

Optimized Prompting Framework for New ChatGPT Agent (2025)

1. Task Framing — High Clarity

Prompt Template:

"You are acting as a fully autonomous agent with the ability to browse, click, type, and execute code or file-based operations. Your task is:

Goal: [Insert the exact outcome here]

Provide a proposed step-by-step plan of action before you begin execution."

Example:

Goal: Create a 5-slide Google Slides deck on "Trends in Nonprofit AI Adoption," export it as a PDF, and save it to my Google Drive.

"Please outline your full approach and confirm that all steps are possible with current capabilities before you begin."

2. Tool Constraints — Clarify Capabilities

Prompt Add-on:

"Before proceeding, check whether any of the following are required and tell me if you cannot do them:

- Logging into password-protected websites
- Uploading files to external apps without connectors
- Making payments or sending emails
- Manipulating data behind paywalls

Only proceed if the full task can be completed. Otherwise, stop and explain what's possible."

Why this matters:

This prevents the agent from falsely confirming something it can't actually do.

3. Execution Mode — Request "Watch Mode"

Prompt Add-on (optional):

"Run this in watch mode so I can observe your steps and approve anything irreversible like sending files, publishing documents, or overwriting data."

Why this matters:

Gives you visibility and control to stop unintended behavior before an action is counted.



4. Step-by-Step Planning Before Execution

Prompt Add-on:

"Start by sharing a plan with numbered steps (e.g., Step 1: Open URL... Step 2: Scrape text...). Then ask:

'Shall I begin?' and wait for confirmation."

Why this matters:

Helps you ensure the agent understands the task correctly before committing a usage credit.

5. Post-Action Summary and Fallbacks

Prompt Add-on:

"After completing the task, provide a short summary of what was successful and where issues occurred.

If the task fails at any point, retry using a different method or offer a revised plan without consuming another agent action."

Why this matters:

Encourages the agent to retry and prevents burning through credits unnecessarily if something fails.

Full Example Prompt Using This Framework

"You are acting as an autonomous AI agent using a virtual computer.

Goal: Go to [URL], extract the top 10 data points related to [topic], create a spreadsheet summarizing those findings, and upload the spreadsheet to my Google Drive.

Before proceeding, check if any of the following are required and confirm whether you can do them:

- Logging into sites
- Downloading from paywalls
- Submitting forms behind authentication

If any are not possible, do not start the action.

Share a step-by-step plan and ask 'Shall I begin?'

Use watch mode and provide a post-task summary. If you fail mid-task, retry or offer alternatives before consuming another agent action. (If you're Plus, you only get 40/mo at the time of this doc creation)

