Task 7 — Browser Extensions Audit Report

This report documents a security audit of installed browser extensions, focusing on permissions, developer reputation, and potential privacy risks.

Summary

The audit identifies extensions with broad permissions or suspicious behavior. This package contains steps to inspect, flags to look for, and remediation actions.

Flagged Extensions

Name	ID (partial)	Risk	Reason	Action
LinkedIn Auto-Connect	dcjimifcoocdj...	High	Automates actions; excessive permissions	Removed
Awesome Screen Recorder	nlipoenfbbik...	Medium	Screen capture + broad access	Disabled
Google Docs Offline	ghbmnnjooekp...	Low	Official Google extension	Kept

Evidence

Place screenshots inside the evidence/ folder. Recommended filenames:

```
evidence/01_extensions_list_before.png evidence/02_removed_LinkedIn_AutoConnect.png
evidence/03_extensions_list_after.png
```

Recommendations

Only install trusted extensions, review permissions, and periodically audit installed extensions. Change passwords and enable 2FA if an extension had access to sensitive sites.