Fraud Alert!

Business employees are being tricked by cyber criminals into wiring money. It's called "business email compromise" and it's today's most prevalent business scam.

Scenario 1: An employee receives an email, seemingly from the CEO or CFO, directing a wire payment. The employee isn't aware that the email is not legitimate and wires the funds.

Scenario 2: Accounting updates its vendor payment records with new payment instructions based on an email. Accounting doesn't realize that the email is not legitimate and wires the funds.

Either way, your business has been tricked and the money is gone. To protect your business and reduce your risk, you must educate your employees. And **act quickly** if you suspect anything is wrong.

Contact your Relationship Manager or

EagleBank Information Security Office
301.281.8050
TheSOC@EagleBankCorp.com

EagleBankCorp.com
301.986.1800

MD | VA | DC

05/20

EQUAL HOUSING LENDER
Member FDIC

For a complete listing of our locations, please visit EagleBankCorp.com

EAGLEBANK

EAGLEBANK

CYBERSECURITY TIPS

Business Email Compromise

What is business email compromise?

It's the work of cyber criminals who hack and hijack business email accounts—typically, but not exclusively, those of CEOs/CFOs—to send bogus emails. Cyber criminals research your business and perhaps infiltrate compromised personal email that may have been used for work purposes (or for convenience). They look for information such as travel plans and other facts about the business.

Cyber criminals often operate when the CEO/CFO is out of town or out of the country and not available in person to verify any bogus internal email payment instructions. Even if the CEO/CFO is emailed back to confirm payment, responses will actually be coming from the cyber criminal, since the email has been hijacked. It can happen at any time—unless employees are cautious and verification procedures are in place.

WHAT ARE SOME OF THE METHODS CYBER CRIMINALS USE?

- Hijacking business email accounts using relatively unsophisticated methods and tools.
- Manipulating email or creating commands that automatically send fraudulent emails to a trash folder or to a hidden folder so they are not visible to the true email account user.
- Sending wire transfer instructions when the CEO/CFO is on official travel, making it more likely that email would be used for official business and, therefore, harder to identify the transaction as fraudulent.
- Marking the wire transfer request as urgent or confidential, stating that it must not be discussed with other company personnel.
- Setting up new website and email addresses that appear almost identical to legitimate business addresses (for example, changing a single letter).
- Directing payments to vendors/suppliers to go someplace else: to the cyber criminals' accounts or to different addresses.

Awareness, vigilance, and adherence to strict verification procedures can greatly reduce your risk of being victimized by cyber criminals.

REDUCE RISKS TO YOUR BUSINESS

- **Look** for any small change to any payee's information and verify it by calling the vendor or supplier to verbally confirm the change, using a phone number from a known contact list.
- **Limit** the number of employees within a business who have the authority to approve and/or conduct wire transfers.
- **Require** dual-approval, generally for wires, but at a minimum for any monetary transactions involving (1) a dollar amount over a specific threshold, (2) new wire beneficiaries, (3) new banks for current beneficiaries, or (4) wire transfers to countries outside the norm.
- **Take** full advantage of security features offered by the bank, including dual controls, dollar limits, notifications, etc.
- **Verify** via phone or in person any email requests involving monetary transactions, even those that are seemingly coming from legitimate sources.
- **Instruct** staff to delay approval of transactions when contacted by the bank with questions about a transaction, so that additional verification within the business can be performed.

TIME IS CRITICAL

If you suspect that your business email may be compromised, **act quickly!**

- Follow your company's incident response procedures.
- Immediately change any passwords that may have been revealed. If you used the same password for multiple resources, make sure to change it for each account and do not use that password in the future.
- Notify the bank and close any accounts that may have been compromised. Watch for inexplicable charges to your account(s).
- Notify law enforcement immediately.

WHOM SHOULD I NOTIFY?

- **FBI:** www.fbi.gov/contact-us/field-offices
- **Secret Service:** www.secretservice.gov/contact/field-offices
- **Internet Crime Complaint Center:** www.IC3.gov

When reporting, be prepared to provide a description of the crime, how it occurred, losses experienced, and your business wiring/ACH instructions.

BE PROACTIVE

Train all employees on social engineering and phishing tactics.

- **Install and maintain anti-virus software, firewalls, and email filters** to reduce some of this traffic, and take advantage of security features offered by your email client and web browser, such as anti-spam and anti-phishing options.
- **Check and use available guidance from official government sources** such as the FTC (www.consumer.ftc.gov/blog/been-hacked-or-hijacked-read). Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group (www.antiphishing.org).
- **Do not send sensitive information over the Internet** without checking that the address starts with "https" and includes a padlock icon so that you know your information is being sent securely.
- **If you are unsure whether an email request is legitimate,** try to verify it by contacting the apparent sender directly—but do not use contact information provided on the website connected to the request or in the email signature. Instead, check previously verified contact information.
- **Be suspicious of unsolicited phone calls, visits, or email messages** from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity by calling a known number or a contact there directly.
- **Pay attention to the addresses of websites and emails.** Malicious websites and email addresses may look identical to a legitimate site, but the address may use a minor variation in spelling or a different domain.
- **Do not provide personal information or information about your business,** including its structure or networks, unless you are certain that the person making the request is authorized to have the information.
- **Do not reveal personal or financial information in an email,** and do not respond to email solicitations for this information. This includes following links sent in emails that entice you to reveal such information.
- **Avoid using personal email addresses for work purposes;** these generally have poor security controls.