TASK-7

OFFICIAL SECURITY REPORT

Title: Identification and Removal of Suspicious Browser Extensions

---

1. Objective

This report outlines the identification, evaluation, and removal process for browser extensions that may pose **security, privacy, or compliance risks**. It specifically focuses on:

- **Email Tracker by Mailtrack**
- **Session Buddy**
- **Bookmarks Quick Search**

---

2. Evaluation Summary

Extension	Purpose	Risk Level	Security Concerns
Mailtrack	Email open tracking (Gmail)	High	Tracks recipients without consent; data transmission to 3rd party
Session Buddy	Tab/session management tool	Medium	Access to browsing sessions; no encryption for stored data
Bookmarks Quick Search	Search bookmarks efficiently	Medium-Low	Minimal functionality; potential data access via bookmarks content

---

3. Detailed Analysis

A. Mailtrack – Email Tracker

- **Function:** Tracks when emails are opened via invisible pixels
- **Permissions:** Full Gmail access, browsing activity
- **Risks:** High privacy intrusion, potential GDPR/CCPA non-compliance
- **Recommendation:** Remove unless explicitly approved and consent obtained

B. Session Buddy

- **Function:** Saves browser sessions and tab history

- **Permissions:** Access to all tab URLs, session data
- **Risks:** Medium – Data not encrypted, risk of exfiltration of sensitive session info
- **Recommendation:** Use alternatives with local encryption; remove if unused or unnecessary

C. Bookmarks Quick Search

- **Function:** Quickly searches saved bookmarks
- **Permissions:** Read access to bookmarks
- **Risks:** Low to Medium – Potential for profiling or malicious redirects if compromised
- **Recommendation:** Monitor for unexpected behavior; low priority removal unless unfamiliar source

---

4. Indicators of a Suspicious Extension

- Requires excessive permissions (e.g., "read all data on all websites")
- Redirects, injects ads, or tracks browsing activity
- Frequently updates without changelog transparency
- Hosted by unknown or obscure developers
- Sends data to unknown third-party domains

---

5. Removal Procedure

Manual Removal in Chrome/Edge:

1. Open browser and go to: chrome://extensions/ or edge://extensions/
2. Locate the target extension
3. Click **"Remove"**
4. Confirm removal
5. Optional:
    - Clear browser cache
    - Restart browser
    - Revoke third-party access in Google Account settings

Automated/Admin Control (For Organizations):

- Use Chrome/Edge Enterprise Policy to **blacklist extensions**

- Maintain **allowlist** of approved tools
- Periodically run browser audit scripts or EDR extension scans

---

6. Recommendations

- 🔍 **Audit browser extensions** monthly for all devices
- ✅ Enforce **least privilege** principle – install only what's necessary
- 🔒 Educate users on risks of seemingly harmless productivity tools
- 📜 Log and monitor extension installs via centralized tools (e.g., MDM, browser telemetry)

---

7. Conclusion

Out of the three reviewed extensions, **Mailtrack** presents the most significant privacy and regulatory risk. **Session Buddy** and **Bookmarks Quick Search** carry moderate to low concerns but should be reviewed for necessity. Unused or unfamiliar extensions should be promptly removed.

---

8. Appendix: Summary Table

Extension	Safe to Keep?	Action Required
Mailtrack	❌ No	Remove Immediately
Session Buddy	⚠️ Conditional	Review Use, Monitor
Bookmarks Quick Search	✅ Yes (with caution)	Monitor Occasionally