10. THREAD HIJACKING / REPLY-CHAIN PHISHING

Attackers take over a legitimate email conversation, replying within the real thread.
This makes phishing emails highly convincing, as they appear to come from a trusted sender and include genuine context.

What Is Thread Hijacking?

Attackers break into someone's email and reply inside legitimate conversations, making the phishing email extremely believable.

Scenario: Maryam Gets a Reply in an Active Thread

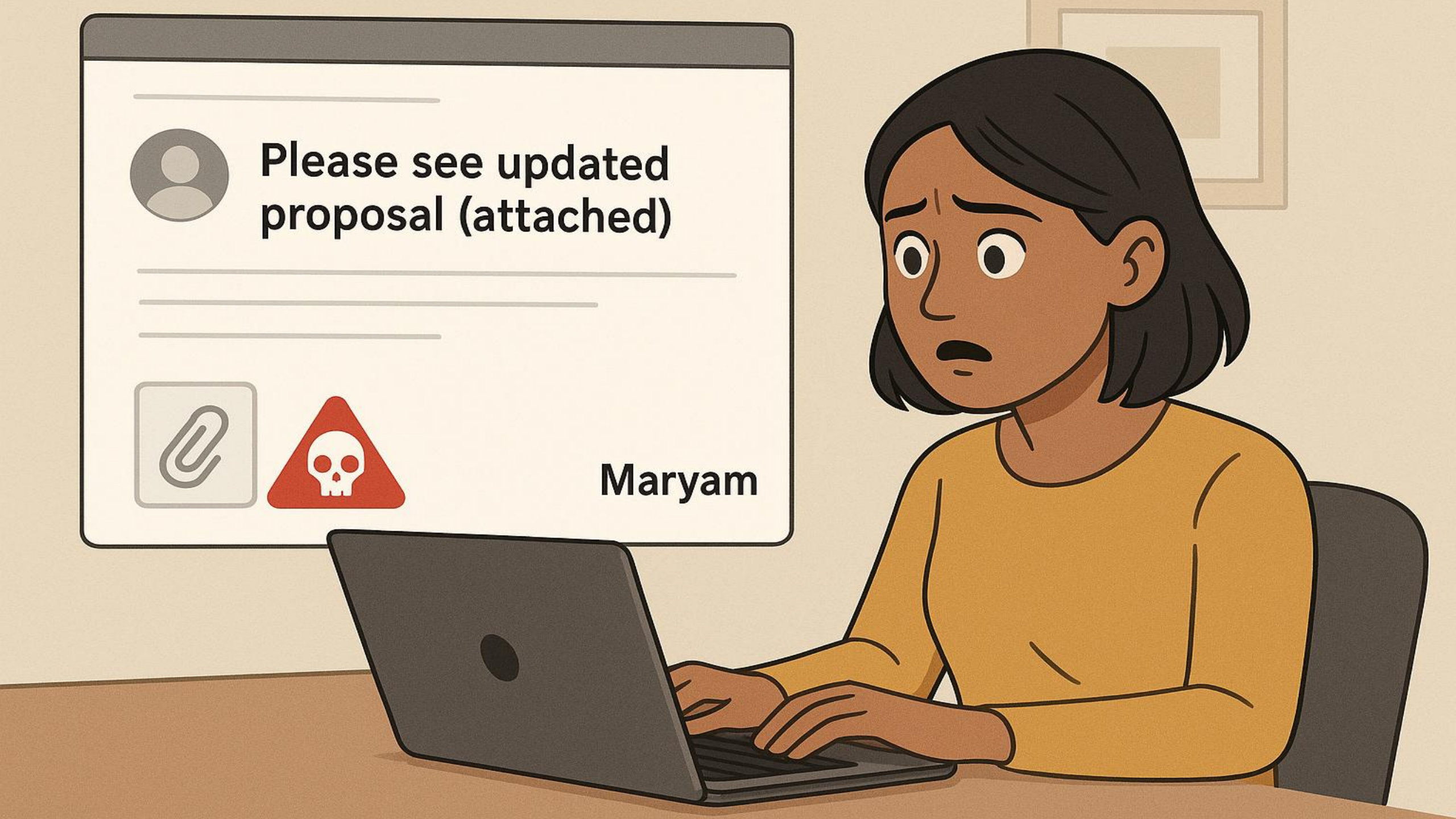
Maryam is discussing a project with a vendor.

Suddenly the vendor replies:

“Please see updated proposal (attached).”

But the attachment is malware, because the vendor’s email was hacked.

Lesson: Even emails in active threads can be dangerous—always verify unexpected attachments before opening them.


Please see updated proposal (attached)
Maryam

Why Thread Hijacking Is Dangerous?

- Trust exists already
- Email context is real
- Sender is legitimate
- No suspicion because the thread is ongoing

Detecting Thread Hijacking

- Attachment is unexpected
- Tone of writing feels different
- Suddenly asking for money or urgent action
- Replies come at odd hours

Prevention Tips

- Use MFA
- Call vendors for financial changes
- Report sudden “updated files”
- Beware of perfect timing (a big red flag)