Before You Click: Phishing Email Checklist

Use this checklist whenever you receive an email asking you to take action—click a link, download a file, or provide information.

Quick Visual Check

- [ ] I looked at the sender's full email address (not just the display name)
- [ ] The email address matches the company's official domain (e.g., @bankname.com, not @gmail.com)
- [ ] There are no misspellings or strange characters in the sender's address
- [ ] The email addresses me by my actual name (not "Dear Customer" or "Account Holder")

The Three-Question Test

- [ ] **Was I expecting this?** This email relates to something I recently did (a purchase, appointment, or request I initiated)
- [ ] **Does the timeline make sense?** The email gives me reasonable time to respond (not "act immediately" or "24 hours")
- [ ] **Can I verify this another way?** I can check this issue by going directly to the company's website or calling their official number

---

Hover and Verify (Before Clicking Any Link)

- [ ] I hovered over the link to see where it actually leads
- [ ] The web address matches the company the email claims to be from
- [ ] There are no extra words like "secure," "verify," or "official" added to the web address
- [ ] The address doesn't use tricks like replacing letters with numbers (amaz0n instead of amazon)
- [ ] The real destination appears before the first slash (amazon.com/account is safe; account-amazon.fakesite.com is not)

Attachment Safety

- [ ] I was expecting this specific attachment from this specific sender
- [ ] The attachment makes sense in context (not a random "invoice" or "photo" I didn't request)
- [ ] If unsure, I contacted the sender through a trusted method to confirm they sent it

---

Trust Your Instincts

- [ ] This email matches how this company normally communicates with me
- [ ] Nothing about this message feels rushed, threatening, or "off"
- [ ] I'm not feeling pressured to act before I've had time to think

---

When in Doubt

- [ ] I did NOT click any links in the suspicious email
- [ ] I did NOT download any attachments
- [ ] I did NOT reply with any personal information
- [ ] I verified the issue by going directly to the company's official website (typed the address myself)
- [ ] I called the company using a number from my statement, card, or their official website—not from the email

---

If You Suspect a Phishing Email

- [ ] Forward the email to spam@uce.gov (Federal Trade Commission)
- [ ] Delete the email from your inbox
- [ ] Empty your trash folder to remove it completely
- [ ] If you clicked a link or shared information, change your passwords immediately
- [ ] Monitor your bank and credit card statements for unusual activity

---

Keep this checklist near your computer for quick reference. When something feels wrong, trust yourself—it's always better to verify than to regret.