



[News](#) > [General](#) > [Supplier Email Compromised!](#)

Supplier Email Compromised!

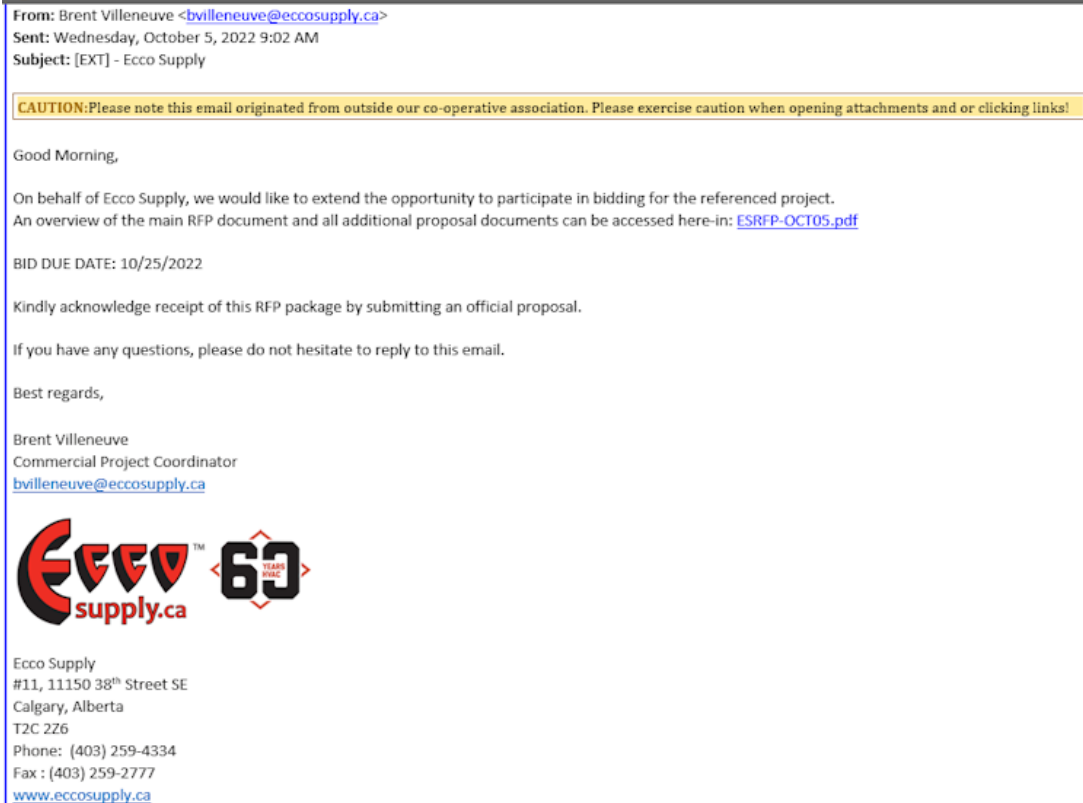
2022-10-05 - Don Guilbeault - [Comments \(0\)](#) - [General](#)

!!!ATTENTION Everyone!!!

One of our Suppliers has had their email compromised and blasted their contacts with a RFP request with a link to a "FAKE PDF" Document. This one was very difficult to identify as a malicious email. One of our Team Members received this email, but it triggered their Spidey senses as unusual. Turns out the email is a phishing attempt.

The only identifiable **RED** flag on this email is when hovering over the link to the PDF document the website seemed just a little off: (<https://eccosupply.brizy.site/>)

The email in every aspect looked like a normal email, See example below:



Our Team Member reached out to me to check in on the email. My recommendation was to confirm the legitimacy of the email by reaching out to the company.

KEY Notes: When reaching out to the company to confirm the legitimacy of an email:

1. DO NOT reply to the email
2. DO NOT contact the company by any contact details provided in the email.
3. Google the company and find their contact information directly from their website.

I contacted Ecco Supply in Calgary and they did confirm that their email system had been compromised.

Great catch by our Team on this one. REMEMBER when in doubt always ask first.