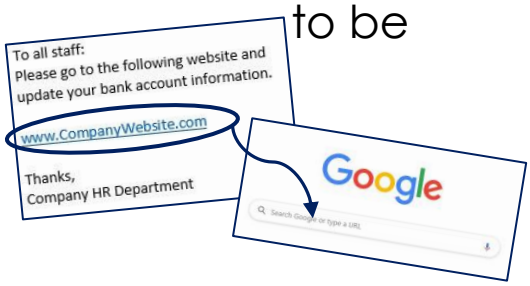
FBI suggestions for avoiding falling victim to a **Business Email Compromise** cyber attack

1

Use secondary channels (e.g. a phone call) to verify requests for payments and/or changes in account information

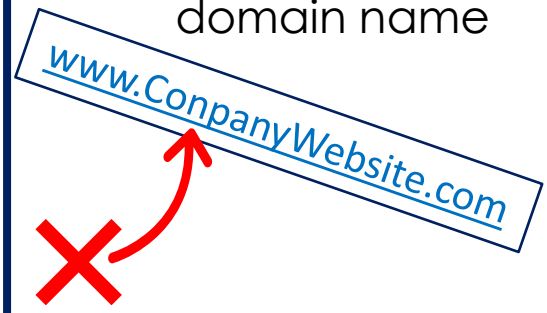
2

Ensure the URL in email is associated with the business from which it claims to be

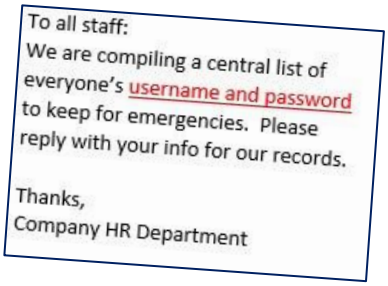


3

Be alert to hyperlinks that may contain misspellings of the actual domain name



4



Refrain from supplying login credentials or Personally Identifiable Information (PII) in response to any emails

5

Monitor personal financial accounts on a regular basis for irregularities, such as missing deposits

6

Perform software updates on all operating systems and software

7

Ensure that security awareness training stresses that employees should practice security techniques with email programs on their mobile devices (verify the email address of the sender, how to inspect URLs, etc.)

8

Adjust settings on employee computers so that they see the full file extensions on any attachments