Texas Capital Bank

The Rise and Risk of Business Email Compromise (BEC)

Business Email Compromise schemes are becoming an increasing threat to companies everywhere. We recommend that organizations employ policies and technology to protect themselves.

Business Email Compromise occurs when an attacker places himself in the middle of business email communication, poses as a trusted colleague, and sends a bogus message to another employee. Using an email address and signature block that is nearly identical to authentic emails that come from the supposed sender, hackers instruct the employee to conduct banking transactions. Requests usually involve sending wires to the attacker's account.

These types of security breaches are on the rise and result in significant losses. The stolen money is often sent overseas to criminal accounts and may never be recovered.

What you can do to protect your company from BEC

We encourage you to establish an internal check and balance system to help ensure that employees do not respond to fraudulent emails. Practicing good security habits can help protect your company's assets and private information from the rising threat of BEC. As part of an overall fraud protection program, we recommend the following:

- *Pay special attention to changing payment types and instructions.*
- Perform call-back verification for any financial transaction requested by email or text message from a colleague
- Require internal dual approvals for financial transactions
- Set reasonable transaction limits for employees
- Install perimeter spam and malicious-content filtering on all business computers
- Conduct security awareness training with regularity
- Remind employees to exercise extreme caution when asked to divulge account information or banking credentials

What to do if you detect BEC

In the event of a compromise, notify the bank and law enforcement as soon as the breach is discovered—***fast notification is critical***!

No organization is immune from either internal or external fraud. It is imperative that you take preventative measures utilizing both technology and best practices.

CONTACT US

Consisting of former law enforcement and IT security experts, our dedicated staff of fraud and security experts is available to answer questions or provide additional advice on fraud protection best practices.

Contact your Relationship Manager or Treasury Sales Officer for more information.

Texas Capital Bank is a wholly owned subsidiary of Texas Capital Bancshares, Inc. We are headquartered in Dallas, Texas, and work with clients across the country. All services are subject to applicable laws, regulations and service terms.