The agent permissions review

Before you connect an agent, MCP server or skill: list what it can do, what it reads, and decide what it's allowed to do without you.

Time **about 25 minutes** Updated **12 Nov 2026** Fill in online at **Learn › Worksheets**

HOW TO USE IT

1. Fill it in from the tool's own documentation, before you connect anything.
2. List every action, and mark which ones change things or can't be undone.
3. Review it again whenever the tool updates or you add a connection.

1. What I'm connecting

Agent, MCP server or skill

Who made it, and why I trust them

Workflow or agent?

- ○ Fixed steps I set (workflow)
- ○ AI chooses the steps (agent)

2. Actions

Allow: runs without asking. Confirm: asks me each time. Off: switched off.

What it can do

	Action	Read-only, changes things, or can't be undone	Allow, confirm or off
Action 1			
Action 2			
Action 3			
Action 4			

3. Outside content and injection

Outside content it will read (web pages, emails, files from others)

Protections

- [ ] Nothing that sends, deletes, publishes or spends runs without my confirmation
- [ ] It has the narrowest access that does the job
- [ ] I'll read each confirmation prompt, not click through
- [ ] I know how to disconnect it

Example answers

> The example is illustrative, based on the email scenario in the lesson. It isn't a review of any real product.

1. What I'm connecting

Agent, MCP server or skill

> An email MCP server for my AI desktop app

Who made it, and why I trust them

> The email provider's own official server, linked from its documentation.

Workflow or agent?

- ○ Fixed steps I set (workflow)
- ◉ AI chooses the steps (agent)

2. Actions

Allow: runs without asking. Confirm: asks me each time. Off: switched off.

What it can do

	Action	Read-only, changes things, or can't be undone	Allow, confirm or off
Action 1	Search and read emails	Read-only	Allow
Action 2	Create a draft	Changes things	Allow
Action 3	Send an email	Can't be undone	Off
Action 4	Delete an email	Can't be undone	Off

3. Outside content and injection

Outside content it will read (web pages, emails, files from others)

> Every incoming email, including from strangers.

Protections

- [x] Nothing that sends, deletes, publishes or spends runs without my confirmation
- [x] It has the narrowest access that does the job
- [x] I'll read each confirmation prompt, not click through
- [x] I know how to disconnect it

Limit what an agent can do, not just what it's told. Anything it can't do, injected text can't make it do. Free to use and adapt for your own work.