# Sun City Computer Club

Cyber Security SIG

January 19, 2023

**Questions, Comments, Suggestions welcomed at any time**

**Even Now**

- Audio recording of this session as MP4 file
- Audio recording available at link shown above

# Audio Recording In Progress

**SIG attendees are required to be members of the chartered club sponsoring that SIG.**
**Sun City Community Association By-law**


# At a local Post Office

# LastPass

- Iteration count  200,101
  or 5000  or 500  or 1
- Vault contents

- Consider password manager for most uses
- Pass Phrase with hint for financial

- Language words seldom in random text

- LastPass on new PC from HP
  Windows 11 Home S
  LastPass could not be easily removed until demoting S

# Norton

- Norton, Avast, Lifelock, Avira, AVG, RepurationDefender, Ccleaner
  Symantec
  Gen Digital
  6,450 Lifelock customers
  Credential stuffing?
  Lack of brute force protections?
  December 1 start?
  December 12 secure efforts

766320031548-#user order id <mhdexghkk3274@gmail.com>

To: [redacted]

Tue 17-Jan-23 6:09 AM

We appreciate you [redacted]osing Norton Services

PERIOD: ONE YEAR

ID FOR ORDER # W36H-9S6Y-H6Y3-T26N

REFERENCE ID# 703221456326521

**AREA OF PLAN : Norton.secure**

**COST OF THE PLAN : $ 323.59**

DATE: THE 17th OF JANUARY 2023

Your computerised security plan has been reinstated for the ensuing term, the regularly listed figure has been regulated for backing, and it'll be taken into account for your records within the coming two times" business days. Given that Norton top excellence constantly costs"

Want any change in the plan? OR want to unsubscribe please get connected with us at +1 805 521 4886

Your cooperation is important valued.||

- Easy to gain access to ANYONE's credit report
- "Way to go, your score is highest yet!"

# Experian

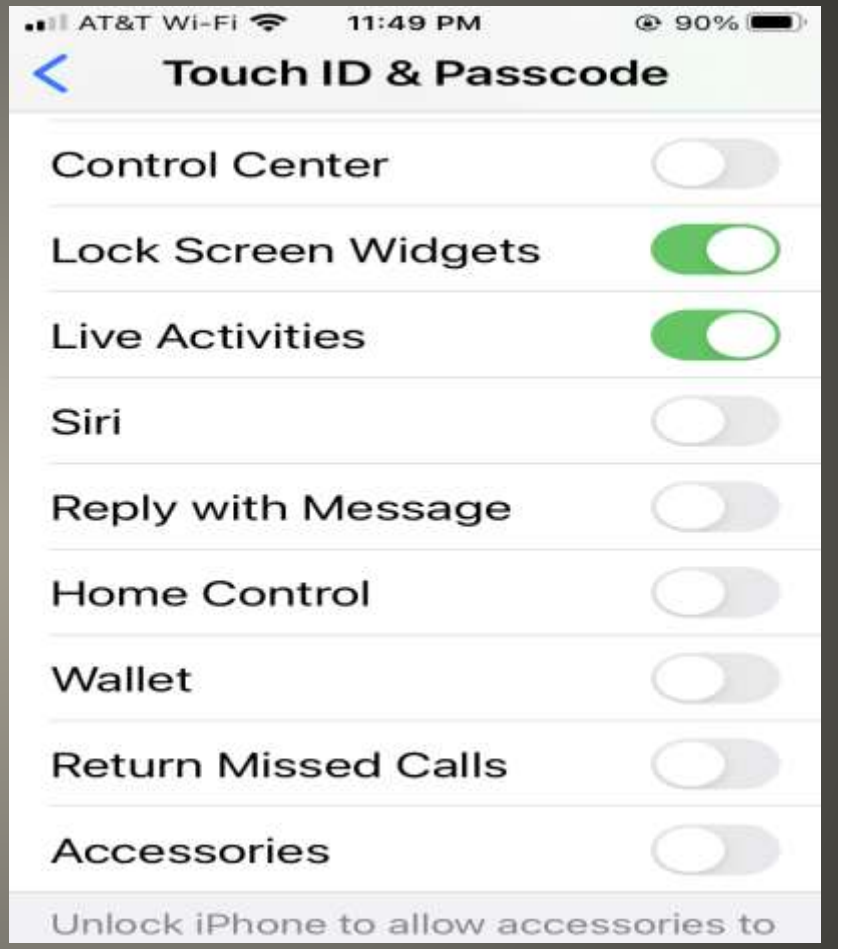
- Control Center access disable while locked
  Why?
  Thieves turn on Airplane Mode
  Bypass lock screen


