1. Introduction

“Hello, this is [Your Name] from the IT Security Team. Am I speaking to [User Name]?”

If yes:

“*Great. I’m calling regarding a security alert we received from our endpoint protection system on your workstation. Do you have a minute to talk?”*

2. Explain the Reason for the Call

“Our system detected a potentially harmful file on your computer. I just need to confirm a few details with you to ensure everything is secure.”

(If they ask what file:)

“The file is named [filename], located in [path]. I just need to check if you were aware of it.”

3. Verification Questions

Ask calmly and clearly:

“Did you download or try to open this file?”
“Do you recognize the name of the file or why it would be on your computer?”
“Do you recall installing any software or tools around the time this alert was triggered?”

If *No* → reassure them.
If *Yes* → ask for the source.

“Where did you download it from — was it an official website or a shared link?”

4. Provide Guidance / Caution

Regardless of their answer, give this message:

“Thank you for the clarification. Going forward, please avoid downloading files or installers from untrusted websites or unknown links. If you’re ever unsure, contact the IT team first so we can verify it.”

5. State the Action Taken

“The file has already been quarantined by our security system, so your device is safe. We are just confirming details to complete the investigation.”

6. Confirm Device Status

“Are you experiencing any unusual behavior on your laptop slow performance, pop-ups, or strange applications?”

If yes → escalate.
If no → continue.

7. Closing the Call

“Thank you for your cooperation. We’ve completed our verification, and everything looks fine on your side. If you come across anything suspicious in the future, please let us know immediately.”

“Have a great day.”