ALERUS

FREE DOWNLOADABLE GUIDE:

PROTECTING YOUR BUSINESS FROM BUSINESS EMAIL COMPROMISE (BEC) FRAUD

BEC fraud is a significant threat to companies of all sizes. This guide is designed to help you safeguard your business by identifying and preventing BEC scams. Follow these steps to ensure your company is protected.

Verify All Email Requests

- **Double-check the sender's email address —** Look closely at the sender's email address. Is it exactly the same as the one you've used before? Watch out for small changes, such as an extra letter or a different domain name.
- **Confirm requests for payment or sensitive information —** Use a known phone number to contact the person requesting payment or sensitive information. Do not reply directly to the email.
- **Be wary of urgent requests —** If the email stresses urgency or pressures you to act quickly, take extra caution. This is a common tactic used in BEC fraud.

Educate Your Employees

- **Regular training on BEC scams —** Schedule regular training sessions for your employees on how to recognize and respond to BEC scams.
- **Implement clear procedures for handling emails —** Establish protocols for verifying email requests, especially those related to financial transactions or sensitive data.
- **Encourage a culture of caution —** Encourage employees to report suspicious emails without fear of repercussions. Better safe than sorry.

Strengthen Your Email Security

- **Implement multi-factor authentication (MFA) —** Require MFA to access email accounts, adding an extra layer of security.
- **Regularly update passwords —** Ensure all employees update their email passwords regularly and use strong, unique passwords.
- **Monitor for suspicious activity —** Regularly review email account activity for any signs of unauthorized access or unusual behavior.

Establish Financial Transaction Protocols

- **Use a multi-person approval process —** Require multiple approvals for significant financial transactions, especially those involving wire transfers.
- **Limit who can request and authorize payments —** Restrict who has the authority to request and approve financial transactions to minimize risk.
- **Verify changes in payment instructions —** Always confirm changes to payment instructions with the vendor or client directly through a known, trusted contact.

Respond Quickly to Suspicious Activity

- **Contact your bank immediately —** If you suspect BEC fraud, contact your bank as soon as possible to attempt to recover funds.
- **Report to authorities —** Report the fraud to the FBI's Internet Crime Complaint Center (IC3) and cooperate with law enforcement.
- **Secure your accounts —** Change passwords for compromised accounts and review account activity for any unauthorized actions.

08.26.2024

What to Do if You've Shared Sensitive Information

- **Contact Alerus immediately —** Reach out to Alerus to secure your accounts if you've accidentally shared sensitive information.
- **Monitor your accounts —** Keep a close eye on your accounts for any unauthorized transactions.
- **Report a compromised card —** If you've shared your card number, call the number on the back of the card and report it as potentially compromised.

Stay Informed and Vigilant

- **Subscribe to cybersecurity alerts —** Stay updated on the latest BEC fraud tactics and threats by subscribing to cybersecurity alerts and bulletins. https://www.cisa.gov/about/contact-us/subscribe-updates-cisa
- **Regularly review security practices —** Periodically review and update your company's security protocols to stay ahead of potential threats.
- **Encourage open communication —** Foster an environment where employees feel comfortable discussing potential security concerns or reporting suspicious emails.