Protect Your Business

AGAINST BUSINESS EMAIL COMPROMISE (BEC)

BEC is a sophisticated scam targeting businesses that regularly perform wire and ACH transfers. The scam is not particular in terms of specific business sectors and/or size of the business.

Criminals research organizations, and track key executives (CEOs/CFOs) in order to learn their email styles. Once able to successfully mimic the communication style, a criminal can succeed in reaching and deceiving employees via email. Employees are prompted to transfer funds to a fraudulent account, unaware that they are being scammed.

BEC BY THE NUMBERS

$2.4B
BEC attackers made **$2.4 billion globally** in 2021

15%
of employees **responded to malicious BEC** attempts

81%
increase in **BEC attacks** in 2022

THE ART OF DECEPTION

The organized criminal groups that engage in business e-mail compromise scams are extremely sophisticated. Here are some of the online tools they use to target and exploit their victims:

- **Spoofing e-mail accounts and websites:** Slight variations on legitimate addresses (john.kelly@abccompany.com vs. john.kelley@abccompany.com) fool victims into thinking fake accounts are authentic. The criminals then use a spoofing tool to direct e-mail responses to a different account that they control. The victim thinks he is corresponding with his CEO, but that is not the case.
- **Spear-phishing:** Bogus e-mails believed to be from a trusted sender prompt victims to reveal confidential information to the BEC perpetrators.
- **Malware:** Used to infiltrate company networks and gain access to legitimate e-mail threads about billing and invoices. That information is used to make sure the suspicions of an accountant or financial officer aren't raised when a fraudulent wire transfer is requested. Malware also allows criminals undetected access to a victim's data, including passwords and financial account information.

If you or your company have been victimized by a BEC scam, it's important to act quickly. Contact Frost immediately. Next, call the FBI, and also file a complaint—regardless of dollar loss—with the FBI's Internet Crime Complaint Center (IC3).**

DON'T BE A VICTIM

The business e-mail compromise scam has resulted in companies and organizations losing billions of dollars. But as sophisticated as the fraud is, there is an easy solution to thwart it: face-to-face or voice-to-voice communications. The best way to avoid being exploited is to verify the authenticity of the email by walking into the requestor's office or speaking to him or her directly on the phone from a trusted number.

Fraud Prevention & Best Practices Checklist

Frost

At Frost, we want to partner with you to protect your company from fraudulent activity. Developing a layered approach focusing on education, technology, business rules and procedures is the best way for you to achieve that protection. While not all-inclusive, this checklist is a great way to get started.

BEWARE OF FRAUD TRENDS ON THE RISE

Business Email Compromise – There continues to be an increase in email fraud where a scammer sends an email to your business from what appears to be a known source. When you receive a transaction request via email, verbally validate the request with the sender before sending it.

Cybercriminals and Your Personal Information – Identity theft is on the rise. Merchants you do business with may fall victim to data compromises. As a result, scammers can gain access to your personal identification information, such as your Social Security number, date of birth, debit card or account number. See ways you can keep your personal information safe below.

USER SECURITY

- [ ] Restrict user permissions to all systems and review settings regularly
- [ ] Implement user limits for electronic payment originations
- [ ] Require dual control for all cash handling steps, payment initiation, payment file handling, and to set up profiles for payment initiation
- [ ] Use repetitive wire transfer profiles whenever possible
- [ ] Require documentation for all internal requests for payments
- [ ] Verbally confirm vendor account changes with a trusted vendor contact
- [ ] Document all procedures, and train for them
- [ ] Audit user activities regularly
- [ ] Educate your employees about email, text and other scams
- [ ] Implement effective hiring practices, including background checks
- [ ] Lead a strong ethics policy by example
- [ ] Email two-step verification when updating sensitive information

SEPARATION OF DUTIES

Employees who:

- [ ] Write checks or initiate electronic payments should not reconcile accounts
- [ ] Initiate electronic payments should not approve them
- [ ] Maintain profiles for electronic payment initiation should not initiate or approve payments
- [ ] Open the mail should not prepare or make deposits

COMPUTER SECURITY

- [ ] Require use of a segregated computer only for banking activities and restrict internet surfing or email use
- [ ] Protect your network using a properly configured firewall
- [ ] Keep your industry standard antivirus and malware software current
- [ ] Apply the latest security updates from the operating system supplier
- [ ] Restrict access to the computer's administrative privileges
- [ ] Disable USB access when not in use
- [ ] Implement procedures to protect laptops when away from the office and before reconnecting them to the network
- [ ] Establish unique login and passwords for all systems and require periodic changes

RISCH RESULTS
RESEARCH. RECRUIT. RETAIN.

