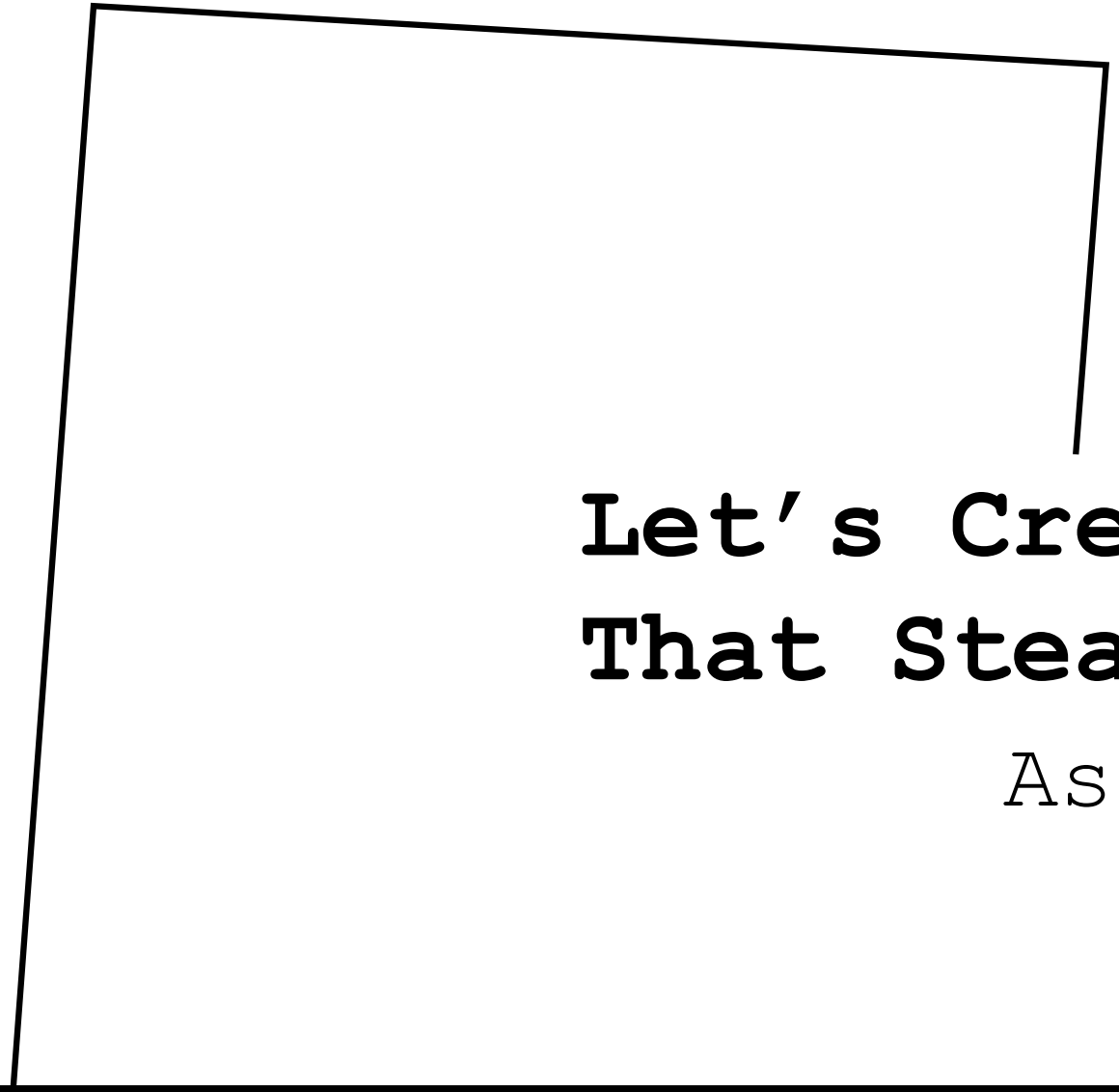
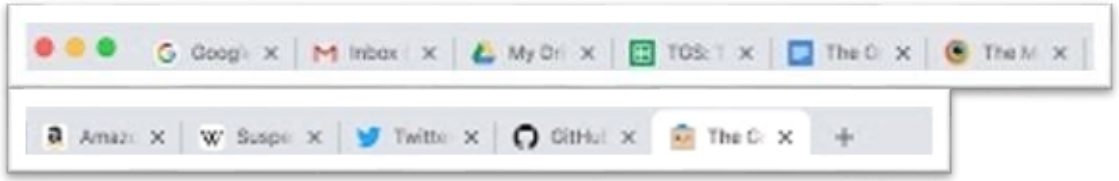
