TIR-20260211 The Risk of Downloading Chrome Extensions in the Workplace

2/11/2026

Prepared for:

Aspire Technology Partners
25 James Way
Eatontown, NJ 07724

NOTICE:

This document is marked TLP: CLEAR, allowing recipients to share this information globally without any disclosure limitations.

This report is governed by the terms outlined in the Master Services Agreement (MSA) or any other master agreement between Aspire Technology Partners and the client receiving this report, along with the Statement of Work (SOW) or Order detailing the services that led to its creation.

Contributor(s)

Portia S. Cole
CTI Threat Researcher
Aspire Technology Partners
pcole@aspiretransforms.com

TABLE OF CONTENTS

Executive Summary

Browser extensions have quietly become one of the least monitored attack paths inside corporate environments. They look harmless and they promise convenience, yet once inside the browser, they operate with the same access level as the employee who installed them. That means access to internal portals, SaaS applications, client data, cloud storage, and active sessions. There is no phishing email involved, just a user installing the wrong extension.

Recent public reporting confirmed that more than 900,000 users downloaded malicious Chrome extensions that impersonated a legitimate AI tool. Those extensions harvested ChatGPT and DeepSeek conversations and sent browsing data to a remote command and control server. One even carried a “Featured” badge in the Chrome Web Store. It looked legitimate, but it was collecting data in the background.

Browser extensions promise productivity, but recent Aspire cases show how quickly they can turn into a security problem. In every case our controls caught it, but installing random Chrome extensions at work still opens the door for someone else to operate under a trusted user’s name.

TIR SUMMARY

ASPIRE

TLDR;

- Recent customer cases involved employees installing malicious Chrome extensions on corporate devices.
- In one case, a fake VPN collected advertising data, AI conversations, and user interaction data.
- The malicious file was detected and quarantined by endpoint security before confirmed data loss occurred.
- Recent public campaigns have shown that browser extensions can harvest ChatGPT content, session data, and browsing activity at scale.
- Extensions operate inside trusted user sessions and often avoid traditional alerts because activity appears legitimate.
- Permission prompts such as “Read and change all data on all websites” or access to clipboard and history are red flags.
- Chrome Web Store availability does not guarantee safety, as malicious extensions have remained available for months or years.
- Browser extensions in the workplace should be governed like enterprise software, not treated as harmless productivity tools.
- Allowing unrestricted extension downloads creates a low-noise access path that attackers actively exploit

What Are Browser Extensions and How Do They Function

A browser extension is a software program that installs directly into a web browser. Its purpose is to add functionality, modify web content, automate tasks, or integrate external services into the browsing experience. Once installed, the extension runs inside the browser environment and interacts with web pages.

Extensions request permissions when installed. Many ask for the ability to read and change data on websites. That language is broad for a reason. It allows the extension to access page content, monitor activity, modify displayed information, and interact with user sessions. If granted, those permissions apply wherever the user browses.

All major browsers support extensions. While this report focuses heavily on Chrome due to recent malicious activity trends, browser extensions across platforms function in a similar way. They operate within the browser process and inherit the user's access level to online resources.

