RISK Alert

ACTIONABLE INSIGHTS FOR BOND POLICYHOLDERS.

CUNA MUTUAL GROUP

Alert Type: Awareness | **Watch** | Warning

Phishing Attacks and Business Email Compromise On The Rise

The 2021 cyber threat landscape was significantly more active across the board, including credit unions. In fact, 77% of organizations faced Business Email Compromise (BEC) attacks in 2021 according to a Proofpoint study (2022 State of the Phish) of more than 600 IT security professionals. BEC often includes payroll redirect, supplier invoicing fraud, and fraudulent wire instructions connected with credit union mortgage or lending departments.

Details

Cybercriminals have gone to great lengths to commit theft or fraud by manipulating credit union executives, employees, and even business members using fake, spoofed, or doctored emails, calls, and digitally-altered recordings. The surge of business email compromise (BEC) and fraudulent instruction scams typically request large wire transfers. These urgent requests often exceed $1 million.

A significant increase in fraudsters using credit union employee's emails to instruct staff to wire funds under the guise of paying vendors has been reported. In many instances, they appear to come from trusted vendors.

Additionally, more targeted attacks against credit union staff within the mortgage department have occurred. These bad actors are spoofing internal staff emails within the credit union's mortgage department requesting wire transfers to pay other financial institutions.

How It Begins

An employee's email is hacked, or computer is infected with malware which allows the fraudster access and change the receiving financial institution and beneficiary information. The email is sent to the wire department which results in the wire being executed and funds sent to the fraudster.

The BEC scam is frequently carried out when an individual compromises legitimate business or personal email accounts through social engineering or computer intrusion to conduct unauthorized transfers of funds. However, the scam is becoming more sophisticated.

BEC & Deepfakes

Between 2019 through 2021, the FBI IC3 has received an increase of BEC complaints involving the use of digitally-altered images, videos, webinars, or audio recordings (called deepfakes) through virtual meeting platforms to instruct victims to send unauthorized transfers of funds to fraudulent accounts. Criminals began using virtual meeting platforms due to the rise in remote work.

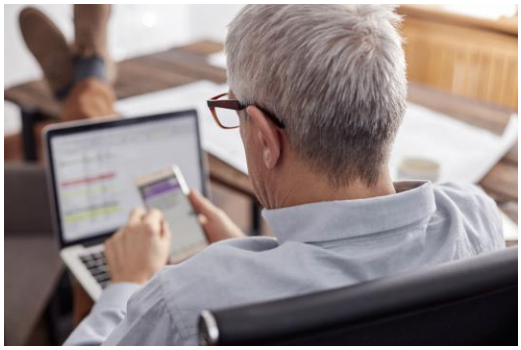
Date: March 8, 2022

Risk Category: Cyber; Cybersecurity; Business Email Compromise; Scams, Fraud; Phishing; Wire Transfers; Lending

States: All

Share with:

- ☐ Executive Management
- ☐ IT
- ☐ Loan Manager
- ☐ People Leaders
- ☐ Risk Manager
- ☐ Transaction Services



Facing risk challenges?

Schedule a free personalized discussion with a Risk Consultant to learn more about managing risk.

Phishing Attacks and Business Email Compromise On The Rise

The most common type of BEC attack is spoofed email account (71%) followed by spear phishing at 69% according to the 2021 Business email compromise report by Cybersecurity Insiders.

Red Flags

Both fraudulent instruction and BEC scams often focus the request as "urgent" or "pay immediately" in hopes that the employee does not take time to scrutinize the request. In addition to the urgency of the message, some red flags include:

- Request to keep transaction confidential
- Communication only through email and refuses other communication channels
- Requests change in direct deposit information or for payments to be made to a different account
- Requests typically come from a high-level executive or authority within your organization
- Requests often coincide with requestor being out-of-the-office as the fraudster has accessed calendars

Risk Mitigation

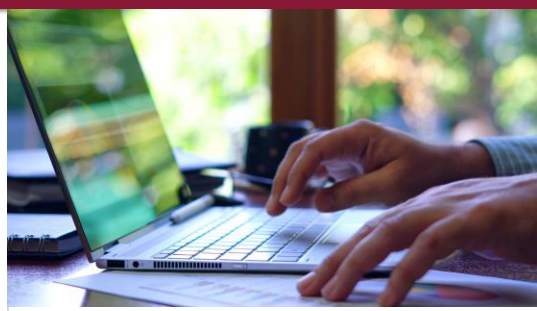
Credit unions should consider these mitigation tips:

- Train staff on BEC and fraudulent instruction scams, including how to protect their email and credentials
- Avoid sharing credit union organizational structure and emails on public websites
- Establish procedures to call the title company / closing agent using a reliable phone number to verify the legitimacy of wire transfer instructions
- Require staff to follow established procedures for handling internal wire transfer requests
- Confirm the legitimacy of the request by verifying with the C-suite executive
- Authenticate requests using a different communication (out-of-band) channel such as verifying face-to-face or calling the requestor's phone extension or cell phone
- Have an alert on all incoming emails that originate outside of your credit union such as: Caution: this email originated from outside your organization. Do not click links or attachments unless you recognize the sender and know it is safe
- Limit the number of staff that have authority to perform or approve wire transfers
- Provide ongoing staff training with penetration testing

Risk Prevention Resources

Access CUNA Mutual Group's Protection Resource Center at cunamutual.com for exclusive risk and compliance resources to assist with your loss control efforts. The Protection Resource Center requires a User ID and password.

- Wire Transfer Risk Overview
- Fraud & Scams eBook
- Call Center Fraud Risk Overview
- Business Email Compromise Risk Overview
- RISK Alert: Preparing For The Risk of Deepfakes



Access the Protection Resource Center for exclusive resources:

- Loss Prevention Library for resources & checklists
- Webinars and Education
- RISK Alerts Library
- Report a RISK Alert

The Protection Resource Center requires a User ID and Password.

FinCEN Program Assists Recovery

The Financial Crimes Enforcement Network (FinCEN) recently issued a Fact Sheet (FIN-2022-FCT1) on its Rapid Response Program (RRP) and how it assists victims and their financial institution recover stolen funds from cyber-related crime, including BEC.

Credit unions incurring a loss from the BEC scam, including the related scam involving fraudulent wire instructions for real estate closings should immediately file a complaint with the FBI at IC3.gov or contact the nearest USSS field office. If a member incurs a loss involving their personal funds involving fraudulent wire instructions for real estate closings, instruct the member to file a complaint.