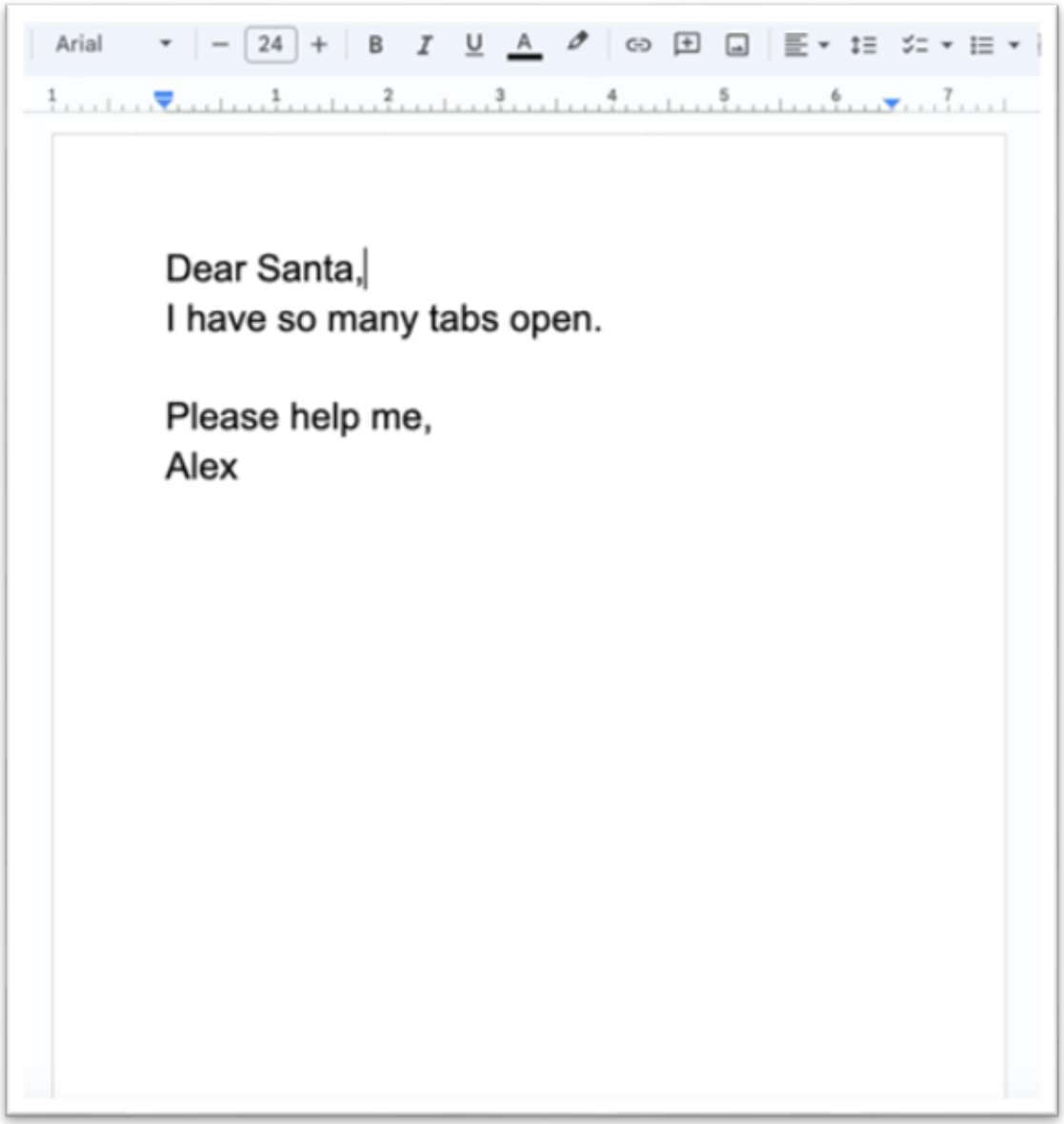