Chrome

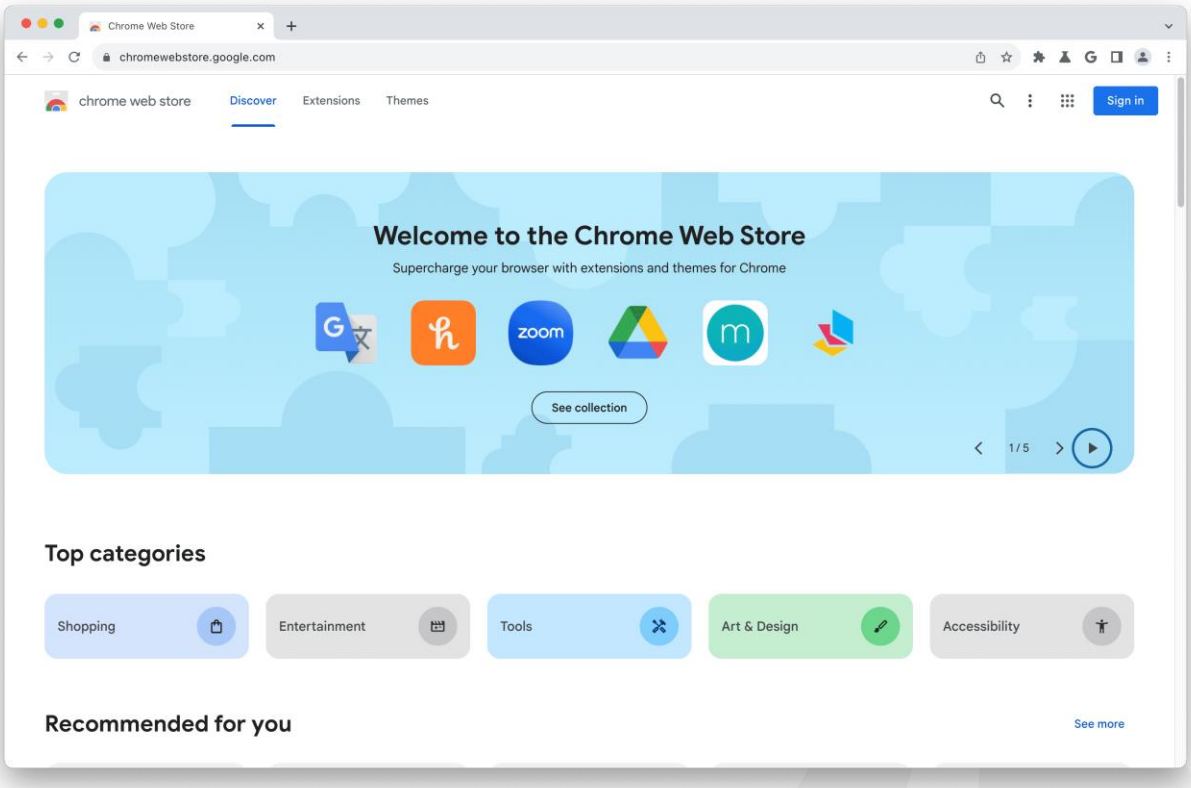
Chrome extensions are distributed primarily through the **Chrome Web Store**. Google reviews submissions, but malicious extensions have **repeatedly bypassed moderation controls** because the extensions behave normally at first. In several public cases, extensions remained available for months or even years before removal.

Chrome extensions can:

- Monitor URLs visited by the user
- Read and modify webpage content
- Access browser storage
- Communicate with external servers
- Inject scripts into active pages

When an extension runs inside a browser session, security tools often see only normal encrypted traffic. The extension's activity blends in with legitimate browsing.

Image 1: Chrome Web Store



WHY CHROME EXTENSIONS ARE APPEALING

Employees download Chrome extensions because they make work easier. The extensions block ads, clean up tabs, save passwords, connect apps, and crank out AI-written emails in seconds.

When you're slammed at work, anything that saves time feels like a win. A tool that shaves off a few minutes or adds an AI sidebar doesn't seem too risky, and most people click past the permission screen without thinking twice.

Common reasons employees install extensions include:

- AI chat overlays for productivity
- VPN services for remote browsing
- Ad blockers
- Screen recorders
- File converters
- Translation tools
- Browser customization utilities

The problem is not the desire for efficiency. The problem is that most users do not evaluate who built the extension, what permissions it requests, or where its data flows once installed.

Image 2: How Chrome Extensions Work

Why Downloading Chrome Extensions in the Workplace Is Dangerous

Chrome extensions operate inside a trusted user session. Once installed, the extension acts with the same privileges as the user. If the user can access Salesforce, internal ticketing systems, cloud storage, or financial tools, the extension can see that activity.

As stated earlier, security tools often treat browser activity as normal behavior. Security tools watch for bad files, strange traffic, and suspicious logins. A browser extension runs after the user is already signed in, inside normal encrypted web sessions, so to most defenses it just looks like regular activity.

If an extension becomes malicious, an attacker can monitor browsing activity, harvest session tokens, scrape data from internal applications, or quietly exfiltrate information. Access can persist as long as the extension remains installed. Some malicious extensions have remained active in public stores for extended periods before detection.

