Is It a Phishing Email?

A step-by-step checklist for clinicians, from Sana Network

Example: An email that looks like it is from your clinical supervisor says, "Please let me know the best number to reach you," but comes from a different address. This is a common impersonation scam. The first message is harmless on purpose. It only wants a reply.

PART 1: SPOT IT (check each box)

- ☐ **1. PAUSE.**
  Quick questions, mild urgency, or requests for discretion from someone senior are classic hooks. Take a breath before you reply.
- ☐ **2. CHECK the real sender address.**
  Look past the display name. Is it a free account (Gmail, Outlook, Yahoo) instead of your organization's address? Are letters swapped, added, or missing in the domain? Heed any warning banner from your email provider.
- ☐ **3. CHECK what is being asked.**
  Be extra careful with requests for your phone number, login or verification codes, payments, gift cards, or client information, especially in an unexpected message.
- ☐ **4. LOOK at the details.**
  Generic greeting or missing name, odd phrasing, vague context, a signature with a name but no title or phone number, or a Reply-To address that differs from the sender.
- ☐ **5. VERIFY another way.**
  Call or text the person at a number you already have, or ask in person. Never use contact details from the suspicious email.
- ☐ **6. DO NOT engage.**
  Do not reply, click links, open attachments, or send numbers, codes, gift cards, or client information until you have verified.

PART 2: REPORT IT

- ☐ **Tell your supervisor, practice owner, or compliance contact.**
  Your report may protect colleagues who received the same message.
- ☐ **Use your email's Report Phishing button.**
  Most providers have one in the menu. Then delete the message.
- ☐ **Forward it to reportphishing@apwg.org.**
  The Anti-Phishing Working Group collects phishing reports.
- ☐ **Report it at ReportFraud.ftc.gov.**
  The Federal Trade Commission tracks scam reports.
- ☐ **If money was lost, act fast.**
  Contact your bank or card issuer right away and file a complaint at ic3.gov (FBI Internet Crime Complaint Center).

PART 3: IF YOU ALREADY REPLIED OR CLICKED

- [ ] **Stop communicating with the sender.**
  Do not answer follow-up emails, texts, or calls. Scammers often move to text once they have your number.
- [ ] **Secure your accounts.**
  Change the password for your email and any account you used, and turn on two-factor authentication.
- [ ] **Check your device.**
  If you clicked a link or opened an attachment, run a security scan and ask your IT support for help.
- [ ] **Think about client information.**
  If protected health information could have been exposed, tell your HIPAA privacy or security contact, write down what happened, and follow your breach-assessment process. Consult an attorney or compliance professional if unsure.

Pro tip: Agree with your supervisor or practice owner in advance on how you will confirm unusual requests, such as a quick phone call or a code word. A shared habit removes the guesswork.

sananetwork.com | This sheet is informational only and is not legal, compliance, or IT advice. Follow your organization's policies and consult a qualified professional for your situation.