

Social Engineering *Red Flags*

FROM ●

- I don't recognize the sender's email address as someone I **ordinarily communicate with**.
- This email is from someone **outside my organization** and it's **not related to my job responsibilities**.
- This email was sent from someone inside the organization or from a customer, vendor, or partner and is very **unusual or out of character**.
- Is the sender's email from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

SUBJECT ●

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?

CONTENT ●

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click on a link or open an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at **compromising or embarrassing pictures** of myself or someone I know?

ATTACHMENTS ●

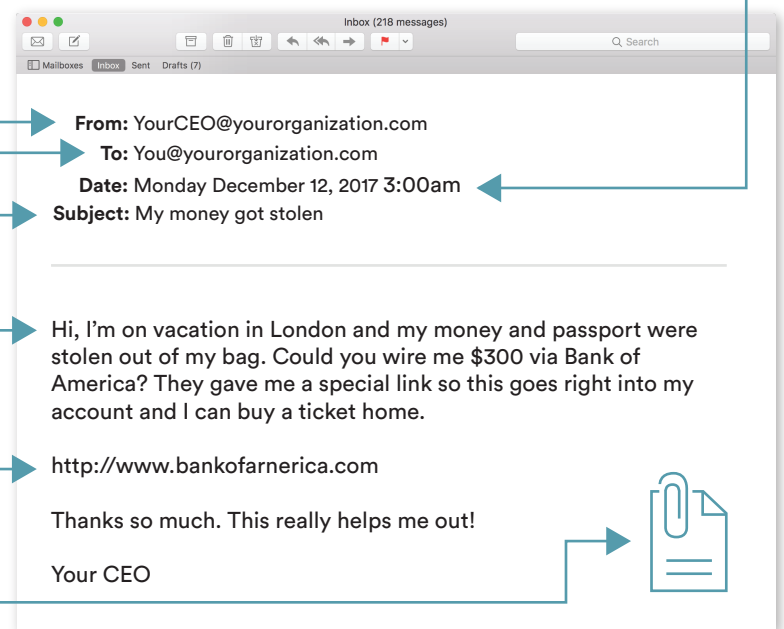
- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on** is a **.txt file**.

TO ●

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

DATE ●

- Did I receive an email that I would normally get during regular business hours, but it was **sent at an unusual time** like 3am?



HYPERLINKS ●

- I hover my mouse over a hyperlink that's displayed in the email address, but the **link-to address is for a different website**. (This is a **BIG** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that has a misspelling** of a known website. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n".