Email Fraud Readiness Checklist

A short, practical self-assessment to help your organization gauge its current readiness against phishing, credential theft, and business email compromise. This is a self-guided reference, not a formal security audit, penetration test, or compliance certification.

Email remains one of the most common paths into an organization. In 2025, businesses reported over $3 billion in losses to business email compromise scams alone, across nearly 25,000 complaints, according to the FBI's Internet Crime Complaint Center.[1] Separately, Verizon's 2025 Data Breach Investigations Report found a human element present in roughly six in ten confirmed data breaches.[2] Readiness is less about any single tool and more about a handful of habits, checks, and verification steps working together.

How to use this checklist

Work through each section with whoever owns IT, finance, and leadership decisions in your organization. Check the box next to each item your organization already does consistently. There is no passing score. The goal is an honest picture of where you stand today.

1. Account and Access Basics

- ☐ Multi-factor authentication (MFA) is required on all email and finance-system accounts.
- ☐ Shared or generic email accounts (e.g. info@, accounts@) have MFA and a designated owner.
- ☐ Former employees and contractors lose email access on their last working day, not weeks later.
- ☐ Admin-level access to the email platform is limited to a small, known group of people.

2. Payment and Vendor Verification

- ☐ Bank detail or payment instruction changes are never actioned from an email request alone.
- ☐ A callback to a known, previously verified phone number is required to confirm changed payment details.
- ☐ Wire transfers and payment changes above a set dollar threshold require a second approver.
- ☐ New vendor payment setups go through the same verification process as changes to existing vendors.

3. Technical Email Controls

- [ ] SPF, DKIM, and DMARC are configured for your organization's email domain.
- [ ] External emails are visibly flagged or banners are shown for messages from outside the organization.
- [ ] Attachments and links are scanned automatically before reaching an employee's inbox where feasible.
- [ ] Look-alike domains similar to your own are monitored or at least periodically checked for.

4. People and Process

- [ ] Employees have a clear, simple way to report a suspicious email (a button, address, or contact).
- [ ] Reported emails are reviewed by someone in a reasonable timeframe, not left unread.
- [ ] Security-awareness training happens more than once a year, in short, practical sessions.
- [ ] There is a basic, written response plan for what to do if someone reports clicking a bad link or entering credentials.

5. Executive and High-Risk Roles

- [ ] Requests that appear to come from executives (payment, gift cards, data, urgent favors) get extra scrutiny.
- [ ] Executives and finance staff know that legitimate leadership will never ask them to bypass normal verification.
- [ ] Publicly available information about your leadership team and their travel is reviewed periodically for impersonation risk.

Reading Your Results

Checked items	What it suggests
16-19	A strong baseline. Focus on keeping the cadence consistent as your team grows.
10-15	A reasonable start with clear gaps. Prioritize payment verification and MFA first.
Below 10	Foundational gaps exist. A structured, ongoing program is likely worth prioritizing.

This checklist does not measure everything relevant to your organization's security, and completing every item does not prevent phishing, business email compromise, or any other incident. It is intended as a starting conversation, not a guarantee.

Want help turning this into an ongoing program?
CyberNest runs a managed security awareness program built around authorized simulations, short practical training, and leadership reporting. Book a no-cost Human Risk Readiness Review to talk it through. No employee testing occurs during the review.

cybernesthub.com/book-a-review

Sources

1. FBI Internet Crime Complaint Center, 2025 IC3 Annual Report. ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf
2. Verizon, 2025 Data Breach Investigations Report. verizon.com/business/resources/reports/2025-dbir-executive-summary.pdf