1. How can browse extensions pose security risks?
   Ans: Browsers extensions can pose security risks if they request excessive permissions, allowing them to access browsing history, stored passwords, or personal data. Malicious extensions can also redirect users to phishing sites, inject ads or malware, and compromise enterprise security.

2. What permissions should raise suspicions?
   ans: include access to all browsing data, the ability to read and change data on all websites, access to the clipboard, which can be exploited to steal sensitive information or inject malicious code.

3. How to safely install browser extensions?
   ans: only download them from official browser stores and check or avoid unrelated access requests.

4. What is extension sandboxing?
   ans: Security technique where a browser run each extension in an isolated environment so it can't directly access system files.

5. Can extensions steal passwords?
   ans: Yes, storing keystrokes

6. How to update extensions securely?
   ans: Automatic updates in browser settings

7. Difference between extensions and plugins?
   ans: Extensions modify browser functionality using web technologies whereas plugins are external programs that handles specific content type.

8. How to report malicious extensions?
   ans: Report abuse or security feedback form.