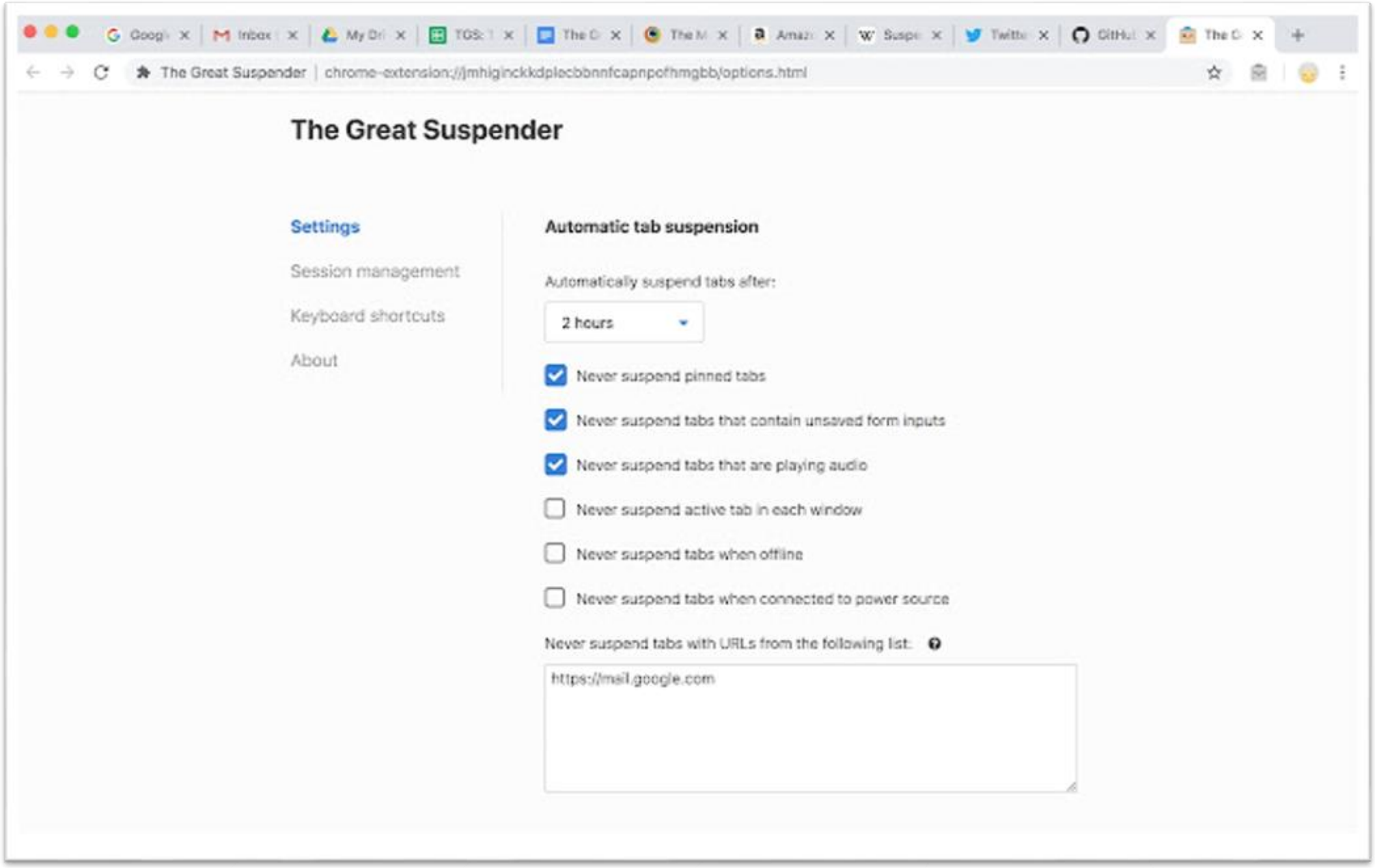
Let's Create an Extension That Steals Everything

