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

GREAT AMERICAN INSURANCE GROUP
Cyber Risk

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.

GREAT AMERICAN INSURANCE GROUP
Cyber Risk