# Memo

**To:** Members and Stakeholders of the Canadian Payroll Association

**From:** The Canadian Payroll Association

**Date:** March 2019

**Re:** Cyber Criminals Targeting Payroll

The Canadian Payroll Association has learned about a new scam targeting payroll professionals through social media.

This particular phishing scam involves emails targeting employee direct deposit account information. Cybercriminals are using LinkedIn to identify individuals who work in payroll for an organization. Scammers then locate another employee of that organization and impersonate that employee by sending an email to the identified payroll representative from a private account requesting that their bank account information be updated to a fraudulent account.

The scam is often only identified when the payroll professional seeks clarification from the targeted employee and applies additional checks and balances before fulfilling the request.

Payroll professionals are warned that they should always apply heightened security for banking-related emails initiated by employees requesting to update or change direct deposit credentials. If you or your colleagues receive a suspicious email, forward it to your IT or HR representative. Protecting your employees' personal data is crucial.

## REMEMBER

- **Employee privacy should be protected at all costs**
- **Every organization should have checks and balances in place that verify changes to banking information are valid**
- **If you are ever unsure about a request coming from an employee, err on the side of caution and take measures to verify the authenticity of the request**
- **Send any suspicious emails to IT and/or HR to initiatite further action, if needed**
- **Remain vigilant about your digital communications**