FRAUD ALERT!

It's called "business email compromise," and it's today's most prevalent business scam.

Scenario 1:

An employee receives an unvalidated email from the CEO or CFO, directing a wire payment.

Scenario 2:

Accounting updates its vendor payment records with new payment instructions based on an unvalidated email.

Either way, the money is gone. To protect your business and reduce risk, educate your employees and act fast if anything is suspect.

Contact your Relationship Manager or

EagleBank Information Security Office
301.281.8050
TheSOC@EagleBankCorp.com

EagleBankCorp.com
301.986.1800

MD | VA | DC

10/22

Member FDIC

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

EAGLEBANK

CYBERSECURITY TIPS

BUSINESS EMAIL COMPROMISE

EAGLEBANK

WHAT IS BUSINESS EMAIL COMPROMISE?

It's the work of cyber criminals who hack and hijack business email accounts at the executive level.

Cyber criminals often operate when the CEO/CFO is 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 be coming from the cyber criminal, since the email has been hijacked.

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 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.
- 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, changing a single letter, for example.
- Directing payments to vendors and/or suppliers to go someplace else.

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 payee's information and verify the change by calling the vendor or supplier directly.
- Limit the number of employees within a business who have the authority to approve and/or conduct wire transfers.
- Require dual approval 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 can be performed.

Time is critical

If you suspect that your business email may be compromised, it likely is. Time is critical.

1. Follow your company's incident response procedures.
2. Immediately change any passwords that may have been revealed.
3. Notify the bank and close any accounts that may have been compromised. Watch for inexplicable charges to your account(s).
4. Notify law enforcement immediately.

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 (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 (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, using previously verified contact information.
- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information.
- 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.
- Avoid using personal email addresses for work purposes.

Whom Should I Notify?

- **FBI** [fbi.gov/contact/fo/fo.htm]
- **Secret Service:** [secretservice.gov/contact/field-offices]
- **Internet Crime Complaint Center:** [IC3.gov]

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