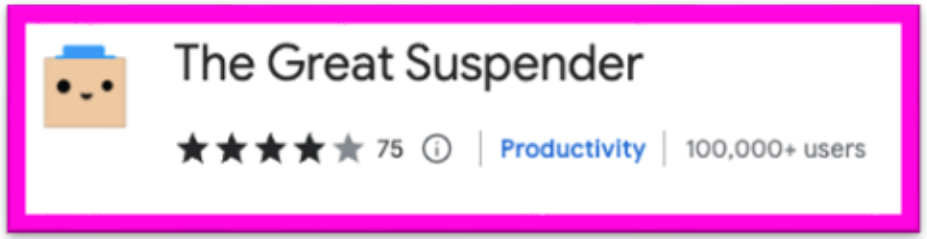
Asaf Shochet Avida

Story Time


Inbox
Twitte
GitHu
The C


Arial
24
Dear Santa,
I have so many tabs open.
Please help me,
Alex


The Great Suspender | chrome-extension://jmhlginckkdplecbbnnfcapnpcfhmgbb/options.html
The Great Suspender
Settings
Session management
Keyboard shortcuts
About
Automatic tab suspension
Automatically suspend tabs after:
2 hours
Never suspend pinned tabs
Never suspend tabs that contain unsaved form inputs
Never suspend tabs that are playing audio
Never suspend active tab in each window
Never suspend tabs when offline
Never suspend tabs when connected to power source
Never suspend tabs with URLs from the following list.
https://mail.google.com


The Great Suspender
75
Productivity
100,000+ users

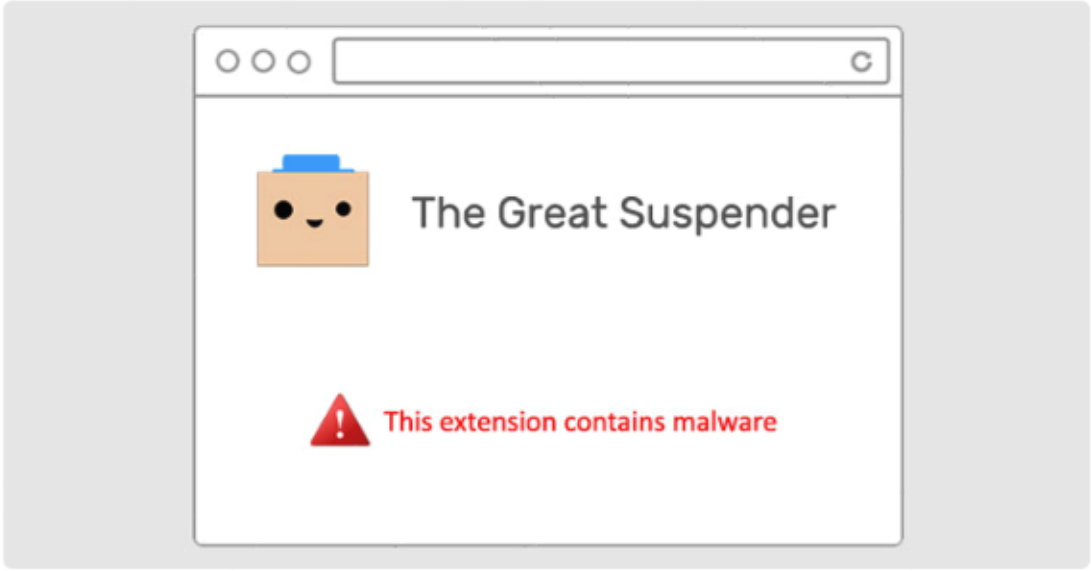
The Hacker News

Subscribe – Get Latest News

Home Data Breaches Cyber Attacks Vulnerabilities Webinars Store Contact

WARNING — Hugely Popular 'The Great Suspender' Chrome Extension Contains Malware

Feb 06, 2021 Ravie Lakshmanan



Google on Thursday removed **The Great Suspender**, a popular Chrome extension used by millions of users, from its Chrome Web Store for containing malware. It also took the unusual step of deactivating it from users' computers.

