Email Header & Link Inspection (Practical Skills)

Why Email Headers Matter

- Email headers show **where the email really came from**.
- Attackers often use fake names but the header exposes them.
- Helpful for checking if a message is real or not.
- You don’t need to be technical — just look at key fields.

Key Header Field #1: “From” Address

- The display name can be fake.
- The real identity is in the actual email address.
- Look for small differences (extra words, numbers, characters).
- If something looks off, don’t trust it.

Key Header Field #2: “Reply-To”

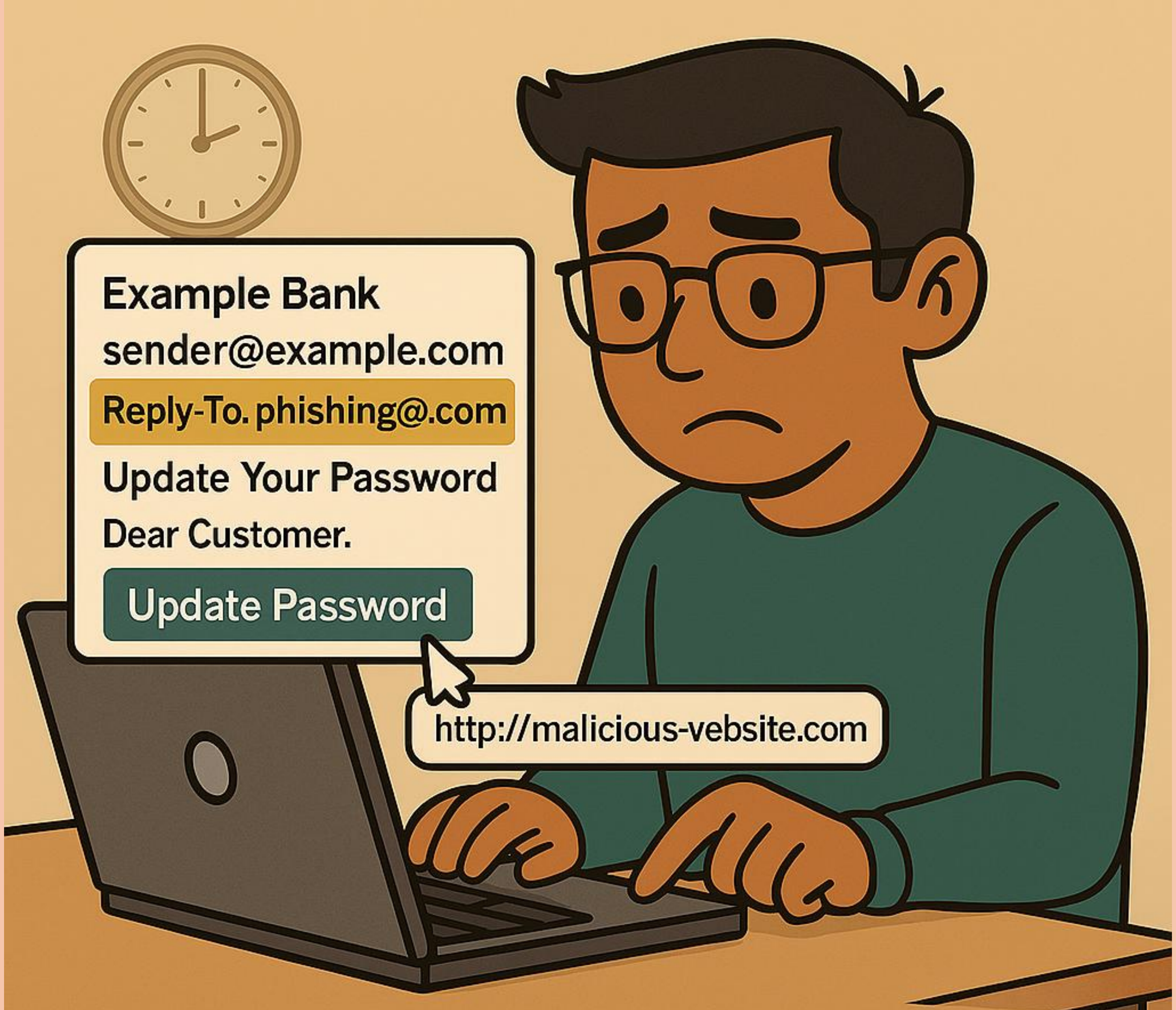
- Attackers use a different “reply-to” address to steal info.
- If the reply address doesn’t match the sender, it’s suspicious.
- Companies rarely use two different addresses for one message.
- Always check both fields.

Key Header Field #3: “Received” Path

- Shows the route the email took.
- If the email claims to be local but the “Received” path shows another country, it’s a red flag.
- You don’t need deep knowledge — just look for unusual locations.
- Trust your instinct if the path looks odd.

How to Inspect Links Safely

- Never click directly — *hover* first.
- Hovering shows the *real* website link.
- If the URL looks odd, long, or unfamiliar, avoid it.
- Attachments should be opened **only if expected!**



Arham almost clicks ‘Update Password,’ but he checks the header and catches the fake link.