WHAT TO DO IF YOU CLICK / YOU THINK YOU'VE BEEN COMPROMISED

Immediate Actions After Clicking a Suspicious Link

Do not panic; act systematically.

Disconnect from the internet if malware may be involved.

Avoid entering any information on the suspicious page.

Report the incident immediately to IT/security teams.

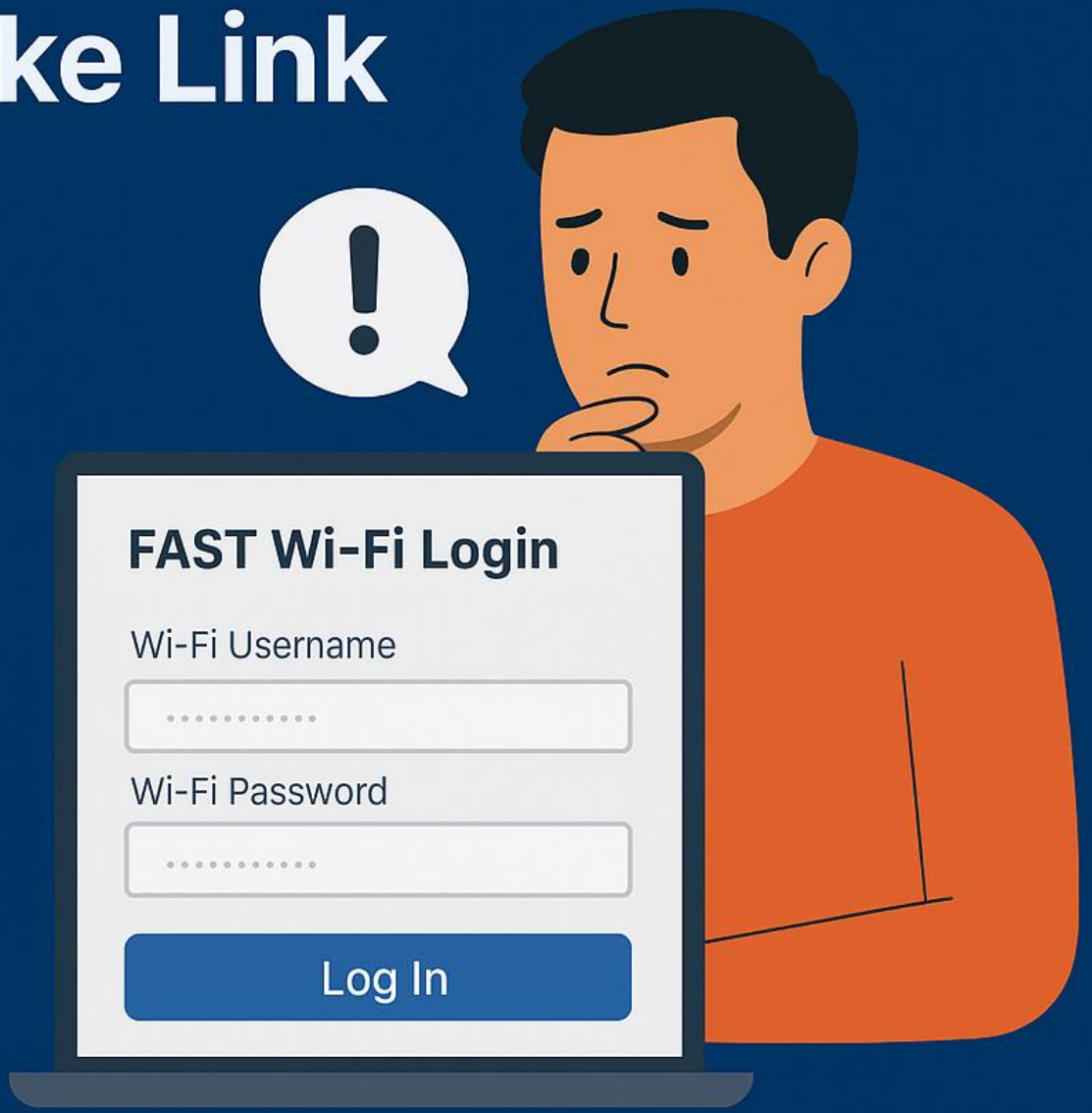
If You Entered Credentials

- Change the affected password immediately.
- Enable or reconfigure MFA for additional protection.
- Inform the security team so they can monitor account activity.
- Assume the credentials are compromised until confirmed safe.

