**Browser Extension Identification Guide**

**Overview**

Browser extensions are small software programs that extend browser functionality, but they can also pose significant security risks. This guide provides comprehensive techniques to identify potentially malicious or suspicious extensions across different browsers.

**Recent Threat Landscape (2024-2025)**

* **December 2024**: Cyberhaven incident - 35 compromised extensions affecting 2.6 million users
* **February 2025**: Additional 16 malicious extensions discovered
* **Ongoing**: Over 100 malicious extensions removed from stores annually

**Key Warning Signs**

**Critical Red Flags**

1. **Unfamiliar Extensions**
   * Extensions you don't remember installing
   * Recently appeared extensions
   * Extensions with generic names like "Helper", "Assistant", "Optimizer"
2. **Excessive Permissions**
   * "Read and change all your data on all websites"
   * Access to browsing history
   * Access to all tabs and browsing data
   * Camera and microphone access (unless specifically needed)
3. **Poor Reputation Indicators**
   * Few or no reviews
   * Recent negative reviews mentioning suspicious behavior
   * Developer with no other extensions or suspicious profile
   * Extensions not found in official store searches (hidden extensions)
4. **Behavioral Anomalies**
   * Browser slowdown after installation
   * Unexpected ads or pop-ups
   * Homepage or search engine changes
   * Redirects to unfamiliar websites
   * Unusual network activity
5. **Technical Red Flags**
   * Recently changed ownership
   * Extension hasn't been updated in over a year
   * Requests for permissions beyond stated functionality
   * Auto-updates without user consent

**Step-by-Step Identification Process**

**Phase 1: Initial Survey**

1. **Create Extension Inventory**

# Chrome  
google-chrome chrome://extensions/  
  
# Firefox  
firefox about:addons  
  
# Edge  
microsoft-edge edge://extensions/

1. **Document All Extensions**
   * Extension name and ID
   * Developer/Publisher
   * Installation date
   * Permission level
   * Purpose/functionality

**Phase 2: Risk Assessment**

For each extension, evaluate:

|  |  |  |  |
| --- | --- | --- | --- |
| Criteria | Low Risk | Medium Risk | High Risk |
| **Developer** | Known company | Individual developer | Anonymous/Suspicious |
| **Reviews** | 100+ positive | 10-100 mixed | <10 or negative |
| **Permissions** | Minimal needed | Some excessive | Highly excessive |
| **Updates** | Recent regular | Occasional | Rare or none |
| **Functionality** | Clear purpose | Vague benefits | Unclear purpose |

**Phase 3: Deep Analysis**

1. **Permission Audit**
   * Review each permission carefully
   * Question necessity for stated function
   * Look for permission escalation over time
2. **Developer Research**
   * Check developer's website and reputation
   * Verify other extensions by same developer
   * Look for contact information and support
3. **Community Feedback**
   * Read recent reviews and comments
   * Check security forums and blogs
   * Search for security advisories

**Browser-Specific Instructions**

**Google Chrome**

**Accessing Extensions**

# Via browser  
chrome://extensions/  
  
# Via command line  
google-chrome --enable-extensions-on-chrome-urls chrome://extensions/

**Chrome-Specific Checks**

1. **Developer Mode Analysis**
   * Enable Developer Mode in chrome://extensions/
   * Look for "Inspect views" links
   * Check for error messages in console
2. **Extension Source Verification**

# Check extension directory  
ls -la ~/.config/google-chrome/Default/Extensions/  
  
# Examine manifest file  
find ~/.config/google-chrome/Default/Extensions/ -name "manifest.json" -exec cat {} \;

1. **Chrome Web Store Verification**
   * Verify extension exists in Chrome Web Store
   * Check if it matches installed version
   * Look for "Published by" verified status

**Chrome Permission Levels**

* **Low Alert**: Bookmarks, history, tabs (limited)
* **Medium Alert**: Active tab, context menus, notifications
* **High Alert**: All sites data, all tabs, downloads, privacy settings

**Mozilla Firefox**

**Accessing Add-ons**

# Via browser  
about:addons  
  
# Via command line  
firefox -P default about:addons

**Firefox-Specific Checks**

1. **Add-ons Manager Analysis**
   * Check "Extensions" and "Themes" sections
   * Look for "Legacy" or unsigned extensions
   * Verify Mozilla Add-ons (AMO) sourcing
2. **Extension Files Examination**

# Firefox profile location  
ls -la ~/.mozilla/firefox/\*/extensions/  
  
# Check extension database  
cat ~/.mozilla/firefox/\*/extensions.json | jq '.addons[].id'

1. **About:support Information**
   * Navigate to about:support
   * Check "Application Basics" section
   * Review "Extensions" section for anomalies

**Firefox Permission Categories**

* **API Permissions**: webRequest, cookies, history
* **Host Permissions**: Specific sites vs. all sites
* **Manifest Permissions**: Background scripts, content scripts

**Microsoft Edge**

**Accessing Extensions**

# Via browser  
edge://extensions/  
  
# Via command line  
microsoft-edge --enable-extensions-on-chrome-urls edge://extensions/

**Edge-Specific Checks**

1. **Extension Source Verification**
   * Check if from Microsoft Store or Chrome Web Store
   * Verify developer certificates
   * Review Edge-specific permissions
2. **Security Settings**