# iOS settings

# iOS Settings

- FaceID & Passcode
- TouchID & Passcode

- Control Center
  Airplane Mode
- Accessories
  USB Drive
- Wallet



# iOS Settings

- Find My
  Locate device on map
  Play a sound to locate it
  Display message on lock screen
  Remotely erase all data on device

- Find My iPhone


# iOS Settings


# Two Factor Authentication to Apple ID

- Does back tap for Flashlight still work?
  yes

- Reviver Rplates
  GPS location
  Access all user records
  Change some text the plate displays
  Fleet owner access


# Digital License Plates


YBI LD TNL CTR EB (16.13.39)
24 Nov 2022 12:38:03

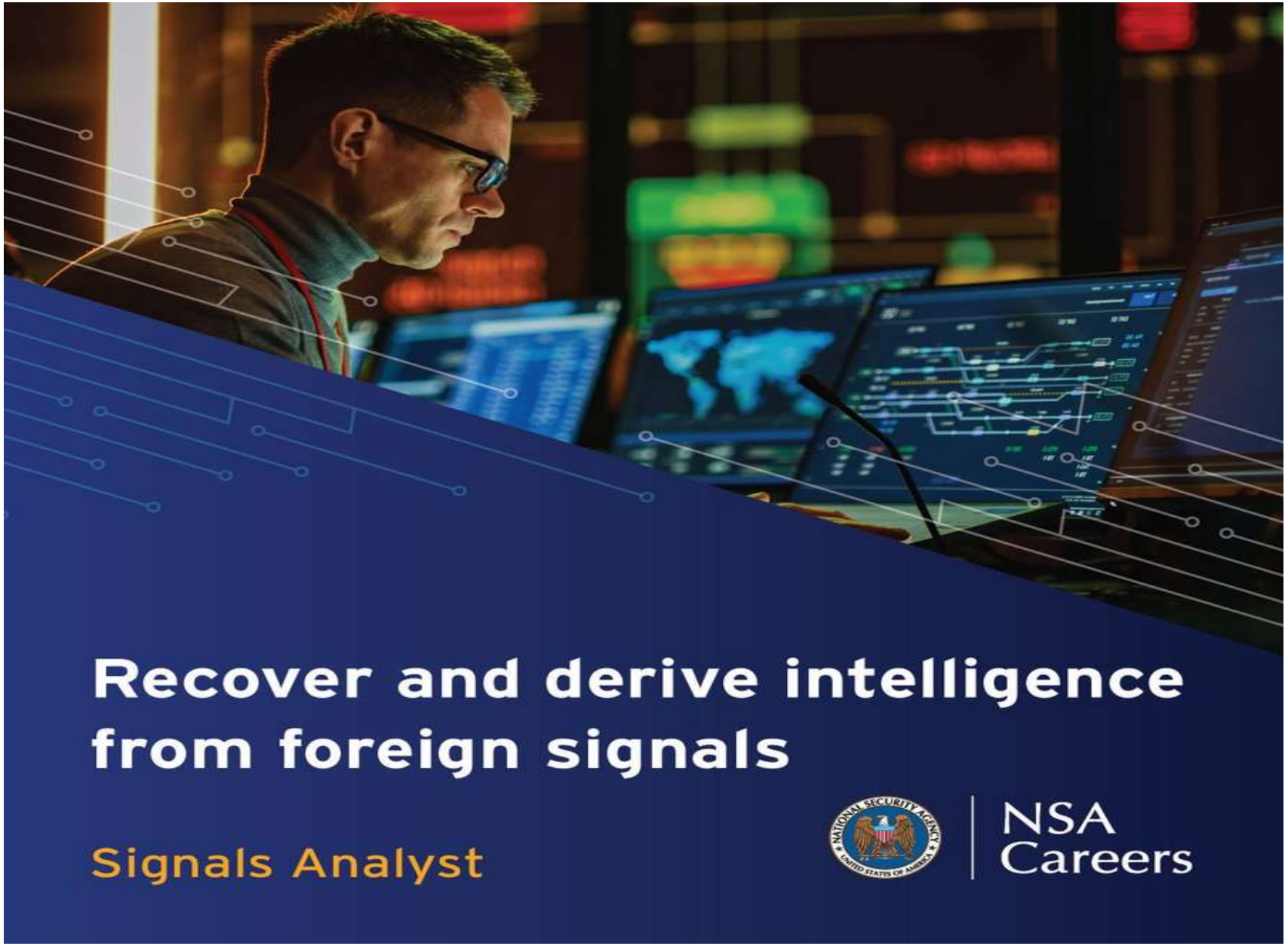
- Netcomm
  Models NF20MESH, NF20, NL1902
  Firmware older than R6B035
- TP-Link WR710N-V1-151022, Archer-CV-V2-160201

```
user@kotr:~/projects/nc20$ ./pwn.py
[*] payload length: 4265
[*] bruteforcing aslr. this could take a while..
.....................................................................
.....................................................................
.....................................................
[*] ohhh? pwned? connecting..


BusyBox v1.30.1 (2022-07-16 10:30:38 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

# 
```

