Top 10 Tips to Avoid Coronavirus Scams

Provided By:

Haycor Computer Solutions

101 Citation Drive - Unit 7

Concord, Ontario L4B 2S4

www.haycorsolutions.ca

Scammers are exploiting fears surrounding Coronavirus to profit from consumers' anxieties, uncertainties and misinformation.

Are you in Canada and wish to report a case of fraud? Contact The Canadian Anti-Fraud Centre

These tips will help reduce your chances of being scammed:

1. Hang up on robocalls. Don't press any numbers. Scammers are using illegal robocalls to pitch everything from scam Coronavirus treatments to work-at home schemes. The recording might say that pressing a number will let you speak to a live operator or remove you from their call list, but it could possibly lead to even more robocalls.
2. Ignore online offers for vaccinations and home test kits. Scammers are trying to get you to buy products that aren't proven to treat or prevent the Coronavirus disease 2019 (COVID-19) — online or in stores. Please read into this Government link to receive the most up-to-date information on Medical Test Kits for Home Use
3. Fact-check information. Scammers, and sometimes well-meaning people, share information that hasn't been verified. Social Media has proven to be full of misinformation and links to malicious websites. Before you pass on any messages, contact trusted sources to fact check. Even if Haycor provides facts, it never hurts to fact-check.
    - Canada Public Health: Coronavirus disease (COVID-19)
    - World Health Organization: COVID-19 Outbreak
    - Center for Disease Control (CDC): Coronavirus
4. Online sellers may claim to have in-demand products, like cleaning, household, and health and medical supplies when, in fact, they don't. You should only purchase from known, established and reputable online sellers.
    - Know who you are buying from and make sure the website is secured. Secured websites have a locked lock symbol beside the URL. Unsecure websites will have unlocked lock symbols.
5. Avoid responding to texts and emails about money from the Government. The details are still being worked out. Anyone who tells you they can get you the money now is a scammer.
6. Be wary of emails "sent" by people in authority asking you to send money, transfer funds, purchase gift cards or email confidential information. A scammer can send an email that looks real, but the scammer is pretending to be the person in authority ("spoofed email").
7. The economic disruption has led to a flood of unusual financial transactions – expedited orders, cancelled deals, refunds, etc. That's why an emergency request that would have raised eyebrows in the past might not set off the same alarms now. In addition, the scammers know teleworking employees can't easily walk down the hall to investigate a questionable directive.
    - Ensure your staff is informed to call the person making the request directly. Make sure you are calling them on a previously known good number to verify prior to taking any actions.
8. Don't click on links from sources you don't know. We recommend hovering over a link before clicking. This will allow you to see the URL before clicking on it. When in doubt, skip it and DO NOT click it. They could download viruses onto your computer or device.

9. Watch for emails claiming to be from the Health Canada, Centers for Disease Control and Prevention (CDC), the World Health Organization, or experts saying they have information about the virus. For the most up-to-date information about the Coronavirus, visit Canada Public Health the Centers for Disease Control and Prevention (CDC) and the World Health Organization (WHO). Secured websites are provided above.
10. Do your homework regarding donations; whether it's through a charity or a crowdfunding website. Don't let anyone pressure and rush you into donating. If someone wants donations in cash, by gift card, or by wiring money, don't do it.

Beware of These Common Scams

Please read below common scams reported to the Canadian Anti-Fraud Center. This list is expected to evolve daily, even hourly.

Cybercriminals have been acting as:

- Government departments
    - Sending out coronavirus-themed phishing emails
    - Tricking you into opening malicious attachments
    - Tricking you to reveal sensitive personal and financial details
- Local and provincial hydro/electrical power companies
    - Threatening to disconnect your power for missing payment(s)
- Centres for Disease Control and Prevention or the World Health Organization
    - Offering fake lists for sale of COVID-19 infected people in your neighbourhood
- Public Health Agency of Canada
    - Giving false results saying you have been tested positive for COVID-19
    - Tricking you into confirming your health card and credit card numbers for a prescription
- Red Cross and other known charities
    - Offering free medical products (e.g. masks) for a donation
- Door-to-door salespeople
    - Selling household decontamination services
- Private companies
    - Offering fast COVID-19 tests for sale
        - Only health care providers can perform the tests
        - No other tests are genuine or guaranteed to provide accurate results
    - Selling fraudulent products that claim to treat or prevent the disease
        - Unapproved drugs threaten public health and violate federal laws
- Cleaning or heating companies
    - Offering duct cleaning services or air filters to protect from COVID-19
- Financial advisors o pressuring people to invest in hot new stocks related to the disease
    - Offering financial aid and/or loans to help you get through the shutdowns