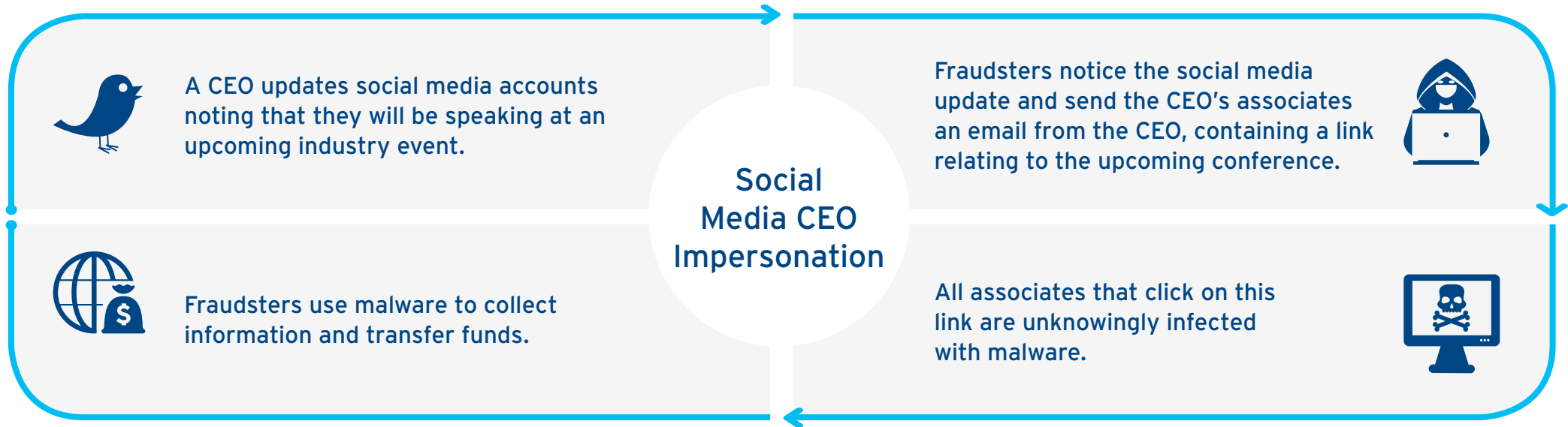


Fraud and Cyber Case Studies



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

© 2017 Citibank, N.A. All rights reserved. Citi and Citi and Arc Design are trademarks and service marks of Citigroup Inc. or its affiliates and are used and registered throughout the world. Citibank, N.A., is incorporated with limited liability under the National Bank Act of the U.S.A. and has its head office at 399 Park Avenue, New York, NY 10043, U.S.A. Citibank, N.A., London branch, is registered in the UK at Citigroup Centre, Canada Square, Canary Wharf, London E14 5LB, under No. BR001018, and is authorised and regulated by the Office of the Comptroller of the Currency (USA) and authorised by the Prudential Regulation Authority. Subject to regulation by the Financial Conduct Authority and limited regulation by the Prudential Regulation Authority. Details about the extent of our regulation by the Prudential Regulation Authority are available from us on request. VAT No. GB 429 6256 29. Ultimately owned by Citigroup Inc., New York, U.S.A.

GRA28549 10/17