

OUTSELL PLAYBOOK

OUTSELL JOURNAL — DECISION WORKSHEET

Prompt injection in marketing agents: separate research from instructions

QUESTION

What can go wrong when a marketing agent reads an external page?

GUIDE TAKEAWAY

External text can contain instructions designed to redirect an agent. Treat retrieved content as data and enforce permitted actions outside the model.

START HERE

Label external inputs.

YOUR SITUATION

Account or cohort

Decision to make

Starting state and exclusions

Evidence sources, dates, and limitations

Unknowns to validate

WORK THROUGH THE GUIDE

1. Label external inputs

Evidence or input

Output or decision

Owner and review point

2. Limit data and tool permissions

Evidence or input

Output or decision

Owner and review point

3. Test a synthetic attack

Evidence or input**Output or decision****Owner and review point**

4. Check execution rejection

Evidence or input**Output or decision****Owner and review point**

5. Rehearse pause and recovery

Evidence or input**Output or decision****Owner and review point****COMPARE THE OPTIONS**

Source text

Useful when: Public research evidence

Limitation: May contain adversarial instructions

Suggested action: Treat as untrusted data

Why this fits our situation**Evidence needed before acting**

Prompt instruction

Useful when: Guiding model behaviour

Limitation: Not an access-control boundary

Suggested action: Add external enforcement

Why this fits our situation**Evidence needed before acting**

Restricted tool

Useful when: A bounded read or write

Limitation: Needs maintained permissions

Suggested action: Inspect permitted destinations

Why this fits our situation

Evidence needed before acting

Recovery plan

Useful when: An unexpected action occurs

Limitation: Unreconciled state can persist

Suggested action: Pause and review the trace

Why this fits our situation

Evidence needed before acting

COMMIT TO A BOUNDED NEXT STEP

Chosen action

Responsible owner

Required approval

Success measure and definition

Review date

Continue, revise, or stop criteria

Guide: <https://outselll.com/blogs/prompt-injection-in-marketing-agents/>

Publisher and evidence policy: <https://outselll.com/editorial-policy/>