Do you see what we see? Business Email Compromise

US$26 billion was lost to phishing between 2016 and 2019.

The number of BEC attempts — also known as

CEO FRAUD or WHALING

increased by 100%

have been reported

reached an average daily volume of 128,700

earliest 10 countries targeted by BEC fraudsters

- United States
- United Kingdom
- Australia
- Belgium
- Germany
- Canada
- The Netherlands
- Hong Kong
- Singapore
- Japan

Top keywords used in emails to catch recipients off guard (July 2018–June 2019)

- Top 10 keywords used in emails
  - Transaction request
  - Important
  - Urgent
  - Hospital
  - Payment

- of targeted BEC attempts were directed at generic email accounts, such as "sales@company.com"

Fraud can be hard to spot at times, but together, we can reduce the risk by following these simple steps.

Always check that the email address is spelled correctly, or hover your mouse over the email address to see the domain URL.

Never release any funds without verifying with the recipient. The best way to do this is to call them, but do not call using the number on the email.

If you suspect any fraud activity, report the incident to the bank or to your local authorities immediately. The quicker the fraud is reported, the higher the chances of recovery.

Sources:
1. Federal Bureau of Investigation, Business Email Compromise the $26 Billion Scam, 2019.

Don’t rely solely on software to keep you safe! Always check that the email address is spelled correctly, or hover your mouse over the email address to see the domain URL.

STOP SUSPICIOUS ACTIVITY

Never release any funds without verifying with the recipient. The best way to do this is to call them, but do not call using the number in the email.

REPORT THE INCIDENT

If you suspect any fraud activity, report the incident to the bank or to your local authorities immediately. The quicker the fraud is reported, the higher the chances of recovery.

www.sc.com/fightingfraud #DoYouSeeWhatWeSee