

When the document gives orders

Year 10 student investigation

What happens when an untrusted document asks for an action?

Hypothesis and criterion

Name the expected effect, the measurement and what would count against your explanation.

Method and reproducibility

Record cases, source, units, parameters, controls and how cases are split.

Paired evidence

Case and split	Baseline	Changed result	Interpretation

Counterexample and revised design

Build benign and attack cases; compare a phrase filter with an independent action allowlist on unseen variants.

Individual defence

Explain one exact result, the mechanism, your limitation and what would overturn your claim.

Handover and tool use

Next test, saved project filename, tools used and which work is your own.

Use fictional data. Download your project before changing devices. On shared devices, turn remembering off and clear your work when finished.