The direct attack path looks like this:

- User installs extension
- Extension requests broad permissions
- Extension communicates with remote server
- Attacker receives browsing data or tokens
- Attacker impersonates user session

Aspire Case Studies

Case #1 - User Installs AI Themed Chrome Extension with Malicious JavaScript

An employee installed a Chrome extension that appeared to be related to AI functionality. Shortly after installation, SentinelOne detected malicious JavaScript files tied to the extension directory. The files were flagged as a known information stealing variant.

The parent process was chrome.exe. The activity resolved to chataigpt[.]pro. Multiple endpoints showed related activity. No additional suspicious applications were installed. The extensions were removed and devices were remediated.

The SOC contained the threat before confirmed data exfiltration. Had the extension remained installed, it could have harvested session information from cloud services. The user could have reviewed the extension's publisher and external reporting before installation.

Case #2 Fake VPN Extension Harvesting Browser Data

In another incident, a user installed a browser based VPN service marketed as a privacy tool. Cisco AMP detected a trojanized extension file within the Chrome extensions cache.

The SOC's analysis revealed that the extension collected advertising data, AI conversation content, and user interactions. The associated domain 1clickvpn[.]com was blocked. The extension was removed and follow up scans returned clean.

The user believed they were improving privacy. Instead, they introduced a surveillance tool into their browser session. Installing only verified VPN services from established vendors could have reduced risk.

Case #3 Malicious AI Sidebar Attempting Command and Control

Cisco Umbrella blocked fifty outbound connections to deepaichats[.]com over a two day period. The domain was categorized as Malware and had multiple threat intelligence flags.

The user had installed "Chat GPT for Chrome with GPT-5, Claude Sonnet & DeepSeek AI." The extension ID matched public reporting tied to a malicious AI impersonation campaign. The extension attempted periodic communication with its command and control infrastructure.

The SOC added the domain to the global block list, initiated a CrowdStrike on demand scan, and reviewed the device in EDR. The user removed the extension. No further detections were observed.

This case mirrored public research describing extensions that exfiltrated ChatGPT and DeepSeek conversations. Because Umbrella blocked outbound traffic, the organization avoided deeper compromise.

Recent Attacks

OX Security's 900,000 User AI Chat Theft Campaign

In late December 2025, researchers at OX Security discovered a campaign involving two malicious Chrome extensions impersonating a legitimate tool from a company called AITOPIA. These malicious extensions were downloaded more than 900,000 times and exfiltrated user data (including ChatGPT and DeepSeek conversations) to attacker-controlled infrastructure. The threat actors stole sensitive AI chat histories and browser activity by requesting broad permissions under the guise of normal functionality. The attackers also abused the Lovable AI web development platform to host misleading privacy policies and hide their identity, making attribution difficult.

Note: There isn't a clear public attribution to a named nation-state or tracked threat group for this specific malicious extension campaign. The threat actors were anonymous and were using infrastructure anonymization techniques to avoid tracing.

LayerX Security's 16 Fake ChatGPT Extension Campaign

In January 2026, cybersecurity researchers from LayerX Security uncovered a coordinated set of at least 16 malicious browser extensions marketed as ChatGPT productivity tools. These extensions were designed specifically to steal ChatGPT session authentication tokens, which effectively allows attackers to hijack active user sessions and access stored AI chat data and account access. The extensions were **published on the official Chrome Web** Store and in some cases on Microsoft Edge's add-ons marketplace. While individual download counts were smaller in this campaign, the coordinated nature and shared malicious behavior profile point to a single threat actor crafting multiple add-ons to broaden distribution.

LayerX did not publicly name the specific threat actor organization behind these extensions, and to date there is no confirmed linkage to a known tracked threat group in public reports. The campaign is attributed generically to unidentified cybercriminals abusing browser extension platforms.

ASPIRE'S RECOMMENDATIONS & HOW TO SPOT RED FLAGS

Malicious Chrome extensions rarely announce themselves as malicious. The warning signs are usually visible before installation, but only if someone slows down and reads the permission screen. The installation prompt often tells the real story.

