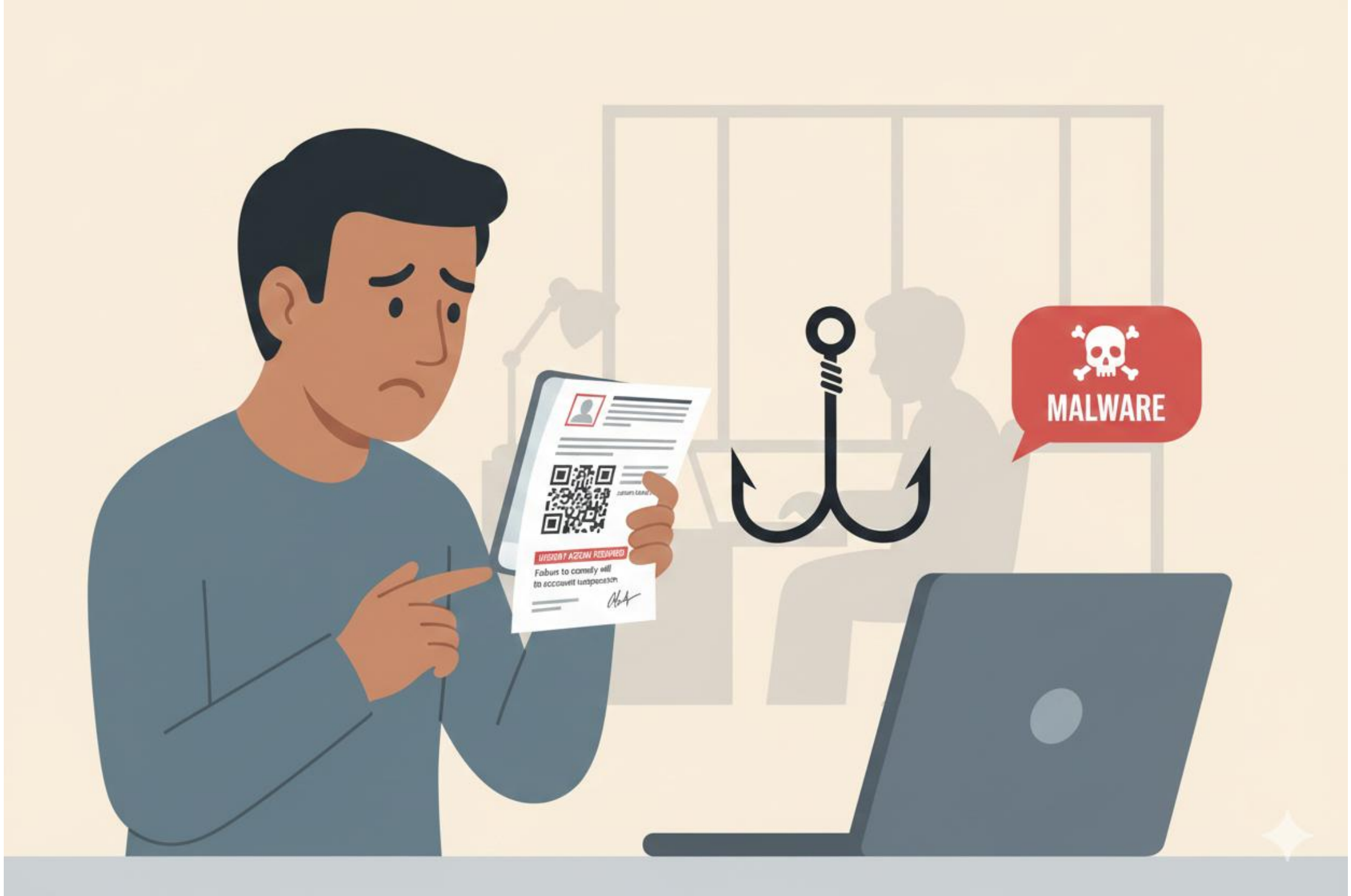
2. MAIL / PHYSICAL LETTER PHISHING

Attackers send printed letters that include malicious QR codes, fake URLs, or forged “official notices” designed to look legitimate. Because physical mail feels more trustworthy and formal, employees are more likely to scan the code, visit the link, or follow the instructions, unknowingly exposing sensitive information or downloading malware.