"This extension contains malware," read a terse notification from Google, but it has since emerged that

Asaf Shochet Avida

Frontend Tech Lead @Evinced

asaf-shochet

frogrammer.net

evinced

Agenda

1. What is a browser extension
2. Build a do-good extension
3. Make it evil 
4. What can we do?
5. Touching summary

What is a web extension?

"Extensions are software programs, built on web technologies that enable users to customize their browsing experience."

https://developer.chrome.com/docs/extensions/

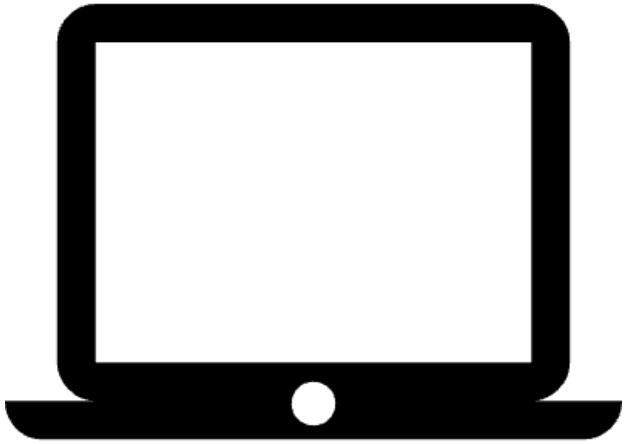
Extension Parts

Manifest

- Metadata
- Behavior
- Permissions

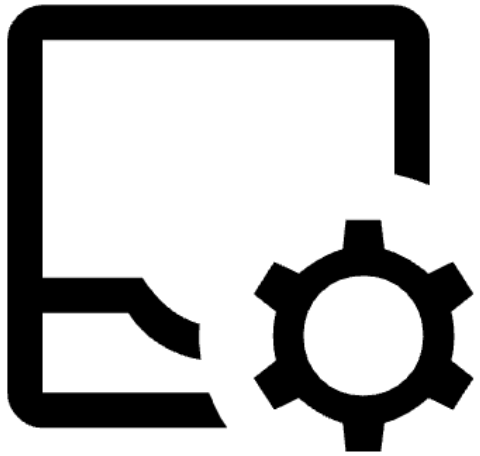
```
{
  "name": "Guardian Angel",
  "version": "6.0.0",
  "description": "Report problemtic sites. Protect your community.",
  "permissions": ["tabs", "activeTab"],
  "host_permissions": ["http://*", "https://*", "<all_urls>"],
  "action": {
    "default_popup": "popup.html",
    "default_icon": {
      "16": "images/frog16.png",
      "32": "images/frog32.png",
      "48": "images/frog48.png",
      "128": "images/frog128.png"
    }
  },
  "icons": {
    "16": "images/frog16.png",
    "32": "images/frog32.png",
    "48": "images/frog48.png",
    "128": "images/frog128.png"
  },
  "background": {
    "service_worker": "background.js"
  },
  "content_scripts": [
    {
      "matches": ["http://*/*", "https://*/*"],
      "js": ["content.js"],
      "run_at": "document_idle",
      "all_frames": false
    }
  ],
  "manifest_version": 3
}
```

