2. Spear Phishing

Spear phishing is a targeted attack that uses personal or company-specific details to appear legitimate.

It focuses on specific individuals or teams, making it harder to detect.

What Is Spear-Phishing?

Spear phishing is targeted, using personal or company details.

Scenario: Maryam Gets a Very Convincing Email

Maryam receives an email that looks like it's "from HR," saying, "Maryam, here is your updated benefits file."

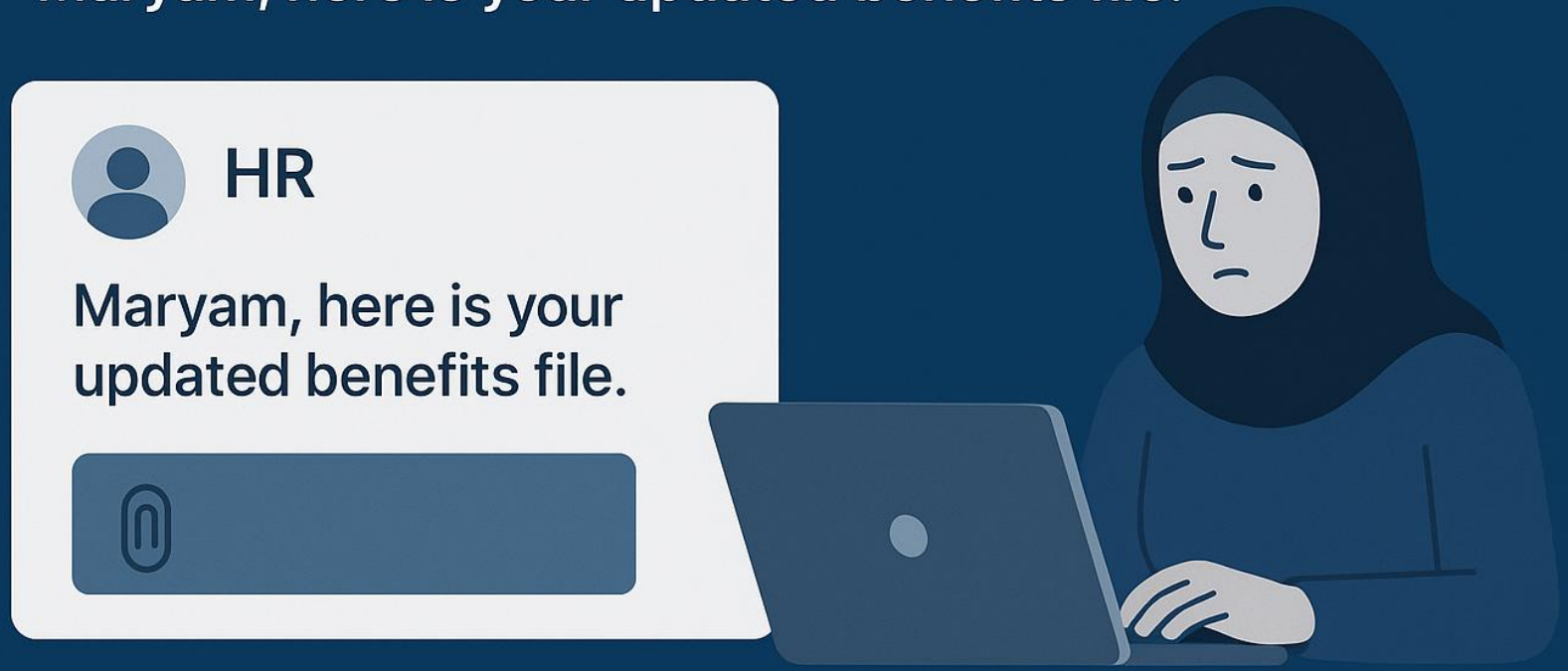
It even includes her department and her manager's name, making the message look completely genuine and hard to doubt.

But the attachment is actually malware that could infect her system if she opens it.

Lesson: Always verify unexpected emails, especially those with attachments, even if they appear personalized or come from trusted sources.

Scenario: Maryam Gets a Very Convincing Email

Maryam receives an email “from HR”:
“Maryam, here is your updated benefits file.”



How Spear-Phishing Is Crafted?

Attackers gather:

- LinkedIn details
- Company hierarchy
- Email signatures
- Social media posts

Red Flags Maryam Could Detect

- Unexpected attachment
- External domain masked as internal
- Tone slightly different from usual HR writing

Defense Tips

- Confirm via Teams/WhatsApp
- Don’t open “urgent documents”
- Trust your gut! If it feels odd, report it