# Edge profile location  
ls -la ~/.config/microsoft-edge/Default/Extensions/

**Permission Analysis**

**Understanding Permission Requests**

**Critical Permissions (Immediate Review Required)**

1. **"Read and change all your data on all websites"**
   * Allows reading passwords, personal information
   * Can modify page content and inject scripts
   * Monitor all browsing activity
2. **"Read your browsing history"**
   * Access to all visited websites
   * Can build detailed user profiles
   * Privacy invasion potential
3. **"Manage your downloads"**
   * Can access downloaded files
   * Potential for malware injection
   * File system access
4. **"Change your privacy-related settings"**
   * Can disable security features
   * Modify cookie and tracking settings
   * Compromise browser security

**Moderate Risk Permissions**

* Access to specific websites
* Read and modify bookmarks
* Notifications and context menus
* Active tab information

**Generally Safe Permissions**

* Storage (limited local storage)
* Idle state detection
* Display unlimitedStorage warnings

**Advanced Detection Techniques**

**1. Network Traffic Analysis**

Monitor extension network activity:

# Use netstat to check connections  
netstat -an | grep :443  
netstat -an | grep :80  
  
# Monitor DNS queries  
sudo tcpdump -i any port 53  
  
# Use browser developer tools  
# F12 -> Network tab -> Monitor XHR requests

**2. File System Monitoring**

Track extension file changes:

# Monitor extension directories  
inotifywait -m -r ~/.config/google-chrome/Default/Extensions/  
  
# Check for suspicious files  
find ~/.config -name "\*.js" -newer /tmp/reference\_file

**3. Process Analysis**

Monitor extension processes:

# Check browser processes  
ps aux | grep -E "(chrome|firefox)" | grep -v grep  
  
# Monitor resource usage  
top -p $(pgrep chrome)

**4. Registry Analysis (Linux equivalent)**

Check browser configuration files:

# Chrome preferences analysis  
cat ~/.config/google-chrome/Default/Preferences | jq '.extensions'  
  
# Firefox prefs analysis   
cat ~/.mozilla/firefox/\*/prefs.js | grep extension

**Real-World Examples**

**Case Study 1: Cyberhaven Extension (December 2024)**

**Attack Vector**: Compromised developer accounts via phishing  
**Impact**: 400,000 users affected  
**Malicious Behavior**:

* Data exfiltration to attacker servers
* Cookie and credential harvesting
* Silent payload downloads

**Detection Signs**:

* Extension update without user notification
* New network connections to unknown domains
* Increased memory usage
* Unexpected permission requests

**Case Study 2: PDF Toolbox Extension**

**Attack Vector**: Legitimate extension turned malicious  
**Impact**: 2+ million users  
**Malicious Behavior**:

* Loading arbitrary code from suspicious websites
* Injecting ads and affiliate links
* Tracking user behavior across sites

**Detection Signs**:

* High user ratings but recent negative reviews
* Permission creep over time
* Code obfuscation in updates

**Case Study 3: Fake VPN Extensions**

**Attack Vector**: Typosquatting and fake functionality  
**Impact**: Thousands of users  
**Malicious Behavior**:

* No actual VPN functionality
* Data harvesting and selling
* Cryptocurrency mining

**Detection Signs**:

* Similar names to legitimate VPN services
* Excessive permissions for claimed functionality
* No clear privacy policy or terms of service

**Automated Tools**

**1. Browser Extension Analyzers**

**CRXcavator (Chrome Extensions)**

# Visit https://crxcavator.io/  
# Enter extension ID for automated analysis  
# Reviews permissions, code quality, and risk factors

**Mitigation Strategies**

**Immediate Actions**

1. **Disable Suspicious Extensions**
   * Don't delete immediately (for forensics)
   * Disable to prevent further damage
   * Monitor for persistence
2. **Change Passwords**
   * All accounts accessed during extension runtime
   * Enable 2FA where possible
   * Check for unauthorized access
3. **Clear Browser Data**
   * Cookies and sessions
   * Cached files
   * Stored passwords (re-enter manually)

**Long-term Prevention**

1. **Regular Audits**
   * Monthly extension reviews
   * Automated monitoring setup
   * Permission change alerts
2. **Installation Policies**
   * Only install from official stores
   * Read reviews and check permissions
   * Verify developer reputation
3. **Browser Configuration**
   * Enable security warnings
   * Disable auto-updates for critical extensions
   * Use separate profiles for different activities

**Conclusion**

Identifying suspicious browser extensions requires a combination of systematic analysis, technical investigation, and ongoing monitoring. By following this guide and implementing the recommended tools and processes, you can significantly reduce the risk of browser extension-based attacks.

**Key Takeaways**

1. **Regular auditing is essential** - Extensions can change behavior over time
2. **Permissions matter** - Always review and understand what access you're granting
3. **Trust but verify** - Even popular extensions can be compromised
4. **Monitor continuously** - Set up automated alerts for extension changes
5. **Stay informed** - Follow security advisories and threat intelligence