# Netcomm & TP-Link Router vulnerabilities

# Current Issues

- NSA director to Congress
  Renew surveillance powers
  Foreign Intelligence Surveillance Act
  due to expire end of this year
  Section 702 2008 renewed 2018 + 6
  2020 Congress let expire 3 provisions of Patriot Act
- IcedID malware:
  Active Directory compromised in 24 hours
- Fortinet FortiOS SSL-VPN
  Infect government organizations
- Tech hiring bubble now bursting

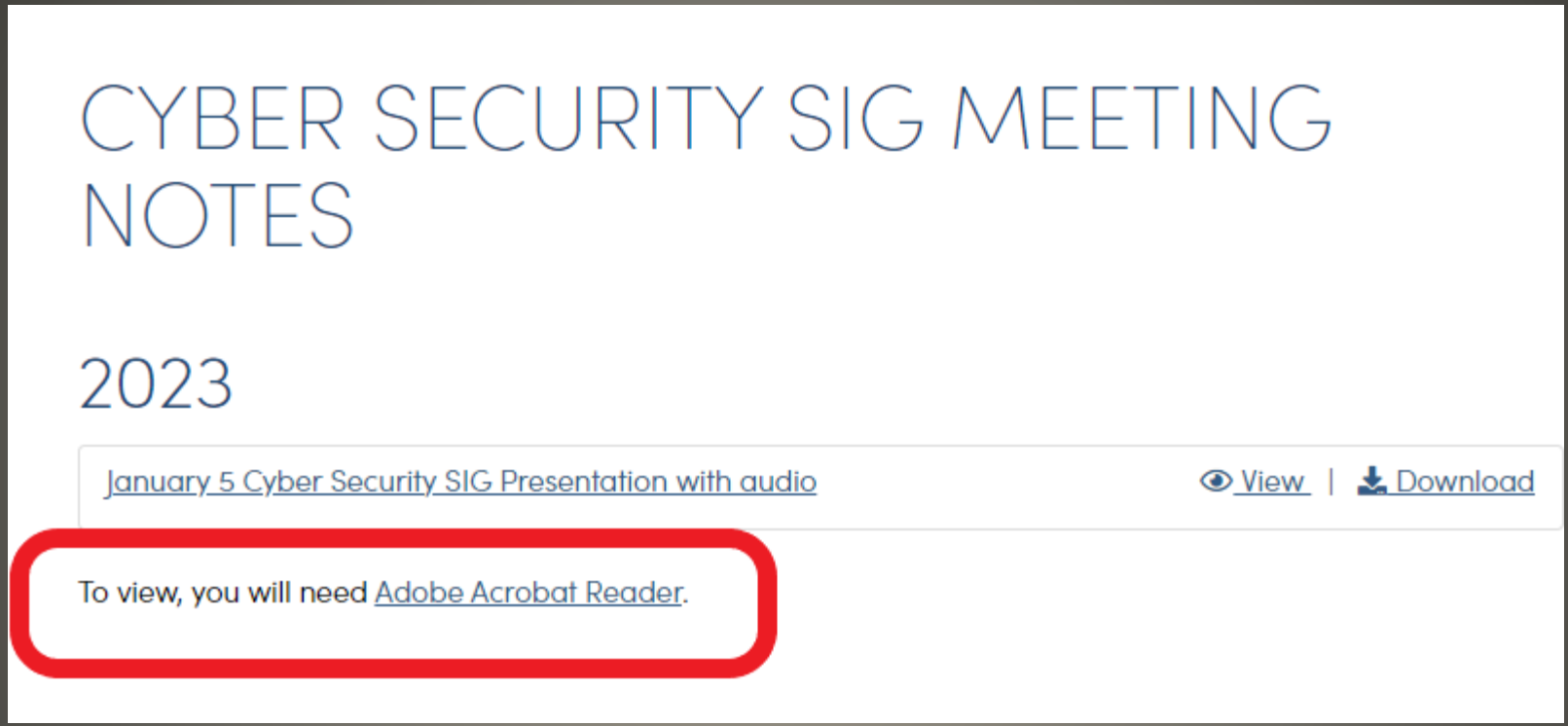

Recover and derive intelligence from foreign signals
Signals Analyst
NSA Careers

# Current Issues

- Android TV box on Amazon
  persistent sophisticated malware in firmware
  T95 Android TV box
- Microsoft retire MSDT
  Microsoft Support Diagnostics Tool  2025
- VLC multimedia player delivering malware
  Poisoning search results
- LastPass, Slack, CircleCI  Insider
- TrustCor CA
- Chromium -> Rust
- ShipManager attack  1,000 vessels
- Montana proposes ban on electric vehicles
- UK Royal Mail outage
- Android 13  clipboard privacy change
- SweepWizzard  multi agency LE raids
- MailChimp breach