Hassan Realizes He Clicked a Fake Link

- Hassan opens a fake “FAST Wi-Fi Login“ page
- He stops before entering his password
- He changes his real Wi-Fi portal password. Reports it to IT

› The fake page is taken down quickly



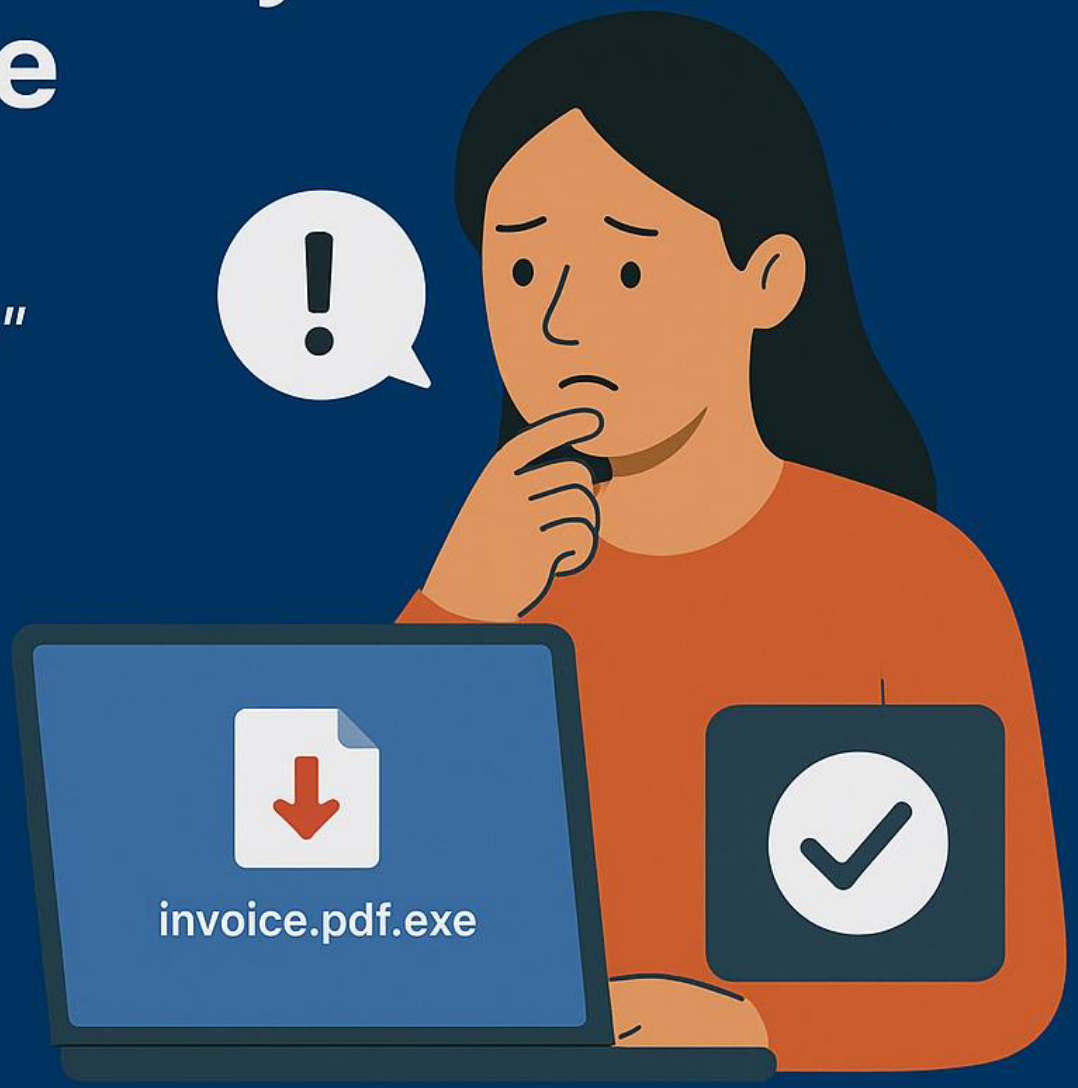
If You Downloaded or Opened an Attachment

- Stop using the system to prevent malware spread.
- Contact IT to run malware and endpoint scans.
- Do not attempt to delete or quarantine files manually.
- Prepare to answer questions about the file type and source.

Maryam Accidentally Downloads a File

- Maryam downloads a suspicious “invoice.pdf.exe“
- She doesn’t run it.
  Reports it to IT right away
- IT scans her system
  → removes the file safely

› Quick action prevents malware infection



Identifying Signs of Compromise

- Unexpected password reset notifications.
- Unknown logins or access attempts.
- Slow device performance or unusual pop-ups.
- Applications behaving abnormally or crashing.

Account Recovery Steps

- Reset passwords for all linked or dependent accounts.
- Review recent login history for suspicious locations.
- Remove unknown devices from account access lists.
- Revoke active sessions and regenerate authentication tokens.