**Text messages about COVID-19 testing:** Scammers send text messages that urge the user to click a link for information on how to get tested for COVID-19, or that offer test results. Some request your health card and credit card to schedule an appointment.

**Government compensation messages:** Fake emails and texts that appear to come from the Government of Canada, offering employment insurance deposits and other government compensation.

If you think you might be a victim of cybercrime, report it to your local police and the [Canadian Anti-Fraud Centre](#).

## How to protect yourself from phishing scams

### Read emails and texts carefully

Read carefully and watch out for these red flags:

- impersonal or generic greetings
- spelling mistakes
- grammatical errors

All of these can suggest that an email is actually a phishing scam.

- 1. Check links in emails by hovering before you click**
- 2. Don't respond to companies or people you don't know**
- 3. Don't click on attachments or links from unknown sources**

Don't click on a link or fill out a form within an email that asks you to:

- verify your account
- reset your password
- provide confidential information

### **Don't feel pressured to reply to an urgent request**

Generally, the greater the sense of urgency, the greater the chance it's a scam. For example, if you receive threatening emails or texts that include phrases like "your account has been suspended," "download immediately for more information," "dial X to hear about your court date," don't panic and don't give out your personal information; they're most likely scams.

If ever in doubt, assume it's a scam.

*Any information provided in this e-mail has been prepared from sources believed to be reliable, but is not guaranteed by Raymond James (USA) Ltd and is not a complete summary or statement of all available data necessary for making an investment decision. Any information provided is for informational purposes only and does not constitute a recommendation. Raymond James (USA) Ltd and its employees may own options, rights or warrants to purchase any of the securities mentioned in e-mail. This e-mail is intended only for the person or entity to which it is addressed and may contain confidential and/or privileged material. Any review, retransmission, dissemination or other use of, or taking of any action in reliance upon, this information by persons or entities other than the intended recipient is prohibited. If you received this message in error, please contact the sender immediately and delete the material from your computer.*

*Raymond James (USA) Ltd. (RJLU) advisors may only conduct business with residents of the states and/or jurisdictions for which they are properly registered. Raymond James (USA) Ltd., member [FINRA/SIPC](#)*

Sources:

- *Ontario Securities Commission*
- *Canadian Bankers Association*
- *Alberta Securities Commission*
- *Government of Canada Anti-Fraud Centre*
- *Government of Canada Finance Department: Protection from frauds and scams*