Red flags include:

- The extension requests permission to **read and change all data on all websites**
- It asks to access **clipboard content, browsing history, or downloads** without a clear functional reason
- A simple utility requesting broad system-level access
- Permissions that feel bigger than the task the extension claims to perform
- Vague privacy policies that mention "anonymous data" but do not explain what is collected
- Recently created developer accounts with unusually high download counts
- Reviews mentioning redirects, popups, or unexpected browser behavior
- Extensions that open new tabs or redirect to external sites immediately after installation
- Extensions that communicate with unfamiliar domains in the background

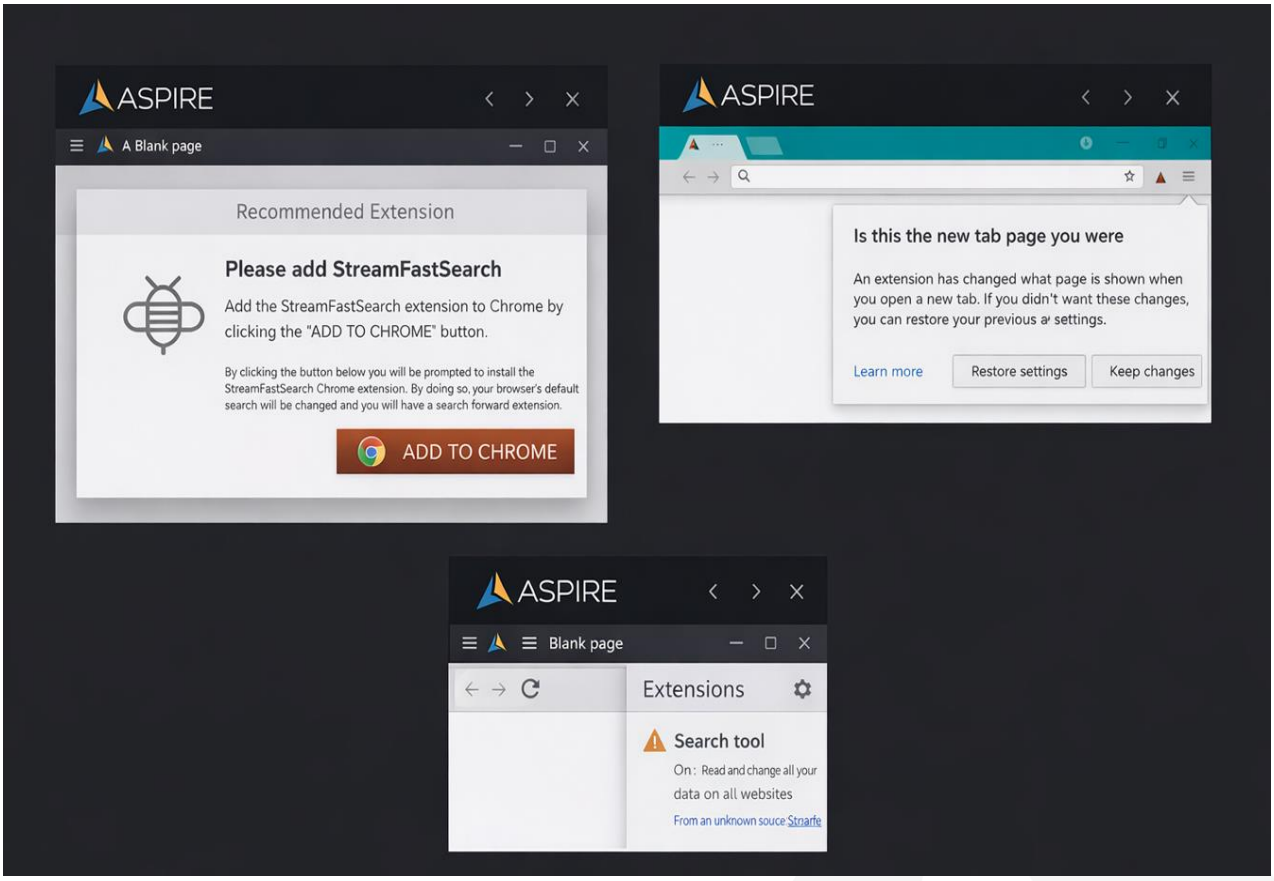
Permissions should always match purpose. An ad blocker does not need access to clipboard data. A formatting tool should not require visibility into every website you visit. When access scope exceeds the stated function, that is not normal. It is risk.

