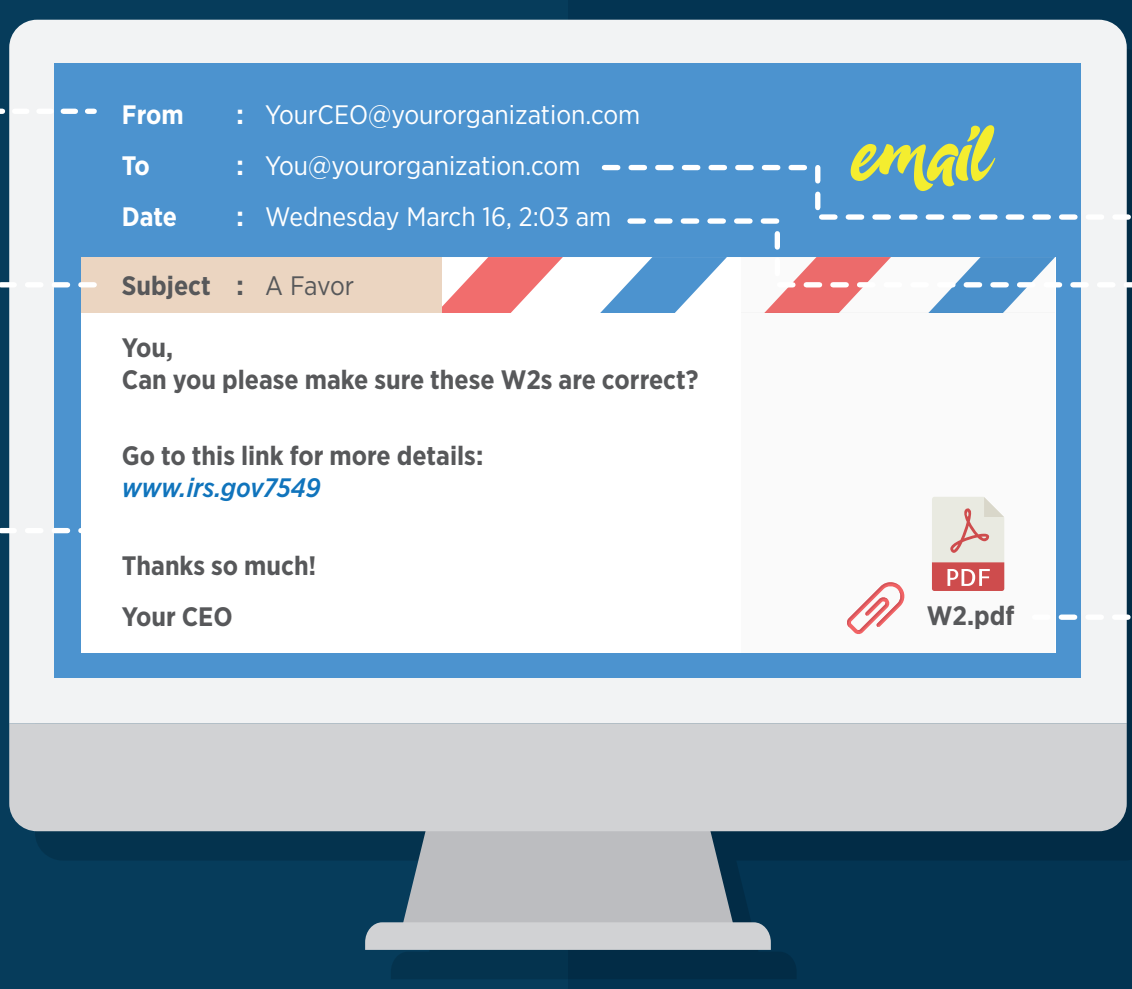
WHAT TO LOOK FOR IN A PHISHING SCAM



From

- I don't recognize the sender's email address – **especially ones from people with whom I regularly communicate.**
- This email is sent by someone **outside of my contacts and/or organization** and **does not pertain to my work.**
- This email was sent by **someone within my contacts and/or organization** (i.e., a team member, customer, vendor, or partner), but **is very unusual or out of character.**
- The sender's email address **contains a suspicious domain** (example: microsoft-support.com)
- I **don't recognize the sender.**
- The email is unusual or unexpected– containing an embedded hyperlink or attachment from someone

To

- I was cc'd on an **email sent to a group of people I don't know.**
- I received an email sent to an **unusual mix of people** – for instance, where everyone's last name starts with the same letter.

Date

- I received an email at an **unusual hour (like 2 a.m.)** that normally comes during business hours.

Subject

- Subject line is **irrelevant or does not fit the message's content.**
- Message is a **reply to an email I've never sent or seen.**

Attachments

- Sender included an **attachment I was not expecting.**
- The **attachment does not make sense** in context of the message.
- The sender **doesn't normally send me attachments.**
- The attachment has a **suspicious file extension** – the only file type always safe to click on is a .txt file.

Content

- The sender is asking me to open an attachment to **prevent something bad from happening or to get something valuable from me.**
- The email is strange – **poor grammar and spelling mistakes throughout.**
- The email asks me **to click on something that seems suspicious.**
- I have a gut feeling that the sender's **request is fishy?**
- The email asks me to look at **compromising or embarrassing information** about me or someone I know.

DYNAMIC EDGE, INC.
BEYOND TECH SUPPORT