■ 8 Email Scams to Watch Out For

■ Fake Email/Customer Service Alerts

Claim: “Verify your account” or “Activate double security.”
Safe move: Don’t click links. Go to gmail.com/outlook.com directly.

■ Spear Phishing (Personalized)

Claim: Uses your boss’s or coworker’s name.
Safe move: Check sender address and verify by phone/text.

■ Government Imposter

Claim: IRS/SSA/FBI threats, “pay now.”
Safe move: Real agencies don’t email fines. Ignore & delete.

■ Bank/Financial Account Scams

Claim: “Suspicious activity, log in now.”
Safe move: Use your bank’s app or website, not the email link.

■ Package Delivery Scams

Claim: UPS/FedEx missed delivery, “pay fee to reschedule.”
Safe move: Track packages on the real site only.

■ Lottery & Prize Scams

Claim: “You’ve won money/a trip/phone!”
Safe move: If you didn’t enter, you didn’t win. Delete.

■ Fake Invoices & Receipts

Claim: “Thanks for your $399 renewal—click to cancel.”
Safe move: Don’t click or call. Check your real accounts.

■ Romance & Help Me Scams

Claim: Online crush or “friend stuck overseas” needs money.
Safe move: Never send money/gift cards. Verify by phone/video.

■■ Quick Security Boost

- Turn on Two-Factor Authentication (2FA).
- Keep spam filters active.
- Update your backup email & phone in account settings.
- Always go to the website directly, never through email links.
- Report scams (Gmail: three dots → Report phishing. Outlook: Report → Phishing).

■ **Golden Rule:** If it’s too urgent, too scary, or too good to be true… **don’t click!**