

7. ATTACHMENT-BASED PHISHING (MACRO MALWARE)

Attackers send malicious PDFs, Word or Excel files, and ZIP/RAR archives that run hidden scripts when opened.

These scripts can install malware, steal data, or give attackers access to the system.

What Is Macro-Based Malware?

Attackers send malicious:



PDFs



Word/Excel
files



ZIP/RAR
archives

that run scripts when opened.

Scenario: Hassan Opens an “Urgent Salary Update” File

Hassan receives a Word file titled:
“Updated Salary Revision – Confidential”

When he opens it, he sees:
“Enable Content to view document.”
The moment he clicks, malware installs silently.

Lesson: Never enable macros or “Enable Content” on unexpected documents. Verify the source first, as attackers often use this trick to install malware.



Updated Salary Revision – Confidential

Enable Content to view document



Why Employees Fall for This?

- Salary
- Bonus updates
- Meeting minutes
- Policy updates are believable pretexts.

Red Flags in Malicious Attachments

- Asking to “Enable Macros”
- Unexpected attachments
- Strange icons (PDF icon but Word file)
- Huge file size for a small message

Prevention Tips

- Never enable macros
- Scan files before opening
- Prefer cloud-viewer mode
- Report unknown senders immediately