

# Protect Your Organization from Business Email Compromise (BEC)

## What is Business Email Compromise (BEC)?

Business Email Compromise (BEC) is a type of cyber attack where attackers gain access to a business email account and use it to deceive employees, customers, or partners into transferring money or sensitive information.

## Common Signs of BEC



### Suspicious Email Characteristics:

- Unusual sender address (e.g., john.doe@c0mpany.com)
- Urgent or unusual requests for action
- Unexpected attachments or links



### Behavioral Red Flags:

- Change in communication style
- Requests for confidential information
- Emails sent at odd hours



### Technical Indicators:

- Spoofed email addresses
- Reply-to address mismatch
- Email header anomalies



### Financial Red Flags:

- Changes in payment instructions
- Requests for large transfers

## How to Prevent BEC



### Technical Measures:

- Implement Multi-Factor Authentication (MFA)
- Use advanced email filtering solutions
- Encrypt sensitive emails
- Regularly update software



### Contact Us:

**Cyber Loss Control**  
cyberlosscontrol@gaig.com



#### **Employee Training:**

- Conduct phishing awareness training
- Establish verification procedures for financial transactions
- Encourage reporting of suspicious emails



#### **Policies and Procedures:**

- Implement email authentication protocols (DMARC, DKIM, SPF)
- Limit access to sensitive information
- Develop an incident response plan



#### **Monitoring and Auditing:**

- Conduct regular audits of email accounts
- Use continuous monitoring tools

## **Stay Vigilant**

By recognizing the signs of BEC and implementing these preventive measures, you can protect your business from significant financial and data losses. Educate your employees and stay proactive in your cybersecurity efforts.

Cyber loss control consultation services are provided by Great American Insurance Company and its affiliates to assist management of insured firms in fulfilling their responsibilities for the control of potential loss producing situations involving their information technology and/or operations. The information provided is intended to provide guidance and is not intended as a legal interpretation of any federal, state or local laws, rules or regulations applicable to your business. The cyber loss control information provided is intended only to assist policyholders in the management of potential loss producing conditions involving their information technology and/or operations based on best practices around cybersecurity controls. In providing such information, Great American does not warrant that all potential hazards or conditions have been evaluated or can be controlled. It is not intended as an offer to write insurance for such conditions or exposures. The liability of Great American Insurance Company and its affiliated insurers is limited to the terms, limits and conditions of the insurance policies underwritten by any of them. Great American Insurance Group, 301 E. Fourth St., Cincinnati, OH 45202. © 2025 Great American Insurance Company. All rights reserved. 0089-CBR (01/25).