Comerica Bank

comerica.com

Fraud Awareness: Business Email Compromise Cyber Scam

Did you know that the majority of businesses consider fraud protection a top priority and have stepped up their protection strategies and internal awareness training? Awareness may help save your business from becoming the next victim of a sophisticated cyber scam called Business Email Compromise (BEC). It's happening daily, involving seemingly harmless, routine email requests.

How Business Email Compromise Works

Based on findings from the Internet Crime Complaint Center (IC3) that has been tracking grievances about this cybercrime for months (click here to review the entire article), there are generally three versions of this scam:

Version 1 – Email appears from a legitimate supplier asking for payment to a new account number

- A business, which often has a long standing relationship with a supplier, is asked to wire funds for invoice payment to an alternate, fraudulent account. The request may be made via telephone, facsimile or email.
- In an email received by the business, the fraudster will spoof the email request so it appears very similar to the legitimate account used to ask for payment in the past. It would take very close scrutiny to determine it was fraudulent. Review the complete addresses shown here. Can you detect the difference?

From: john_smith@rickymasonllc.net To: sam_johnson@globaltech.com	From: john_smith@rickiymasonllc.net To: sam_johnson@globaltech.com

Version 2 – Employee gets an email from who they think is the boss or other authorized person in the organization, asking for a wire to be sent

- The email accounts of high-level business executives (CFO, CTO, etc.) are compromised (spoofed or hacked). A request for a wire transfer from the compromised account is made to a second employee within the company who is normally responsible for processing these requests. The wire transfer includes instructions to urgently send funds.

Version 3 – Supplier or vendor receives email they think is from you, asking for payment

- Requests for invoice payments to fraudster-controlled bank accounts are sent from this employee's personal email (after their personal or company email account is hacked) to multiple vendors identified from this employee's contact list.
- The business may not become aware of the fraudulent requests until they are contacted by their vendors to follow up on the status of their invoice payment.

Protection Suggestions

The Internet Crime Complaint Center (IC3) and Comerica Bank have numerous protection and best practice suggestions that will help you protect, prepare and respond should your business become a victim of a BEC scam or any cyber incident:

Awareness is Your First Line of Defense

- Anyone can learn more about cyber security by accessing Comerica's five online learning modules. If you haven't viewed them yet, you're missing out! Suggest all your employees review them; Click here to open Cyber Security 101 available on comerica.com.
- Review Comerica informational handout "Cyber Awareness Best Practices for Businesses" by clicking here. Schedule a meeting with key financial personnel at your business to ensure they are complying with the best practices.
- Any Internet-connected organization can fall prey to a disruptive network intrusion or costly cyberattack. A quick, effective response to cyber incidents can prove critical to minimizing the resulting harm and expediting recovery. Click here to review this online document presented by the Department of Justice to learn about the latest methods for responding to and reporting cyber incidents.

Fraud Awareness: Business Email Compromise Cyber Scam

Make it Difficult for a Fraudster

- Establish a company website domain (avoid free web-based email; e.g., Hotmail™, Yahoo™) and use it to establish company email accounts.
- Be careful about what is posted to social media and company websites, for example: Determine if it's necessary to disclose job duties/ descriptions, hierarchal information, out-of-office details, direct phone numbers and email addresses.
- Consider additional IT and financial security procedures and 2-step verification processes. For example:*
  - **Important** – establish other communication channels within your company and with your business partners, such as telephone calls, to verify significant transactions.
  - Immediately delete unsolicited email (spam) from unknown parties. Do NOT open spam email, click on links in the email or open attachments. These often contain malware that will give subjects access to your computer system.
  - Do not use the "Reply" option to respond to any business e-mails. Instead, use the "Forward" option and either type in the correct email address or select it from the email address book to ensure the intended recipient's correct email address is used.
- Beware of sudden changes in business practices. For example, if a current business contact suddenly asks to be contacted via their personal email address when all previous official correspondence has been on a company email, the request could be fraudulent.

When to Contact Comerica

Ask questions – Cybercrimes are constantly changing, so software and fraud prevention tools have to change as well. Education and awareness of all employees is the first line of defense, but you may also want to determine if you are taking advantage of all the fraud solution options that Comerica offers. We are here to help:

To learn more about strategies and solutions that can help you protect your organization and yourself against fraud, contact your Treasury Management representative or Treasury Management Services at 888.341.6490.

Report suspicious activity – Make sure your employees know how and to whom to report suspicious activity within your company and with accounts at your financial institution. Immediately contact your financial institution if you notice unauthorized activity, your computer performance changes significantly or you receive an unexpected request for a one-time password, token or other information during an online session.

Notify us immediately if you discover any unauthorized or unusual activity involving your Comerica accounts.

Treasury Management customers: Contact Treasury Management Relationship Services at 800.852.3649.

All others: Contact your Comerica relationship manager or the nearest Comerica banking center.

*The foregoing suggestions are for informational purposes only. These suggestions are not intended nor should they be used as an exclusive list of potential solutions aimed at the detection and prevention of cyber-crime and related fraud risks. Comerica is not an information technology expert and is not offering specific information technology or other computer systems advice. Accordingly, you and your company should consult your own computer systems or information technology expert(s) to adequately address any and all issues relating to cyber-crime detection and prevention including, without limitation, any potential computer or systems infection, viruses or malware.