RED FLAGS

FOR EMAIL-BASED FINANCIAL FRAUD

BUSINESS EMAIL COMPROMISE CHECKLIST

Know what to look for in suspicious emails before financial damage is done.

SENDER RED FLAGS

- ✘ Email from a public domain (e.g., @gmail.com)
- ✘ Slight misspelling in the domain (e.g., @companny.com)
- ✘ Display name matches a known contact, but the address doesn't
- ✘ Unusual for this person to contact you directly

CONTENT RED FLAGS

- ✘ Uses urgent or secretive language: "ASAP" or "confidential"
- ✘ Requests to skip normal procedures or not tell others
- ✘ Mentions of being in a meeting or unavailable to talk
- ✘ Requests for wire transfers or gift card purchases
- ✘ Grammar, spelling, or tone feels "off" or unprofessional

FINANCIAL RED FLAGS

- ✘ New or changed payment instructions
- ✘ Request to send money to an international account
- ✘ Large or unusual payment amounts
- ✘ Unannounced changes to vendor invoices

TIMING & CONTEXT RED FLAGS

- ✘ Sent outside normal business hours (nights, weekends, holidays)
- ✘ Happens during staff transitions, vacations, or roll changes
- ✘ First-time request from the sender for this type of task

VERIFY BEFORE YOU ACT!

- ✓ Call the sender using a known number — don't rely on email
- ✓ Hover over links to verify their true destination
- ✓ Review past email threads for consistency
- ✓ Report suspicious emails to IT or your cybersecurity team