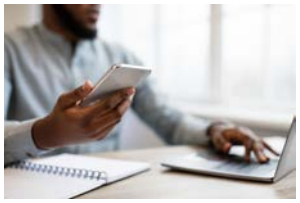
Loss Prevention T.I.P.S.
Together Improving Processes & Safety

How to Avoid Business Email Compromise/Social Engineering Losses

TML RISK POOL

It began as a routine email with a trusted vendor--nothing out of the ordinary. When a request came through to update bank account details, the employee made the change without verifying it. But the message wasn't from the vendor--it was a cyber criminal. By the time the mistake was discovered, over $300,000 had already been wired to the wrong account. A **socially engineered fraudulent wire transfer** (often attributed to or called **Business Email Compromise or BEC**) is one of the most common and costly cyber losses organizations face. For public entities, we consistently see the same pattern: attackers impersonate a trusted person (executive, vendor, attorney, or staff member) and pressure someone to change payment details or send a wire urgently. Below are some best practices that significantly reduce the risk of this type of loss.

1 **Independent Verification of Payment Requests.** Any request to change vendor banking information, or an employee,s direct deposit details, should be independently veri ed using a trusted phone number already on le. Email instructions alone should never be relied on for payment-related changes. Coverage could be impacted without taking this necessary step.



2 **Dual Authorization for Wire Transfers.** All wire transfers should require two separate levels of approval to reduce the risk of unauthorized transactions. For higher-dollar transfers, additional approval thresholds should be established, such as requiring executive or CFO authorization.

3 **Formal Vendor Payment Change Process.** Vendor banking changes should follow a standardized payment change process using a formal request form and should be veri ed directly with the vendor through an existing, trusted point of contact

4 **Email Security Awareness.** Employees should receive training to recognize Business Email Compromise (BEC), impersonation attempts, and other payment-related fraud schemes. Ongoing awareness is critical to helping employees identify and stop fraudulent activity before funds are released.

5 **Email Account Protection.** Email accounts should be protected with strong security controls to reduce the risk of compromise. This includes requiring Multi-Factor Authentication (MFA) for all users, enabling external email warning banners, and implementing email authentication protections such as SPF, DKIM, and DMARC. These safeguards help reduce spoo ng, phishing, and unauthorized access attempts.

LEARN MORE WITH THESE ADDITIONAL RESOURCES:

- Cyber Squad Video: Preventing Fraudulent Instruction and Recognizing Phishing Attack Types
- FBI —Business Email Compromise: How We Can Help
- Online Learning Center: Business Email Compromise (Cyber) - What It Is and How to Avoid 6 Figure Losses