Social Engineering Red Flags

NBT BANK

FROM:
- I **don't recognize** the sender's email address as someone I normally communicate with.
- This email is **outside my job responsibilities and isn't from someone within the organization**.
- This email is **out of character** for someone inside or outside the organization.
- The sender's email address is a **suspicious domain**.
- I **don't know the sender personally** and neither do people I trust.
- I have **no business relationship** or **past communications** with the sender.

TO:
- The email was sent to others, but **I don't know them personally.**
- The email was sent to an **unusual mix of people**. (i.e. people whose last names start with the same letter or a random mix of email addresses)
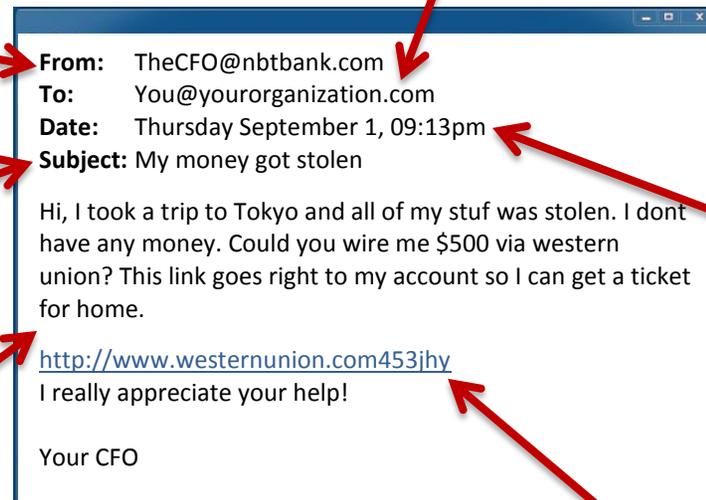
ATTACHMENTS:
- Their email contains an **embedded hyperlink** or **attachment**.
- The attachment **makes no sense** with the message and this person doesn't usually send me these attachments.
- The attachment has a **potentially dangerous file type**. (Only **.TXT files** are safe)

SUBJECT:
- The subject line is **irrelevant** to the message and **doesn't match** its content.
- The message is a reply to something that was **never requested**.

From: TheCFO@nbtbank.com
To: You@yourorganization.com
Date: Thursday September 1, 09:13pm
Subject: My money got stolen

Hi, I took a trip to Tokyo and all of my stuf was stolen. I dont have any money. Could you wire me $500 via western union? This link goes right to my account so I can get a ticket for home.

http://www.westernunion.com453jhy
I really appreciate your help!

Your CFO

DATE/TIME:
- The email was sent **outside of normal business hours** from someone you work with.

CONTENT:
- The sender is asking to click on a link to **avoid consequences** or **gain something of value**.
- The email has **grammatical or spelling errors**.
- The request to click a link or attachment makes me feel **uncomfortable**.
- The email asks me to look at an **embarrassing or compromising** picture of myself or someone I know.

HYPERLINKS:
- The hyperlink that displays in the email is **different** than the one that displays when the mouse is hovered over the link.
- The email contains **long hyperlinks with no further information**.
- The hyperlink is a known address that is **spelled incorrectly**. (ex. nbtbamk.com)