GRADE·A

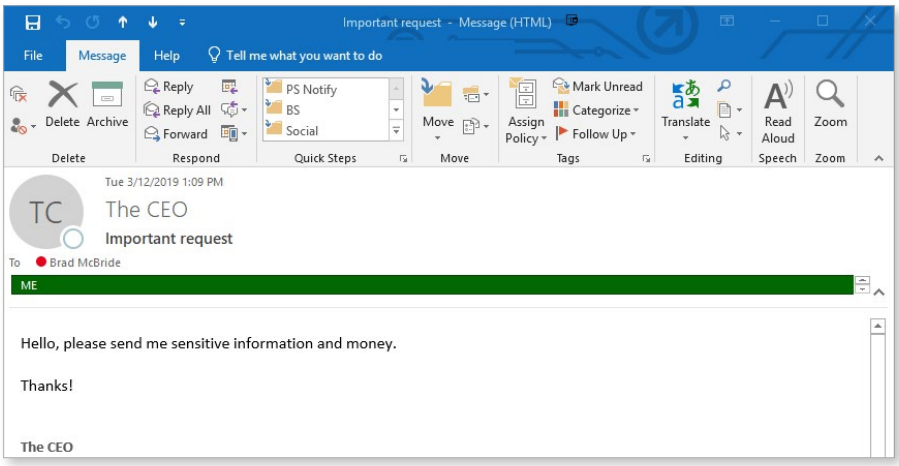
Detecting Scammers

If you ever receive an email that seems a little strange in any way - asking for any sensitive information, involves money, you never know - it's important to check and make sure it is coming from the right person.

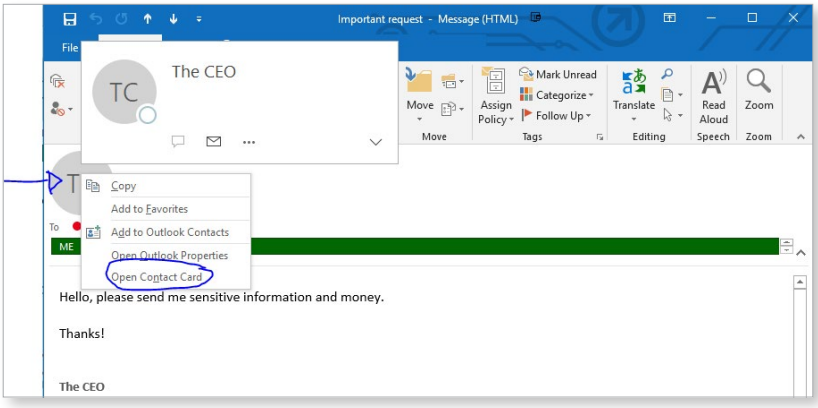
Surprisingly (and unfortunately) scammers are sometimes able to use the same display name as someone in your company - even if their email address is not correct.

Here are some steps you can follow to check if the email address is correct.

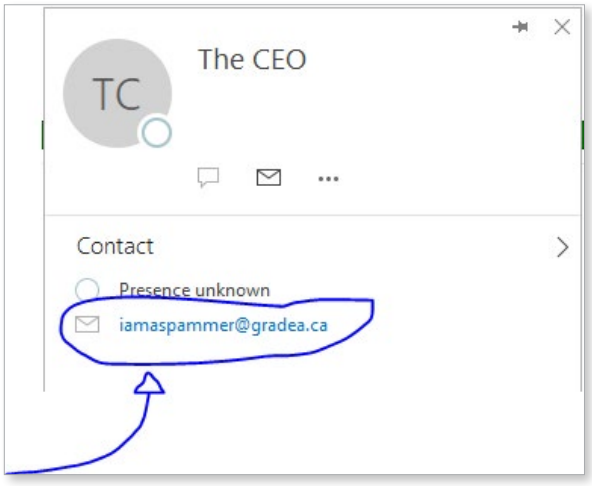
This example is an email that appears to be from "The CEO".



First - check to make sure that this is, in fact, the CEO's email addresses. To do that, Right Click (or if in webmail, just hover the mouse for 3 seconds) on their picture (or initials/name if there is no picture) and select "Open Contact Card".



The contact card will open for the sender, and you can see in the circle below that it isn't from the CEO's email address. Instead it appears to be a different email address, most likely a spammer trying to scam the company in some way.



The email is fake, what do you do?

In this case you should report this email to Grade A or your IT department and we will block the account in your spam filter. However, these spammers constantly change email accounts and companies, and they may try again from a new address. It's important to always be vigilant and double check. If you are ever in doubt reach out to Grade A or your IT department and we can check the email for you to make sure it is legitimate.

Having Trouble?

You can also email us at info@gradea.ca or call us at 613-721-3331 or 1-866-5-GRADEA.