5. CLONE PHISHING

Attackers copy a legitimate email you previously received and make it look identical,
but they replace the original link or attachment with a malicious one designed to trick you.

Scenario: Maryam Receives a “Resent Document”

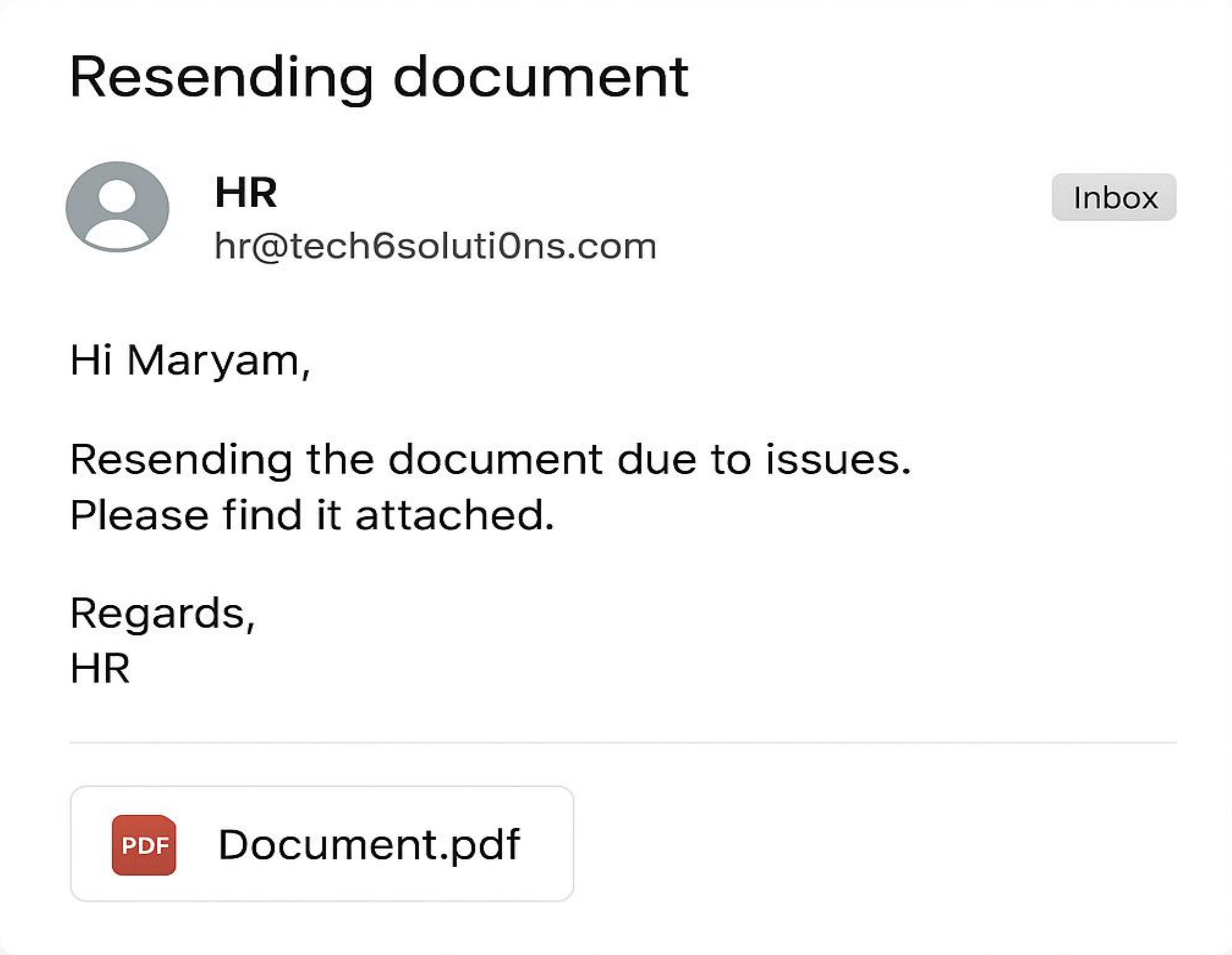
Maryam earlier received a genuine file from HR.

Two days later, she receives another email saying,

“Hi Maryam, resending the document due to issues.”

Everything looks identical, same layout, same wording, same subject, but this time the link is malicious.

Lesson: Attackers often rely on familiar-looking messages, so always recheck links and sender details even if the email resembles one you’ve already seen.



Resending document

HR
hr@tech6soluti0ns.com

Hi Maryam,

Resending the document due to issues.
Please find it attached.

Regards,
HR

Document.pdf

How Clone Phishing Tricks Employees?

- Familiar email thread = trust
- Same sender name
- “Resending due to error”
- Fake secure-looking PDF link

Red Flags Maryam Should Notice

- Small difference in sender domain (e.g., hr@tech6soluti0ns.com)
- File icon looks odd
- No reason for HR to resend the same file

Prevention Tips

- Always compare with the **original email**
- If the link looks different → don't click
- Forward to security team when unsure