anchor@anchor-cyber:~$ cat bec-prevention.md

ANCHOR CYBER SECURITY LLC

# BEC Prevention Checklist

Business Email Compromise — wire transfer controls, email authentication, financial process safeguards, and social engineering red flags. Based on FBI IC3 guidance and FinCEN advisories.

$ bec --wire-controls

## Wire Transfer & Payment Controls

BEC causes more dollar losses than any other cybercrime category. The attack exploits process gaps, not technical vulnerabilities — controls must be procedural.

☐ **Establish a call-back verification procedure for all wire transfers**

Call the requestor at a known, pre-established phone number — not a number in the email. Never use contact information from the request itself.

☐ **Require dual authorization for any outbound wire above a defined threshold**

Two individuals must independently approve — not just review the same email thread. Define the threshold in written policy (common: $5,000–$25,000).

☐ **Create an explicit change-of-bank-account procedure**

Any request to update a vendor or employee bank account requires: written request + manager approval + call-back verification to an established number. Changes are not effective until confirmed.

☐ **Prohibit wire transfers or ACH changes initiated solely by email**

Email can be the notification, never the sole authorization. The actual approval must occur through an out-of-band channel.

☐ **Limit same-day wire capability to named, pre-approved staff**

Attackers exploit urgency.

Require next-day settlement for new payees unless the urgency has been verbally verified by a senior officer.

☐ **Review and verify new-vendor ACH instructions before first payment**

Call the vendor directly using a number from your records or their official website — not from the invoice. Confirm routing and account numbers verbally.

☐ **Train accounts payable staff on common BEC scenarios annually**

CEO fraud, vendor impersonation, invoice manipulation, and real estate wire fraud are

the four most common patterns. Tabletop the scenarios, not just slides.

```
$ bec --email-auth
```

## Email Authentication — SPF, DKIM, DMARC

SPF and DKIM establish identity; DMARC enforces policy on mismatches. A domain without DMARC enforcement (p=none) is spoofable by anyone.

☐ **Publish an SPF record listing every server authorized to send as your domain**

Include all email sending sources: mail servers, ESPs, marketing tools, HR systems. Use `~all` (softfail) initially, then `-all` (hardfail) once the full sending inventory is confirmed.

☐ **Enable DKIM signing in your email platform for your primary domain**

DKIM key length: minimum 2048 bits. Rotate DKIM keys annually. Verify signature via a header analyzer after enabling.

☐ **Publish a DMARC record and advance to enforcement (p=reject) over time**

Start with `p=none` to collect reports, then `p=quarantine`, then `p=reject`. Use DMARC aggregate reports (`rua=`) to find legitimate sources before tightening policy.

☐ **Enable DMARC reporting and review aggregate reports monthly**

Aggregate reports (`rua`) show all sources sending as your domain. Forensic reports (`ruf`) include sample failing messages. Both are needed to catch unauthorized use.

☐ **Cover all subdomains in DMARC policy**

Set `sp=reject` in your DMARC record to apply enforcement

to subdomains you don't use for email. Unprotected subdomains are common BEC spoofing targets.

☐ **Monitor for lookalike domain registrations**

Attackers register domains like `company-invoices.com` or `c0mpany.com`. Use a domain monitoring service or periodic manual searches for common substitutions on your key domains.

**Example DMARC record (enforcement)**

```
TXT @ _dmarc.yourdomain.com
"v=DMARC1; p=reject; sp=reject; adkim=s; aspf=s; rua=mailto:dmarc-reports@yourdomain.com; pct=100"
```

**Example SPF record**

```
TXT @ yourdomain.com
"v=spf1 include:_spf.google.com include:sendgrid.net ip4:203.0.113.10 -all"
```

$ bec --red-flags

## Social Engineering Red Flags

BEC relies on bypassing process controls by manufacturing urgency, authority, or trust. Train staff to recognize these patterns — and to treat them as reasons to slow down, not speed up.

**Unusual urgency**
Request must be done today, before EOD, while the executive is traveling

**Secrecy demand**
"Don't tell anyone," "this is confidential," "handle this personally"

**Executive impersonation**
Email appears from CEO/CFO but reply-to is a different domain

**New bank account for existing vendor**
Change of payment details with a plausible explanation attached

**New contact at a known vendor**
"Our accounting team changed — please send invoices to this new address"

**Slight domain variation**
`vendor-corp.com` instead of `vendorcorp.com`; character substitution

**Request skips normal process**
"Skip the usual approval — I'll handle it when I'm back"

**Wire to unfamiliar geography**
Domestic vendor suddenly requesting wire to foreign account

Sources: FBI IC3 BEC Advisory, FinCEN Advisory FIN-2019-A006, CISA #StopRansomware resources. Anchor Cyber Security LLC.

exit 0