Defending Against COVID-19 Cyber Scams

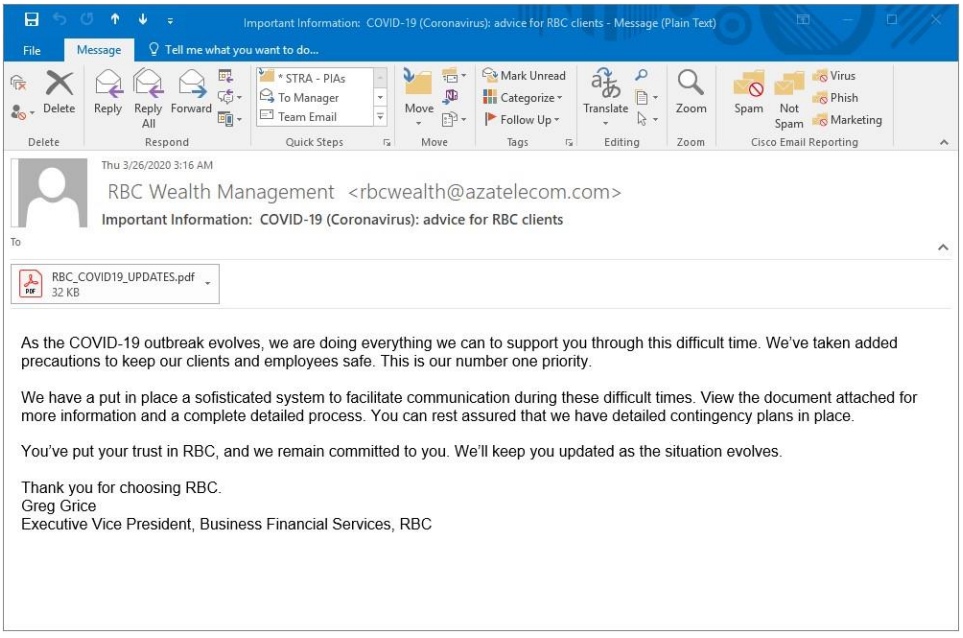
Northern Health's Information Security team warns individuals to remain vigilant for scams related to Coronavirus Disease 2019 (COVID-19).

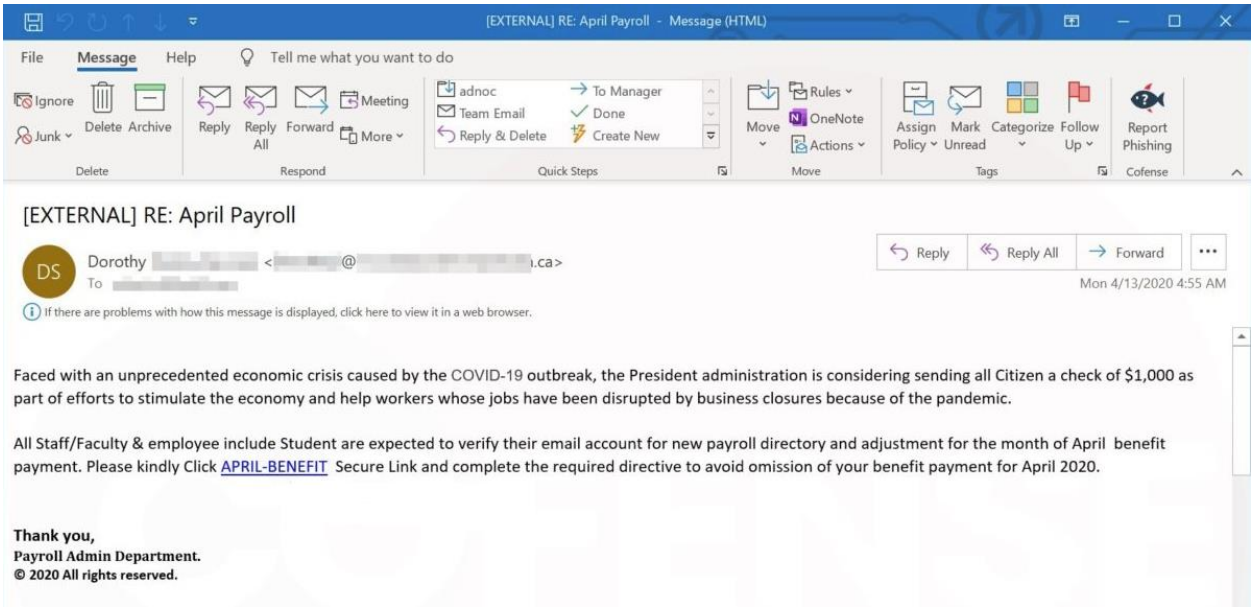
Cyber criminals are sending emails with malicious attachments or links to fraudulent websites to trick victims into revealing sensitive information or donating to fraudulent charities or causes. Exercise caution in handling any email with a COVID-19-related subject line, attachment, or hyperlink, and be wary of social media pleas, texts, or calls related to COVID-19.