Scripts



Content Script

Runs on the page itself



Background Script

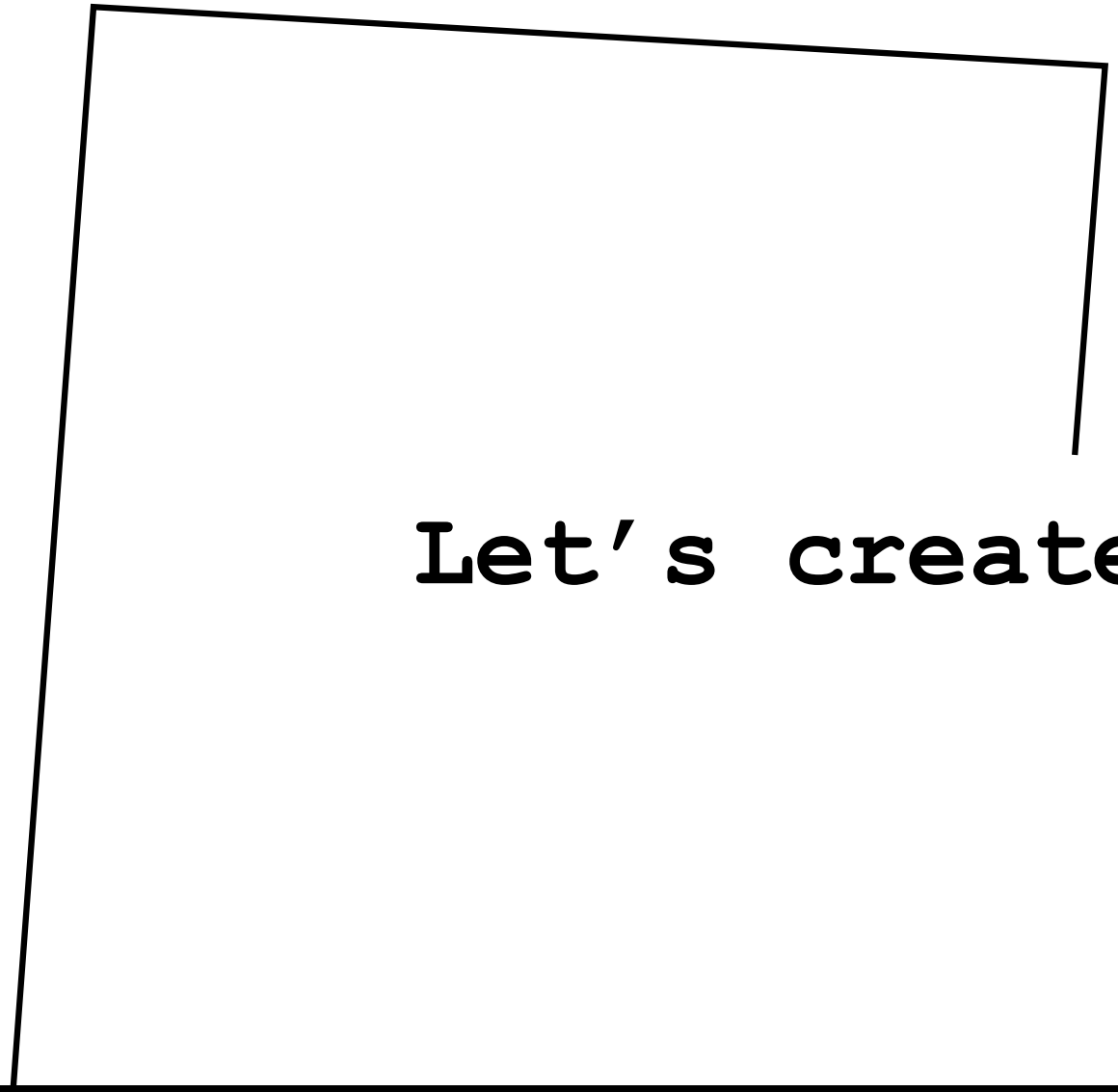
Service worker, no UI

Responds to browser events

Available Permissions (Partial)

- Active Tab
- Downloads
- Geo Location
- Identity
- Web Navigation - Browsing history
- System Storage - Connected storage devices

https://developer.chrome.com/docs/extensions/reference/permissions-list



Let’s create an extension!

Say hi to…

Report harmful content. Protect your freedom.

