Fraud and Cyber Case Studies

Social Media CEO Impersonation

A CEO updates social media accounts noting that they will be speaking at an upcoming industry event.

Fraudsters notice the social media update and send the CEO's associates an email from the CEO, containing a link relating to the upcoming conference.

All associates that click on this link are unknowingly infected with malware.

Fraudsters use malware to collect information and transfer funds.

A CEO updates their social media accounts noting that they will be speaking at an upcoming industry event.

Using the compromised email addresses, the Fraudster sends emails to staff responsible for accounts payable a request to change vendor or supplier account details and to transfer funds.

Fraudsters notice this social media update. Fraudsters send the CEO's associates an email asking that they click on a link relating to the upcoming conference

All associates that click on this link are unknowingly infected with malware. The malware infection allows the hacker to compromise the email addresses of these associates.

Red Flags: Fraudulent emails – Verify the authenticity of all email addresses before responding; Hyperlinks – Always verify the source of the email before clicking on any links contained within an email.

citi.com/treasuryandtradesolutions

GRA28549 10/17