Security teams should reinforce this by:

- Training users to read permission prompts before clicking install
- Blocking known malicious domains at the DNS layer
- Monitoring extension directories through EDR
- Maintaining visibility into installed browser extensions across endpoints

These visuals below show realistic browser prompts and warning signs a user may encounter when installing a malicious Chrome extension. They highlight common red flags such as unexpected "Add to Chrome" pop-ups, sudden changes to the browser's new tab page, and extensions requesting broad access like "read and change all data on all websites" from unknown sources.

Image 3: Early Warning Signs of a Compromised Browser



CONCLUSION

Browser extensions are no longer minor productivity tools, but identity adjacent software components operating inside authenticated sessions. That makes them attractive to threat actors seeking low friction access to corporate data.

Organizations in technology, healthcare, financial services, legal services, manufacturing, education, retail, and the public sector frequently rely on browser-based SaaS platforms. In these industries, malicious extensions create exposure to data theft and session hijacking.

Threat actors leveraging this attack path often fall into categories such as financially motivated cybercriminals, data brokers, and operators running spyware campaigns. Public reporting has also shown infrastructure overlaps tied to broader cybercrime ecosystems.

MITRE MAP

Aspire's SOC TTPs

Initial Access	T1204 – User Execution
Command and Control	T1071.001 – Application Layer Protocol: Web Protocol T1071.004 – Application Layer Protocol: DNS
Collection	T1056 – Input Capture
Exfiltration	T1567 – Exfiltration Over Web Services

ASPIRE PROTECTS

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors. Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyberattacks.
- **Aspire Managed Detection and Response (MDR)**

- Accelerate the maturity of your security operations and reduce risk with faster threat detection and response capabilities. Aspire MDR delivers around-the-clock protection across cloud, network, and endpoints in one integrated solution.
- Our team of experts act as an extension of your IT operations to quickly identify and mitigate security threats before they impact your business.

- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

INDICATORS OF COMPROMISE (IOCS)

Aspire's SOC IoCs

Domains

- chataigpt[.]pro
- 1clickvpn[.]com
- deepaichats[.]com
- extensions[.]aitopia[.]ai
- aitopia[.]ai

Extension ID

- fnmihdojmnkclgjpcoonokmkhjpjechg

SUPPORTING DOCUMENTATION

Chrome Extensions: Are you getting more than you bargained for? | SECURITY.COM

Top 5 Browser Extension Security Risks & 5 Ways to Prevent Them

Browser Extension Security Risks and Best Practices

Prevent Breaches by Spotting Malicious Browser Extensions

Chrome extensions are a security nightmare; here's why you should avoid them - The Mac Security Blog

Dangers of Browser Extensions – NOVA Blog

Understand the risks of permissions for Chrome extensions - Chrome Enterprise and Education Help

More Than Half of Browser Extensions Pose Security Risks

Chrome Extension Privacy Concerns - CyberHoot

Browser Extensions: How to Vet and Install Safely | Information Security Office

What Are Browser Extensions? | CrowdStrike

Chrome's new "Proceed with Caution" warning when installing new or untrusted extensions - gHacks Tech News

Chrome Extensions Security Risks Every Business Should Know

Google Chrome Security: Protect Against Malicious Extensions | Adoverse IT

Dozens of malicious extensions for Google Chrome | Kaspersky official blog

Malicious Browser Extensions: An Overlooked Security Threat

Malicious Chrome Extensions Steal ChatGPT Conversations

APPENDIX II: DISCLAIMER

This document and its contents are not intended to serve as legal advice and should not be used as a substitute for it. The results of a Security Risk Assessment are intended to guide the implementation of diligent measures to reduce the risk of potential vulnerabilities being exploited to compromise data.

While the Services and this report may offer information that the Client can use to support its compliance efforts, the responsibility for evaluating and fulfilling compliance obligations rests solely with the Client, not Aspire. This report does not guarantee or assure the Client's compliance with any law, regulation, or standard.