Business Email Compromise Prevention & Response One-Page Checklist

Print and post near Accounts Payable, Payroll, and Vendor Management workstations.

Before You Change Banking / Send Funds

- Pause: Is there urgency, secrecy, or pressure? Treat as suspicious.
- Verify out-of-band using a known phone number on file. Do not use phone numbers or links in the email.
- Use dual control for vendor adds/changes and high-risk payments.
- Require supporting documentation and log who verified, when, and how.

Email Hygiene

- Never approve payments from a personal email account.
- Look for look-alike domains and subtle misspellings.
- Report unexpected mailbox rules/forwarding or login alerts immediately.
- Use MFA for email and financial systems.

If You Suspect BEC

- Call the bank's fraud line to recall or hold the payment.
- Notify internal IT/leadership; secure the account (reset, revoke sessions, remove rules).
- Report to FBI at IC3.gov and contact Enduris at enduris.us.
- Preserve all emails, headers, invoices, logs.

Quick Reference

- Golden Rule: Never change payment instructions based on email alone.
- Second Factor: Always call a known contact to verify vendor/bank changes.
- Recordkeeping: Document verification steps for every change.