

5 EMAIL SECURITY AWARENESS WARNING SIGNS

- 1 This email is from someone outside my organization and it's not related to my job responsibilities.
- 2 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.
- 3 Is the email message a reply to something I never sent or requested?
- 4 Do I have an uncomfortable gut feeling about the sender's request to open an attachment or click a link?
- 5 I hover my mouse over a hyperlink that's displayed in the email message, but the link-to address is for a different website. (This is a big red flag.)

5 SOCIAL ENGINEERING AWARENESS TIPS

- 1 Don't click on direct links (in emails, text messages, etc.), especially those that are asking you to enter sensitive information. It's best to go directly to the source.
- 2 Don't respond to phone requests asking for personal or financial information. If you are concerned, find the correct number and call the organization yourself.
- 3 Don't overshare on social media. These details can provide hackers with your location, ammunition to craft spear phishing attacks, and answers to security questions. Think before you share!
- 4 Be aware of your surroundings. Make sure you know who should and shouldn't be in your facility and that they've followed the requirements for entry.
- 5 Slow down. Most attacks convey a sense of urgency so pause and think about if what the person is asking for is legitimate.

5 PHISHING AWARENESS WARNING SIGNS

- 1 I don't recognize the sender's email address as someone I ordinarily communicate with.
- 2 I received an email that was also sent to an unusual mix of people. For example, a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.
- 3 Did I get an email with a subject line that is irrelevant or does not match the message content?
- 4 Is the email out of the ordinary, or does it have bad grammar or spelling errors?
- 5 Is the email asking me to look at a compromising or embarrassing picture of myself or someone I know?

5 CEO FRAUD

AWARENESS WARNING SIGNS

- 1 This email was sent from someone inside the organization or from a customer, vendor, or partner and is very unusual or out of character.
- 2 I received an email with a hyperlink that is a misspelling of a known web site.
- 3 Did I receive an email that I normally would get during regular business hours, but it was sent at an unusual time like 3 a.m.?
- 4 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?
- 5 I don't have a business relationship nor any past communications with the sender.

5 RANSOMWARE AWARENESS WARNING SIGNS

- 1 This is an unexpected or unusual email with an embedded hyperlink or an attachment from someone I haven't communicated with recently
- 2 I received an email that only has long hyperlinks with no further information, and the rest of the email is completely blank.
- 3 The sender included an email attachment that I was not expecting or that makes no sense in relation to the email message.
- 4 Is the sender asking me to click a link or open up an attachment that seems odd or illogical?
- 5 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.