# HOW TO

# Prevent and Respond to Business Email Compromise

## WHAT IS BUSINESS EMAIL COMPROMISE (BEC)?

BEC is a sophisticated cyber scam where attackers use email to impersonate trusted individuals—such as mayors, finance officers, or vendors—to deceive employees into:

- ☑ TRANSFERRING FUNDS TO FRAUDULENT ACCOUNTS
- ☑ SHARING CONFIDENTIAL INFORMATION
- ☑ CHANGING PAYROLL OR VENDOR PAYMENT DETAILS

## HOW BEC ATTACKS HAPPEN?

1. **Email Account Compromise** – Criminals hack or spoof an official email account.
2. **Social Engineering & Impersonation** – Attackers pose as trusted contacts (supervisors, vendors, or government officials).
3. **Urgent, Deceptive Requests** – Emails pressure recipients to bypass verification and act quickly.
4. **Funds or Data Theft –** Money is wired to fraudulent accounts, or sensitive data is stolen for future fraud.

## BEST PRACTICES TO PREVENT BEC

- ☑ **Verify All Payment Requests** – Always confirm changes to wire instructions or payments with a phone call using a known, trusted number.
- ☑ **Train Employees to Spot Phishing** – Educate staff on red flags like urgency, unfamiliar senders, and unexpected attachments.
- ☑ **Use Email Security Tools** – Enable anti-phishing software, domain authentication (DMARC, DKIM, SPF), and fraud alerts.
- ☑ **Implement Multi-Factor Authentication (MFA)** – Require MFA for email, financial systems, and critical accounts.

## WHAT TO DO IF YOU ARE TARGETED

1. **Call the Bank Immediately** – Attempt to freeze or reverse fraudulent transactions.
2. **Report the Incident** – Notify IT, finance personnel, law enforcement, NYS DHS, and the FBI's IC3 (Internet Crime Complaint Center).
3. **Secure Systems** – Disconnect affected accounts, change passwords, and review access logs.
4. **Preserve Evidence** – Keep fraudulent emails, transaction details, and any communications.
5. **Inform Stakeholders** – Notify employees, vendors, and partners to prevent further fraud attempts.
6. **Investigate & Strengthen Controls** – Assess vulnerabilities and update policies to prevent future attacks.

**WE ARE HERE TO HELP**

For any questions or additional support, contact our Cyber Risk Specialist, Elisabeth Dubois, Ph.D.
Phone: 518-949-0127 | Email: edubois@wrightinsurance.com