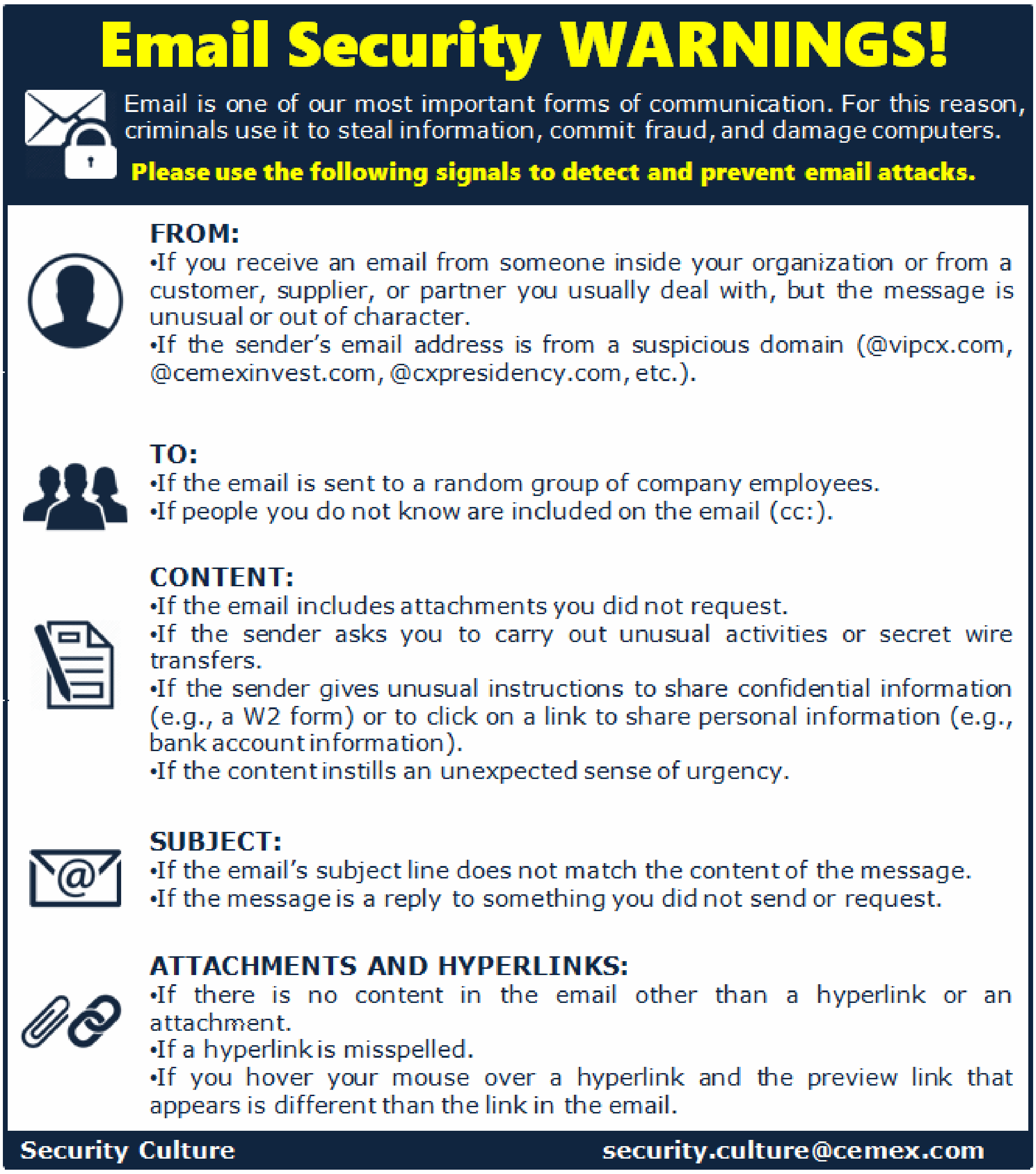

Email Security WARNINGS!

Email is one of our most important forms of communication. For this reason, criminals use it to steal information, commit fraud, and damage computers.

Please use the following signals to detect and prevent email attacks.

FROM:

- If you receive an email from someone inside your organization or from a customer, supplier, or partner you usually deal with, but the message is unusual or out of character.
- If the sender's email address is from a suspicious domain (@vipcx.com, @cemexinvest.com, @cxpresidency.com, etc.).

TO:

- If the email is sent to a random group of company employees.
- If people you do not know are included on the email (cc:).

CONTENT:

- If the email includes attachments you did not request.
- If the sender asks you to carry out unusual activities or secret wire transfers.
- If the sender gives unusual instructions to share confidential information (e.g., a W2 form) or to click on a link to share personal information (e.g., bank account information).
- If the content instills an unexpected sense of urgency.

SUBJECT:

- If the email's subject line does not match the content of the message.
- If the message is a reply to something you did not send or request.

ATTACHMENTS AND HYPERLINKS:

- If there is no content in the email other than a hyperlink or an attachment.
- If a hyperlink is misspelled.
- If you hover your mouse over a hyperlink and the preview link that appears is different than the link in the email.

Security Culture **security.culture@cemex.com**