MALWARE

Scenario: Maryam Receives a “Bank Notice” Letter

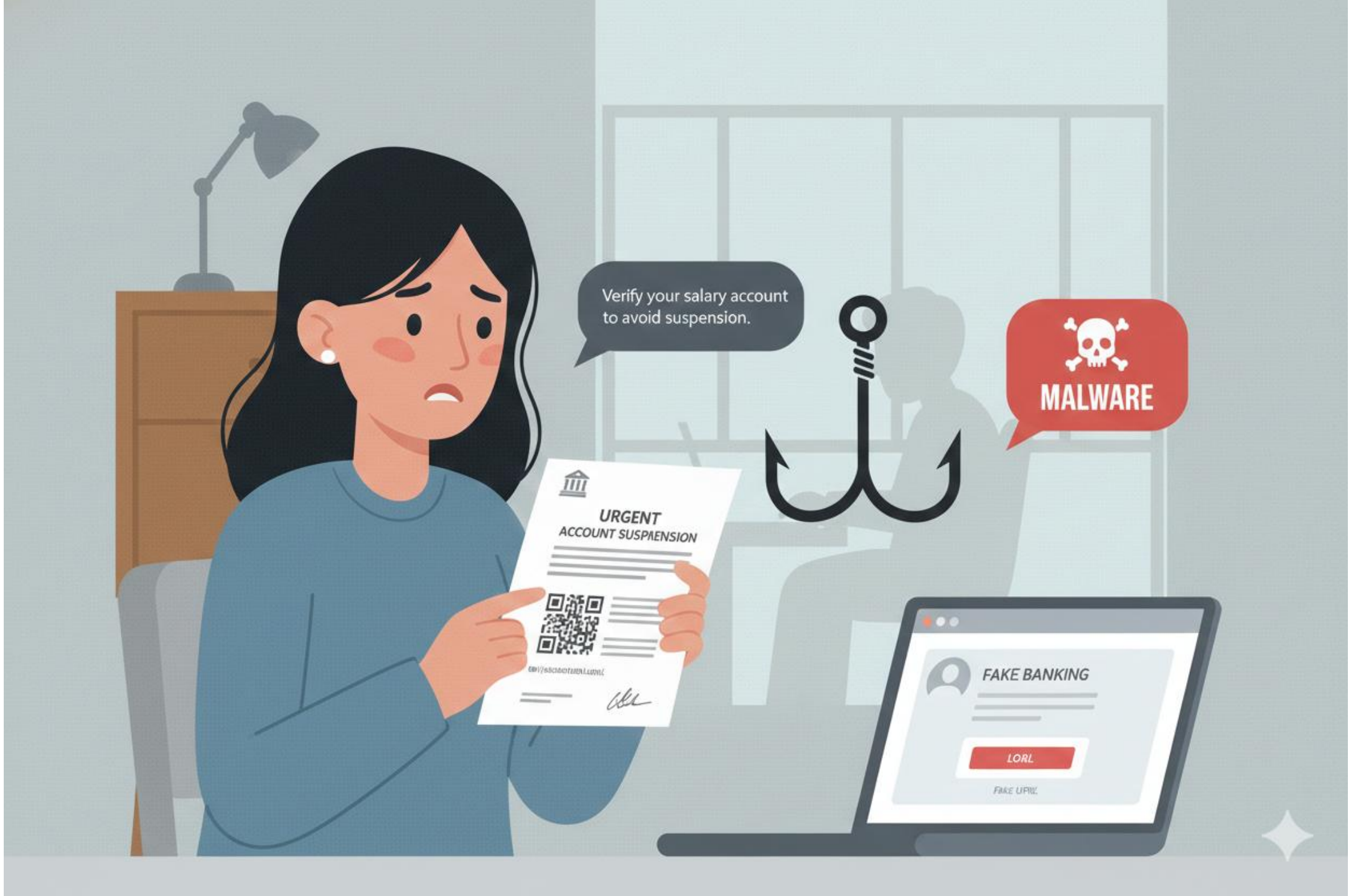
A letter arrives at Maryam’s desk:
“Verify your salary account to avoid suspension.”

It contains a QR code that leads to a fake banking page designed to capture her login details.

The paper looks official, logo, stamp, formatting, making it seem like a legitimate, urgent request.

The attacker relies on the trust people place in physical documents.

Lesson: Always verify unexpected physical notices with the actual organization. Never scan QR codes or follow instructions from unsolicited letters without confirmation.


Verify your salary account to avoid suspension.
MALWARE
URGENT
ACCOUNT SUSPENSION
FAKE BANKING
LORL

How Physical Phishing Tricks Employees?

- Realistic printing
- Official-looking language
- QR codes bypass typing suspicion
- Uses fear (“account suspension”)

Red Flags Maryam Should Notice

- Typos in letter
- Generic greeting
- Urgent tone
- Unknown sender address

Prevention Tips

- Don’t scan QR codes from unverified letters
- Confirm with sender through official numbers
- Report suspicious physical documents
- Shred unknown mail containing links or codes