North Texas Nonprofit Institute

Revitalizing Your Team

How NFP Leaders Can Reclaim Talent and Reduce Turnover

certified WBENC WOMEN'S BUSINESS ENTERPRISE

10,000 small businesses

WE RUN ON EOS

Becoming a Talent Magnet

Potential employees want to know	Think of 1-2 stories per section to share
Impact: How have employees made an impact on the lives of your stakeholders?	1 2
Mission: Share employee testimonials that show their role in the mission.	1 2
Superheroes: Who are your superheroes for the world to know?	1 2

Beyond Compensation

Fostering growth and engagement in nonprofits

Mentorship, professional development, and Career pathways:
Pairing experienced staff with newer employees can provide guidance and a path for growth. Offer subscriptions to online learning platforms or stipends for courses related to their work.

Employee resource groups (ERGs):
Create groups around common identities or interests to foster community and inclusion.

Health and wellness programs:
Offering workshops or resources related to mental health, physical fitness, nutrition, etc.

Feedback mechanisms:
Implement regular feedback sessions or anonymous suggestion boxes to ensure employee voices are heard.

Employee-led initiatives:
Encourage employees to pitch and lead projects they're passionate about, even if they're outside their typical job duties.

Regular team-building activities:
These can be workshops, retreats, or even fun outings to foster stronger team relationships.

Transparent decision-making:
Involve employees in decision-making processes, or at least provide clarity on how and why decisions are made.

Cultural sensitivity training:
Ensure that the workplace is inclusive and respectful of all cultures and backgrounds.

Employee recognition programs:
Regularly spotlight and celebrate the achievements and milestones of employees.

Physical workspace improvements:
Consider small changes like comfortable seating, plants, or communal spaces.

Community engagement opportunities:
Allow employees to take time off to volunteer, or organize group volunteer activities.

Are traditional hiring methods no longer bringing in the best talent that is uniquely right for your organization?

Interview Support Resource

If you want to know X, how can I ask the question legally?

Illegal Question	Alternative Legal Question for Equivalent Information
Do have children? Will they interfere with your work?	Describe your availability for this position. Are you able to work flexible hours or overtime if needed? How do you handle unexpected changes to your schedule?
Where do you live?	Are you willing to relocate? Do you have reliable transportation to commute to the workplace?
Do you have a car?	Do you have reliable transportation to commute to the workplace? Are you comfortable with the location of the job?
How old are you?	What are your long-term career aspirations? Or, How does this job fit into your career plan? (candidate's commitment to their career and their potential longevity with the company?)
Do you have any disabilities?	Do you have any specific skills or experience that would be relevant to the job? Or, Can you perform the essential functions of the job?
What's your nationality?	Are you authorized to work in the US without any restrictions?
Are you pregnant?	Do you have any current commitments that would prevent you from fulfilling the job responsibilities?
What's your religious affiliation?	Are you available to work on our scheduled operating days?
Are you married?	Are you able to relocate if the job requires it?
Have you ever been arrested?	Have you ever been convicted of a crime that is reasonably related to the job duties for this position?
What is your gender?	This job requires a uniform; do you have any concerns with wearing the standard uniform?

If the candidate volunteers information about their disability or need for accommodation, you can ask follow-up questions to understand their needs and discuss potential accommodations that would allow them to perform the job duties.

MarshMcLennan Agency

Adam Sammons, CIC
Executive Vice President
P: 469-866-8515
E: Adam.Sammons@MarshMMA.com

Alex Sullivan, CIC
Advisor, Business Insurance
P: 469-866-8515
E: Alex.Sullivan@MarshMMA.com

Hard Market Playbook

Relationships

- Broker
- Underwriter
- Stakeholders
- Industry Peers

Expertise

- Industry-Specific
- Coverage Forms
- Market Knowledge

Resources

- Human Capital
- Market Access
- Data / Technology

Strategy / Tactics

- Alignment
- Program Design
- Implementation

Communication

- Pre-Renewal
- Post-Renewal
- When 💩 hits the ____

Kevin Mulhall,
Senior Technical Customer Success Manager,
Tech Soup

Cybersecurity Checklist

Functional Area	*Implementation Stage*	*Associated Products*	*Cost or Budget*	*Managing Staff or Partner*
Identify				
Protect				
Detect				
Respond				
Recover				