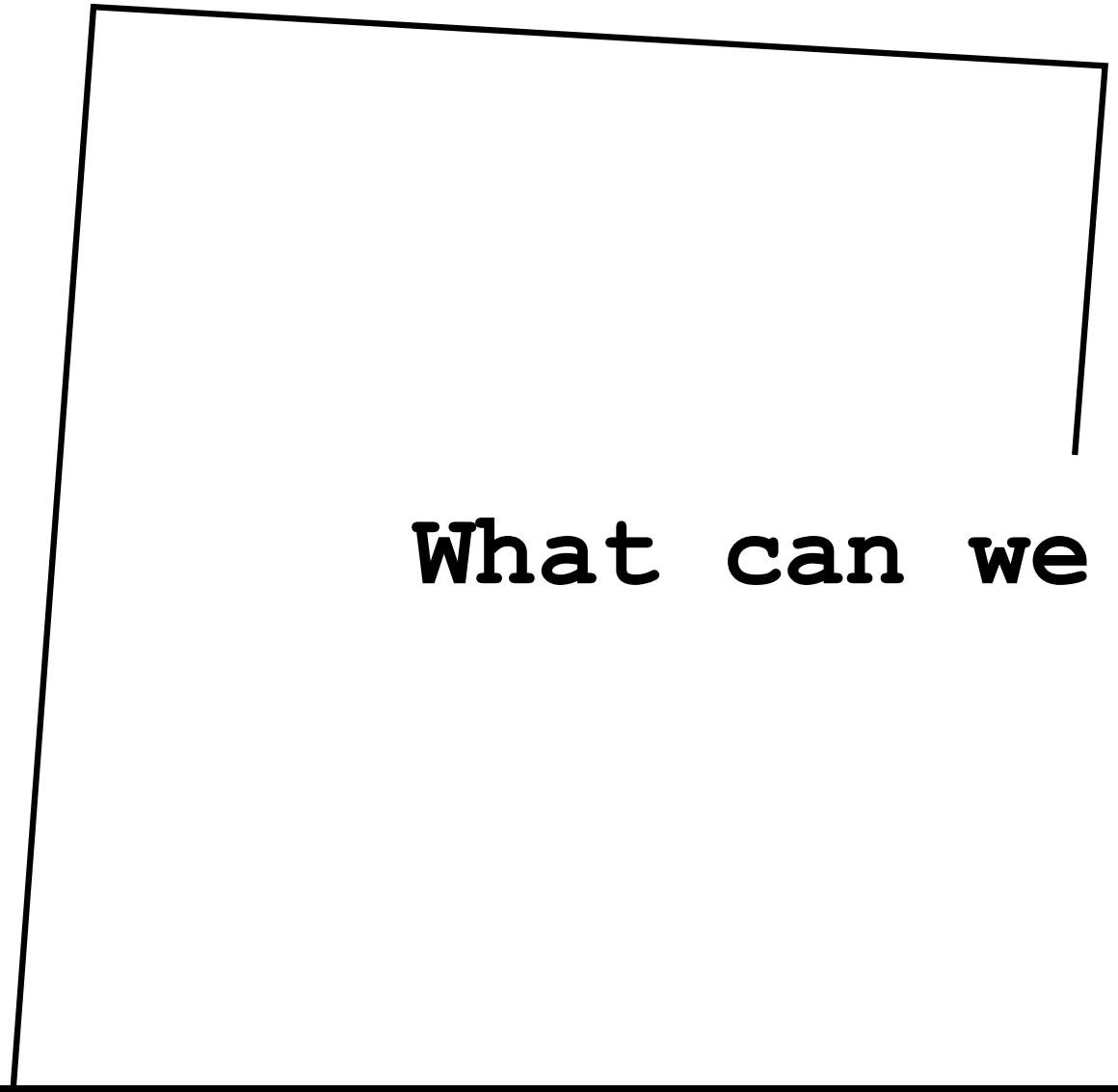
And now

Code Code Code Code Code Code Code Code Code Code Code Code Code
Code Code Code Code Code Code Code Code Code Code Code Code Code
Code Code Code Code Code Code Code Code Code Code Code Code Code
Code Code Code Code Code Code Code Code Code Code Code Code Code
Code Code Code Code Code Code Code Code Code Code Code Code Code
Code Code Code Code Code Code Code Code Code Code Code Code Code
Code Code Code Code Code Code Code Code Code Code Code Code Code
Code Code Code Code Code Code Code Code Code Code Code Code Code
Code Code Code Code Code Code Code Code Code Code Code Code Code
Code Code Code Code Code Code Code Code Code Code Code Code Code
Code Code Code Code Code Code Code Code Code Code Code Code Code
Code Code Code Code Code Code Code Code Code Code Code Code Code
Code Code Code Code Code Code Code Code Code Code Code Code Code
Code Code Code Code Code Code Code Code Code Code Code Code Code
Code Code Code Code Code Code Code Code Code Code Code Code Code
Code Code Code Code Code Code Code Code Code Code Code Code Code
Code Code Code Code Code Code Code Code Code Code Code Code Code
Code Code Code Code Code Code Code Code Code Code Code Code Code
Code Code Code Code Code Code Code Code Code Code Code Code Code
Code Code Code Code Code Code Code Code Code Code Code Code Code
Code Code Code Code Code.

Code.

Github Link

https://github.com/AsafShochet/extension-that-steals-everything

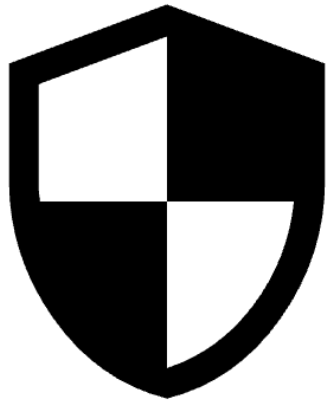


What can we do?

Mv3 To the Rescue?

Performance

Move Background to Service Worker



Security

