Allied Solutions

Wednesday | January 18, 2023

Fraud Risk Bulletin

Exclusive, As-It-Happens Risk Updates and Insights

BUSINESS EMAIL COMPROMISE SUMMARY

Business email compromise is a sophisticated email tactic used to impersonate the CEO or other senior executive to scam employees – typically in accounting – to send a wire transfer, update bank account information, or provide account details.

This type of fraud is inexpensive to execute as it only requires a few minutes of the fraudster's time to research social media or the company's website. By stalking social media sites like LinkedIn, they have access to information employees may assume only an insider would know. Quickly perusing an executive's page can inform the hacker of an individual's travel plans, large company events, and that person's general manner of speaking. In return, the ROI is high as business email compromise relies on humans' innate desire to please their superiors.

HOW THE ATTACKS ARE PLOTTED

Sometimes referred to as 'CEO fraud attacks', hackers use spear-phishing methods to impersonate CEOs, COOs, or CFOs to invoke a sense of urgency and trick targeted employees who are attuned to upper-level executives contacting them directly. Using compromised email accounts, the hacker will create a sense of urgency, e.g., mentioning a company event or emulating a senior executive's communication patterns, to get the employee to act quickly.

RISK MITIGATION STEPS

- Pause and authenticate any interaction with an executive – or any employee – asking directly for funds.
    - Contact the person making the request in-person, with a phone number you have, or one obtained by human resources. Never rely on the phone number listed in the email.
    - Ask the next-level supervisor to review the request.
- Be wary of all email attachments and links, especially if the request is unexpected. Employees may not want to inconvenience upper management, but it's critical to ask for authentication before opening unfamiliar files.
- Use security technology fraud prevention platforms like anti-impersonation software, DNS authentication, and anti-malware programs to filter out the majority of attacks. There are also programs available that alert users if an email is received from outside your domain.
- Outline policies and procedures regarding emails requesting the transfer of money, a change to bank account information, vendor payments, or sending confidential data. These policies and procedures should be communicated to existing and new employees.
- Conduct security awareness training for all employees on a regular basis.

RISK MITIGATION RESOURCES

- FBI Business Email Compromise resource.
- Tap into knowledge from our experts by visiting our risk alerts library.
- Register for upcoming Let’s Talk Fraud educational webinars where Allied experts provide tools, tips and fraud prevention strategies to help safeguard your organization.

LinkedIn Twitter Facebook