Interview Questions and Answers

---

1. How can browser extensions pose security risks?

Browser extensions can access sensitive browser data, including browsing history, saved passwords, cookies, and active sessions.
Malicious or poorly designed extensions may exploit these permissions to **track user activity, inject ads, steal credentials, or redirect users to phishing sites**.
Even legitimate extensions can become risky if their developers are compromised or sell the extension to malicious actors.

> **In short:** Extensions act as small software pieces inside your browser — if untrusted, they can spy, steal, or manipulate what you see online.

---

2. What permissions should raise suspicion?

Certain permissions indicate a higher security risk, especially if they don't align with the extension's purpose.
Red-flag permissions include:

- "Read and change all your data on all websites you visit."
- "Access your browsing history"
- "Manage your downloads"
- "Access clipboard data"
- "Communicate with cooperating native applications"
- "Access file system or local storage"

If an extension with a simple purpose (like changing a theme) requests full site data access — that's a **warning sign**.

---

3. How to safely install browser extensions?

To install extensions safely:

1. **Use official stores only** — Microsoft Edge Add-ons, Chrome Web Store, or Firefox Add-ons.
2. **Check the publisher** — prefer verified developers or well-known organizations.
3. **Read user reviews** and watch out for reports of ads, pop-ups, or suspicious behavior.
4. **Check permissions** before installing — install only if they make sense.
5. **Avoid unnecessary extensions** — fewer add-ons mean fewer attack vectors.
6. **Regularly review** installed extensions and remove unused ones.

> Always treat an extension like any other software installation — verify it before you trust it.

---

4. What is extension sandboxing?

Extension sandboxing is a security mechanism that **isolates browser extensions from directly accessing the system or other browser components**.
Each extension runs in a restricted environment (sandbox) with limited privileges, so even if it's compromised, the damage is contained within its own scope.

For example, a sandboxed extension cannot read local system files or modify browser memory directly.
This helps prevent privilege escalation and protects the browser from full compromise.

---

5. Can extensions steal passwords?

Yes — if an extension has **permissions to read data from web pages or intercept keystrokes**, it can potentially steal credentials.
Malicious extensions may:

- Capture login details entered on websites
- Inject fake input fields on legitimate login pages
- Export saved credentials or tokens

Modern browsers implement security checks, but if users grant **"read and change data on all sites"** permissions, extensions can still abuse it.
Hence, it's crucial to install only trusted extensions and monitor permissions regularly.

---

6. How to update extensions securely?

Safe update practices include:

1. **Allow automatic updates** from official browser stores — they verify and sign updates.
2. **Avoid downloading .crx or .xpi files manually** from unknown sources.
3. **Review change logs** if available before applying updates.
4. **Check for publisher changes** — if ownership changes, re-evaluate trust.
5. **Re-enable extension permissions manually** if prompted, rather than blindly accepting.

> Secure updates ensure your extensions get patches without introducing new threats.

---

7. Difference between extensions and plugins?

Aspect	Extensions	Plugins
Purpose	Modify or enhance browser behavior (UI, features)	Handle specific web content types (e.g., Flash, Java)
Integration	Run inside the browser's sandbox	Operate outside or alongside the browser
Security	Safer runs in a restricted environment	Higher risk; deeper system access
Example	Ad blocker, password manager	Flash Player, Java Plugin
Modern Support	Widely used	Mostly deprecated in modern browsers

Essentially, extensions extend browser functionality safely, while plugins integrate external capabilities that are now mostly obsolete.

---

8. How to report malicious extensions?

To report a suspicious or malicious extension:

- **Microsoft Edge Add-ons:** https://microsoftedge.microsoft.com/addons → Open extension page → Click **"Report abuse"**.
- **Chrome Web Store:** Go to the extension page → Scroll down → Click **"Report abuse"**.
- **Firefox Add-ons:** Visit the add-on's page → Click **"Report this add-on for abuse"**.

Additionally:

- Provide screenshots or detailed descriptions of the issue.
  Mention suspicious behavior (data theft, redirects, CPU spikes, etc.).
- If you suspect system-wide infection, also notify your **IT security team** or **browser support**.

Reporting helps protect the community and prevents others from being affected by the same threat.