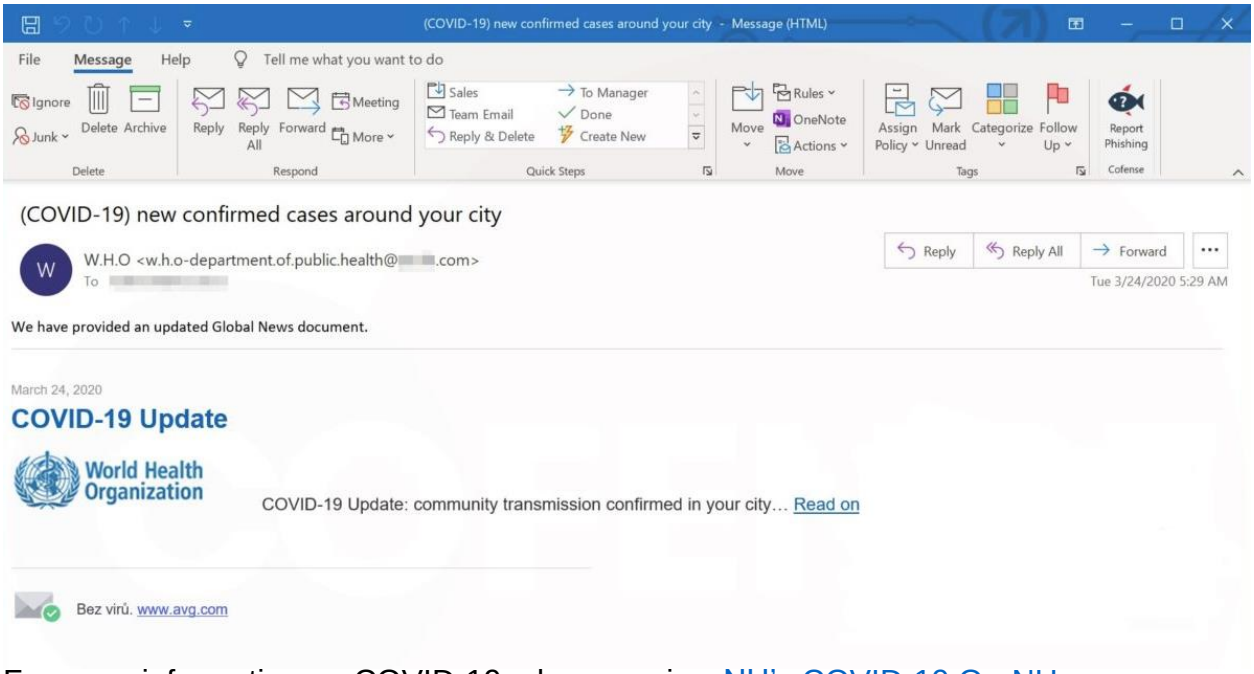
NH InfoSec encourages individuals to remain vigilant and take the following precautions and recommendations.

- Avoid clicking on links in unsolicited emails and be wary of email attachments. For more details take a look at our Phishing security bulletin for more information.
- Use trusted sources—such as legitimate, government websites—for up-to-date, fact-based information about COVID-19.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information.
- Verify a charity's authenticity before making donations. Review the Canada Revenue Agency Charities listings page on Charity Scams for more information.
- Take our Information Security awareness course on LearningHub – click here to register.

SAMPLES OF MALICIOUS EMAIL:







For more information on COVID-19, please review [NH's COVID-19 OurNH page.]