Cybersecurity News

NEWS AND INFORMATION TO HELP PROTECT COMPANIES AND EMPLOYEES

APRIL 2021

MUFG CISO DISCUSSES CHALLENGES AND OPPORTUNITIES IN CYBERSECURITY

Chief Information Security Officer (CISO), **Devon Bryan** brings extensive cybersecurity experience to leading the security efforts at MUFG. In a new MUFG video, Devon addresses the following topics:

- Challenges faced by CISOs
- How CFOs can support CISOs
- What employees can do to support cybersecurity efforts
- Becoming a CISO

Visit Cybersecurity: A CISO's Thoughts - YouTube to view the third video in this series and learn more about Devon's thoughts and approach to cybersecurity.

"We have to make sure we are exercising the appropriate due diligence to keep our information and organization safe."

— Devon Bryan, CISO, MUFG

MOBILE DEVICE SECURITY GUIDELINES

Employee mobile device use increases productivity, but also presents security risks because the devices are used to access organizational data. Some organizations issue devices, while others enable employees to use their own devices. To help support greater security for sensitive data, the National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) (an agency of the U.S. Department of Commerce) provides mobile security practice guides for:

- Corporate-Owned Personally-Enabled (COPE) devices that are owned by the enterprise and issued to the employees
- Bring Your Own Device
- Cloud and hybrid models

In addition, NCCoE provides a mobile threat catalog of security controls and countermeasures that address mobile threats.

Source: National Cybersecurity Center of Excellence. *Mobile Device Security.* https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security.

(continued)

BEST PRACTICE: PROVIDE A CYBERSECURITY TOOLKIT

A strong security awareness program empowers employees to support an organization's cybersecurity efforts. One way to help set the tone and establish a cybersecure mindset is by providing a cybersecurity toolkit to managers and administrative assistants who can help lead security awareness during the employee and contractor onboarding and offboarding processes.

The cybersecurity toolkit can include:

- A cybersecurity overview
- An explanation of insider threat red flags with examples
- The role of the manager
- Guidelines for remote working
- Onboarding and offboarding checklists
- Examples of unusual activities and how to report them
- Key terms, points, and tips

MUFG Union Bank, N.A.
A member of MUFG, a global financial group

MUFG

BUSINESS EMAIL COMPROMISE (BEC) SCAMS: HOW TO IDENTIFY AND PREVENT LOSSES

BEC scam losses have continued to grow each year since the U.S. Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3) began tracking the scam in 2013. Losses have been reported in all 50 states and 177 countries.[1]

BEC fraud involves a fraudster hacking into an email account and impersonating the holder of the email account (e.g., CEO, CFO, attorney, business counterparty) to request a staff member who is authorized to instruct payments to transfer funds to the fraudster's account.

The fraudster typically requests the transfer using a format and language similar to genuine requests to make the fraudulent request appear credible.

If successful, it is often difficult or impossible to retrieve those funds because they are immediately moved elsewhere or withdrawn with little or no available audit trail or other trace of their ultimate destination.

Identifying BEC fraud

Indications of an attempted BEC fraud include, but are not limited to, the following:

- A request to transfer funds urgently, especially, but not always, near the end of the day (or payment cutoff time) or before a weekend or holiday.
- Pressure not to follow usual procedures.
- Instructions to keep the transfer confidential or secret.
- Transfers to bank accounts that have not previously received funds from the organization.
- Changes in the receiving bank account's details from prior transactions.
- Transfers to bank accounts in countries that have not previously (or with frequency) received funds from the organization.
- Transfers in currencies that are unusual for the transaction type or recipient's presumed location or country.

Preventing BEC fraud

Following are steps that can help protect against BEC fraud.

1. Review security measures

- Routinely check the internal information security environment. In many BEC scams, computers or entire data systems are hacked or infected with viruses or malware. Keep antivirus software updated and never reflexively open a link in an unexpected email or text.
- Communicate via secure methods (e.g., encrypted communication methods, password protected attachments with strong and unique passwords). Change passwords to systems frequently, using strong and unique passwords.

2. Confirm and consult

- Confirm requests received by email using an alternative communication method (e.g., communicate via telephone using contact details you have on file). Never use new contact details that come in the email requesting a transfer.
- When replying by email, do not use an automatic "reply" function. Instead, manually re-enter an email address you know to be correct (which is on file) in a new email thread. Fraudsters often use email addresses that appear identical but differ slightly from the correct one.
- Consult colleagues or staff cybersecurity professionals with any doubts about whether a transfer request is genuine, particularly in cases where the request is described as confidential or urgent.

3. Review the internal approvals framework

- Check that internal procedures for authorizing, sending, and executing fund transfer requests are as strong as they can be.
- Review the list of authorized staff to ensure staffing is sufficient to accommodate when some employees are absent.

BEC fraud is just one prominent type of payment fraud. There are many others. Fraudsters are using increasingly sophisticated techniques that include voice impersonation and other social engineering tricks to get staff members to share account security credentials and related details or otherwise exploit vulnerabilities in systems or procedures to accomplish their crimes.

[1] *Cyber Criminals Conduct Business Email Compromise through Exploitation of Cloud Based Email Services, Costing US Businesses Over Two Billion Dollars,* Federal Bureau of Investigation, Cyber Division. March 2020. https://www.ic3.gov/Media/News/2020/200707-4.pdf.

This *Cybersecurity News* contains news and information designed to help protect your company and employees.

8913482-M-Online (04/21)