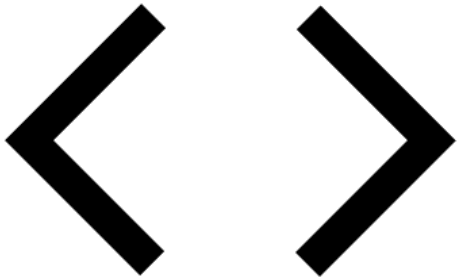
No external code execution

Improve permissions model

```
{
  "name": "Guardian Angel",
  "version": "6.0.0",
  "description": "Report problemtic sites. Protect your community.",
  "permissions": ["tabs", "activeTab"],
  "host_permissions": ["http://*", "https://*", "<all_urls>"],
  "action": {
    "default_popup": "popup.html",
    "default_icon": {
      "16": "images/frog16.png",
      "32": "images/frog32.png",
      "48": "images/frog48.png",
      "128": "images/frog128.png"
    }
  },
  "icons": {
    "16": "images/frog16.png",
    "32": "images/frog32.png",
    "48": "images/frog48.png",
    "128": "images/frog128.png"
  },
  "background": {
    "service_worker": "background.js"
  },
  "content_scripts": [
    {
      "matches": ["http://*/*", "https://*/*"],
      "js": ["content.js"],
      "run_at": "document_idle",
      "all_frames": false
    }
  ],
  "manifest_version": 3
}
```

```
  },
  "background": {
    "service_worker": "background.js"
  },
  "content_scripts": [
    {
      "matches": ["http://*/*", "https://*/*"],
      "js": ["content.js"],
      "run_at": "document_idle",
      "all_frames": false
    }
  ],
  "manifest_version": 3
}
```

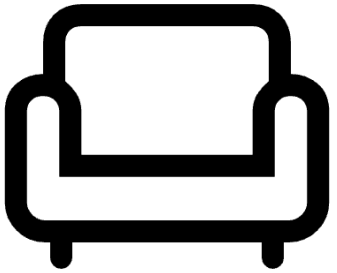
No, Really. How can we defend?



No way to block extension

Allow/Block Extensions

Restrict Permissions



Prefer known vendors

Disable when not needed

Review permissions

Touching Summary

Extensions are powerful

Extensions can be evil

Now what?

Thanks for listening!

Asaf Shochet Avida

asaf-shochet

frogrammer.net

evinced