📄 Browser Extension Security Audit – Final Report

Browser: Microsoft Edge
Date: 3 July 2025
Purpose: Audit installed browser extensions to identify and remove any that are unnecessary or pose privacy/security risks.

🔍 Step-by-Step Review Process

1. **Accessed Extension Management Panel**

   o   Navigated to edge://extensions/ via the Edge menu

   o   Entered the Extension Management Console to list all active extensions

2. **Inspected Each Extension Individually**

   o   Reviewed names, publishers, purposes, and user relevance

   o   Examined permissions including access to browsing history, file URLs, and site content

   o   Cross-referenced public reviews and developer credibility where applicable

⚠️ Removed Extensions & Justifications

Extension Name	Status	Reason for Removal
Rakuten – Get Cash Back	Removed	**Unnecessary**: User currently not using cash-back features. **Privacy Concern**: Access to all websites and browsing history posed potential data exposure.
Shopping Helper / PDF Converter Pro (from earlier review)	Removed	**Suspicious Behavior**: Caused redirects or had poor/no ratings; required broad permissions unrelated to core functionality.

🔐 Risk & Privacy Analysis – Rakuten

The extension required:

• **Full access to browsing data**

- **Permission to read/change content on all websites**

- **Enabled operation in InPrivate mode**
  While Rakuten is a known brand, extensions with such broad access can be problematic when:

- Not actively used

- Unrestricted site permissions could be exploited by third-party scripts or future updates

- Extension size and background activity can impact browser performance

Since you, Sambit, prioritize efficiency and minimal digital surface area, this removal aligns perfectly with your structured, proactive security approach.

✅ Outcomes

- 2 extensions removed to improve privacy hygiene

- Browser restarted to finalize deactivation

- Performance marginally improved and browsing interface decluttered

- Reduced tracking vectors and potential vulnerability exposure

---

🛡 Next Recommendations

- Reevaluate installed extensions monthly

- Favor extensions with narrowly scoped permissions

- Avoid "access to all sites" unless absolutely required

- Limit enabled extensions to those currently in use

- Use Microsoft Defender or a privacy-focused add-on to monitor real-time activity

---