Part of you is dying to click the link. After all, the email came from the CEO and she needs your help. Sure, it wasn't your fault the company's payroll wasn't dispersed, but you could really shine with one click of the mouse that would release the funds and make everyone happy.

Signs of a potential phishing email checklst:

- ☑ The sender address or domain is different or not what you'd expect.
- ☑ The email is from someone you don't normally receive emails from, like the CEO.
- ☑ The email is from a vendor you don't work with or recognize.
- ☑ The request seems out of the ordinary or uncharacteristic.
- ☑ The list of addressees is empty or filled with names you don't recognize.
- ☑ The email includes a suspicious link or attachment.
- ☑ The attachment is of a file type you don't typically receive or don't recognize.
- ☑ The link, when hovered over, reveals a web address that's different.
- ☑ The hyperlink spelling is different than the expected spelling.
- ☑ The email includes nothing but long hyperlinks and no message.
- ☑ The email arrives outside of business hours or late in the day or on weekends.
- ☑ The subject line has nothing to do with the content of the email.
- ☑ The email addresses a request you never made or has nothing to do with you.
- ☑ The message has a sense of urgency or an alarming tone.
- ☑ The message hints at negative consequences if action isn't taken or unrealistic rewards if it is.
- ☑ The message refers to compromising information or pictures of you or people you work with.
- ☑ The email is poorly written, grammatically off or filled with typos or mistakes.
- ☑ The email as a whole feels off or your instincts tell you something isn't quite right.

So why would you hesitate?

We've got 18 reasons.

Barracuda®
Your journey, secured.