

CHECKLIST

Business Email Compromise (BEC) Prevention Checklist

A practical guide to closing the gaps that let BEC and wire fraud attacks succeed.

Business Email Compromise is one of the costliest and fastest-growing forms of cybercrime — and it rarely involves malware. It relies on impersonation, urgency, and gaps in financial process. Use this checklist to harden both your technical defenses and your financial controls.

Email Authentication

- ☐ **Configure SPF, DKIM, and DMARC** on all sending domains to prevent spoofing.
- ☐ **Set DMARC policy to reject or quarantine** rather than monitor-only, once validated.
- ☐ **Deploy inbound/outbound email filtering** to catch impersonation and lookalike domains.
- ☐ **Flag external senders** with a visible warning banner on inbound email.

Financial Controls

- ☐ **Require dual authorization for wire transfers** above a defined dollar threshold.
- ☐ **Require call-back verification for payment changes** using a known, independently-sourced phone number — never one provided in the email.
- ☐ **Restrict who can initiate or approve** changes to vendor banking details.

Training & Awareness

- ☐ **Run phishing simulations quarterly** not just during onboarding.
- ☐ **Train finance and executive staff specifically** on BEC and CEO-fraud tactics.
- ☐ **Establish a clear, no-blame reporting process** for suspicious emails.

Technical Safeguards

- ☐ **Enforce multi-factor authentication** on all email and financial system accounts.
- ☐ **Monitor for suspicious mailbox rules** (auto-forwarding, auto-delete) that indicate compromise.
- ☐ **Restrict legacy email protocols** that bypass MFA (e.g., POP/IMAP where not needed).

Incident Response for BEC

- ☐ **Define immediate steps** if a fraudulent transfer is suspected (bank contact, law enforcement, IC3 report).
- ☐ **Maintain contacts for your bank's fraud department** and cyber insurance carrier in advance.

73% of cyber incidents in 2024 involved BEC, and 58% of cyber insurance claims trace back to BEC or wire fraud — making financial-process controls just as important as technical ones. (Source: industry claims reporting; verify current figures before publishing.)

Worried About BEC Exposure?

Cenova Cyber can review your email security and financial controls for BEC gaps.

Contact us for a free consultation.

www.cenovacyber.com