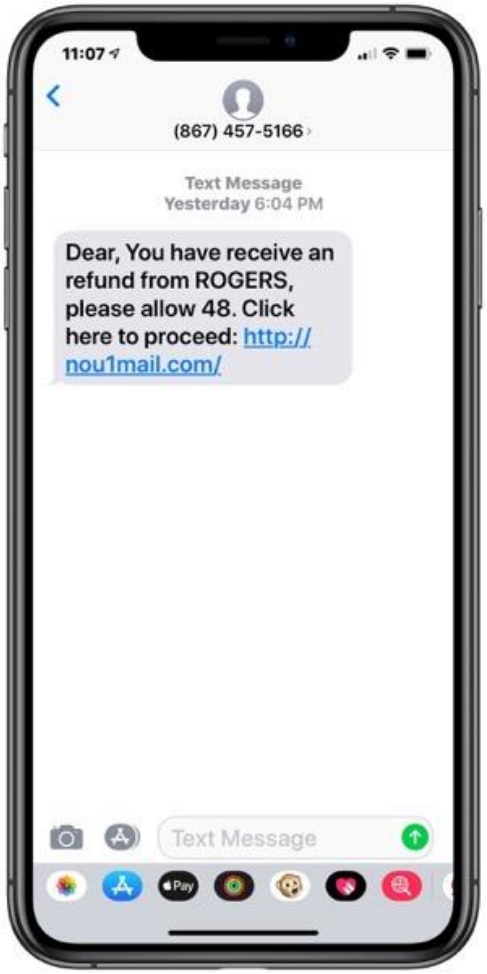
Phishing Text Scams

You can never be too cautious when receiving a text message from *anyone* that is not one of your known contacts.

Since the onset of the pandemic, it is more important than ever to use caution as fraudsters are taking advantage of the influx of online shopping by impersonating companies like Amazon, Canada Post and PayPal.



The text message will direct the user to click a link to:

- Update/confirm account information
- Confirm an order that was placed
- Accept a refund for an alleged "overpayment"

By clicking on the link and entering personal information, the fraudster can use it to perpetrate a scam. Furthermore, by simply clicking the link, you may download malicious software to your device without your knowledge or consent. This malicious software could potentially track everything you do on your device including your e-mail, social media, and online banking accounts.

How do I spot a Phishing Text Scam?

- Spelling/grammar errors
- A sense of urgency to respond or something bad will happen
- Company name, email or website will look *identical* to the legitimate company's
  Example: www.netfix.com instead of www.netflix.com (missing one letter)

- The situation doesn't make sense: you don't have an account with the company, you never purchased anything, or you did purchase something but *definitely* didn't overpay
- Hover your mouse **(but don't click!)** over the provided link and the *true* destination will appear.

If you ever have *any* doubt about the legitimacy of a text message, do a Google search to obtain the legitimate contact information to inquire directly.

For more information about scams, fraud prevention or to report a fraud, contact the Canadian Anti-Fraud Centre toll free at 1-888-495-8501 or visit their website

www.antifraudcentre-centreantifraude.ca/