Protecting Your Business from Cyber Fraud

CADENCE Bank

Company-Wide Education and Awareness are Your Best Defense

Every business is vulnerable to fraud. As the world grows more dependent on digital efficiencies, each company's defense must be equally reliable and nimble to combat fraud. Beware that the awareness level of your personnel is a major risk factor.

Your employees remain constant targets for cyberattacks, especially via Business Email Compromise (BEC), a type of scam in which the attacker gains access to a corporate email account and poses as the CEO or another authority figure to defraud the company of money.

> **In 2021, the Internet Crime Complaint Center (IC3) reported 19,954 Business Email Compromise complaints with losses of approximately $2.4 billion.**
>
> *– Federal Bureau of Investigation Internet Crime Complaint Center (IC3)*

This pervasive form of fraud can result in wire transfer fraud, whereby finance employees unknowingly transfer money to an account controlled by the fraudster. All it takes is a single human error.

Take action to educate yourself and your personnel about fraud prevention and exercising sound judgment. Use these essential tips to protect your company and prepare your personnel before cyber thieves strike.

Instant & Irreversible

Wire transfers are an immediate form of payment. Once a scammer has obtained the wired funds, the transfer most likely cannot be reversed.

KNOW THESE MOST COMMON BEC TACTICS

Spot the warning signs of a scam or scammer before it's too late.

Trigger Words in Subject Lines

Beware of words such as request, payment, transfer and urgent – these are often a fraudster's first hook.

CEO Fraud

Via email, fraudsters pose as the company CEO or other high-ranking executive requesting employees transfer money to an account they control.

Fake Invoice

Attackers pretend to be suppliers requesting fund transfers for payments to an account owned by fraudsters. Companies with foreign suppliers are often targeted with this email tactic.

Tips To Protect Your Business: Prevent Fraud with Smarter Systems

Positive Pay

Protect yourself from check fraud by sending a daily file of issued checks, reviewing checks paid to your account that did not match the issuance file, and returning fraudulent or unauthorized checks.

ACH Positive Pay

Review incoming debits and return unauthorized items before they are deducted from your account.

Dual-Factor Authentication

Implement dual-control authentication, meaning one employee initiates a wire transfer and another employee approves the same wire transfer.

KNOW THESE MOST COMMON BEC TACTICS

Account Compromise

Attackers hack into an executive's or employee's email account, using it to request invoice payments to vendors listed in their email contacts. Payments are then sent to fraudulent bank accounts.

Attorney Impersonation

Posing as a lawyer or a law firm employee, fraudsters claim to need sensitive information, such as 'verifying' the bank account from which settlement funds are to be withdrawn. These bogus requests often happen at the end of the day and may occur by phone.

Data Theft

This info-gathering tactic targets HR and bookkeeping employees. Attackers use deceptive emails (or phone calls) to obtain personally identifiable information (PII) or tax statements of employees.

Cyber Safety Industry Best Practices for Personnel

Verbally Verify

- Treat every email request you receive with payment instructions as potentially fraudulent until verified.
- Call the customer who initiated the request via phone using a number from within your company's database. Do not call the phone number in the email.
- Confirm every aspect of every transaction, including ABA and account number, even if the request seems authentic.

Don't Recognize the Sender?

- Avoid clicking on links or opening attachments.
- Don't reply to the email – it could be a fraudster.
- Report the email to IT or Information Security.

What to Do if Your Company is a Victim of a Cybercrime

If you believe your business is the recipient of a compromised email or a victim of a BEC scam:

- Notify your bank right away to request a recall or reversal as well as a Hold Harmless Letter or Letter of Indemnity.
- File a comprehensive complaint with the Internet Crime Complaint Center (IC3) at www.IC3.gov. Be descriptive, complete all required data fields, and identify your complaint as "Business Email Compromise" or "BEC."
- Visit www.IC3.gov for updated PSAs about BEC trends and other fraud schemes.

FRAUD AWARENESS CAN PROTECT YOU

That's why the Cadence Bank team is dedicated to helping your company and personnel fight fraud effectively.

For more information, contact Treasury Management Client Support.

Call 1-800-329-0289 or email us at treasurymanagement@cadencebank.com.

CADENCE Bank

CadenceBank.com/Treasury-Management