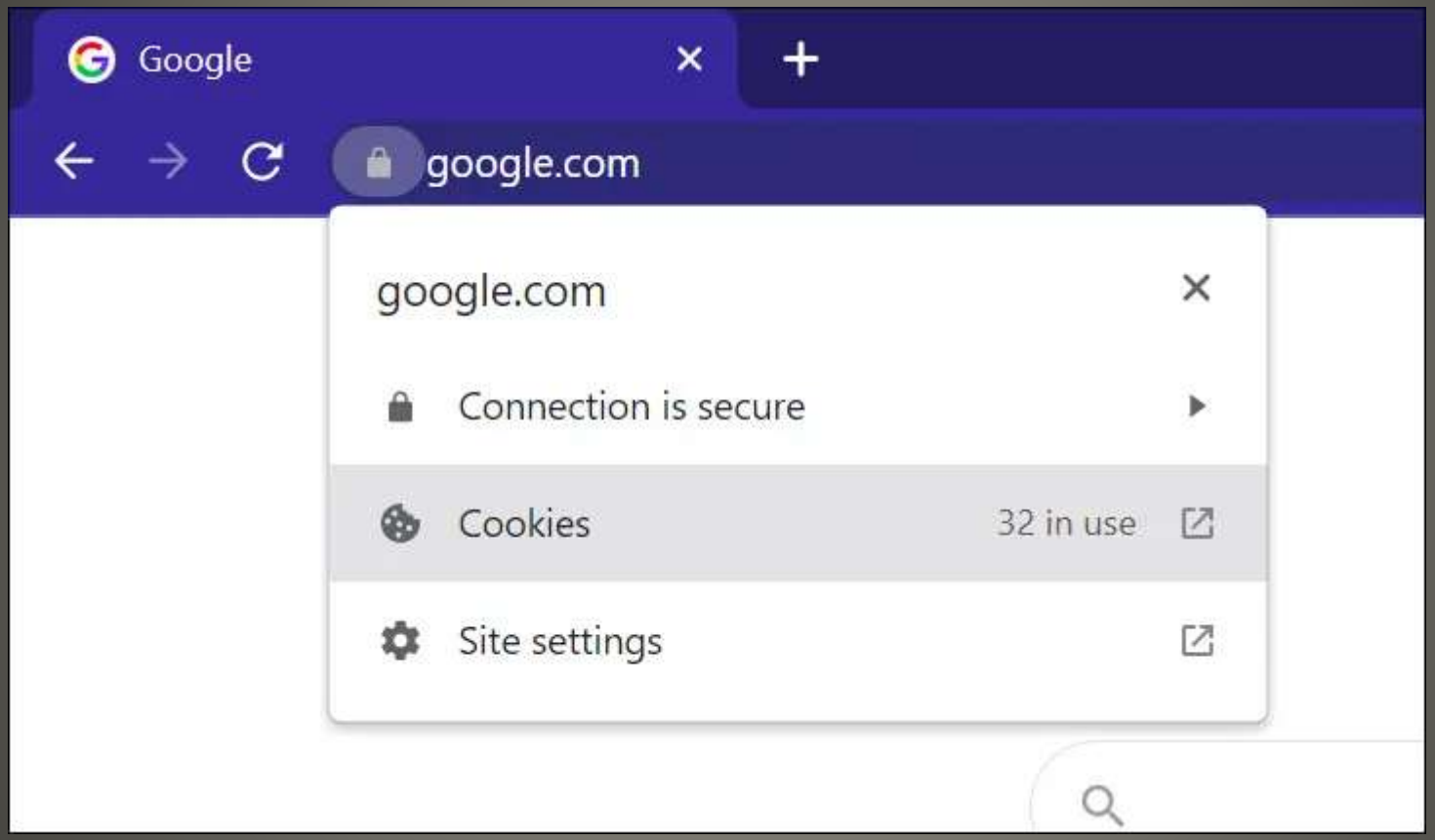
# Current Issues

- Nissan data breach
  Usernames, DoB, Nissan Motor Acceptance Number
  Breach in June  Disclosed  1/16/2023
- New power, New team Bitzlato issue
  Bitzlato  cyber currency exchange
  helps criminals with ransomware payments
  National Cryptocurrency Enforcement Team
  Announced formation October 2021
  Fiscal 2021 Defense Authorization Law
- PayPal sending thousands users credential stuffing attacks notices  12/6/2022 – 12/8/2022
  Investigation results posted 12/20/2022
- Initial Access Brokers market booms



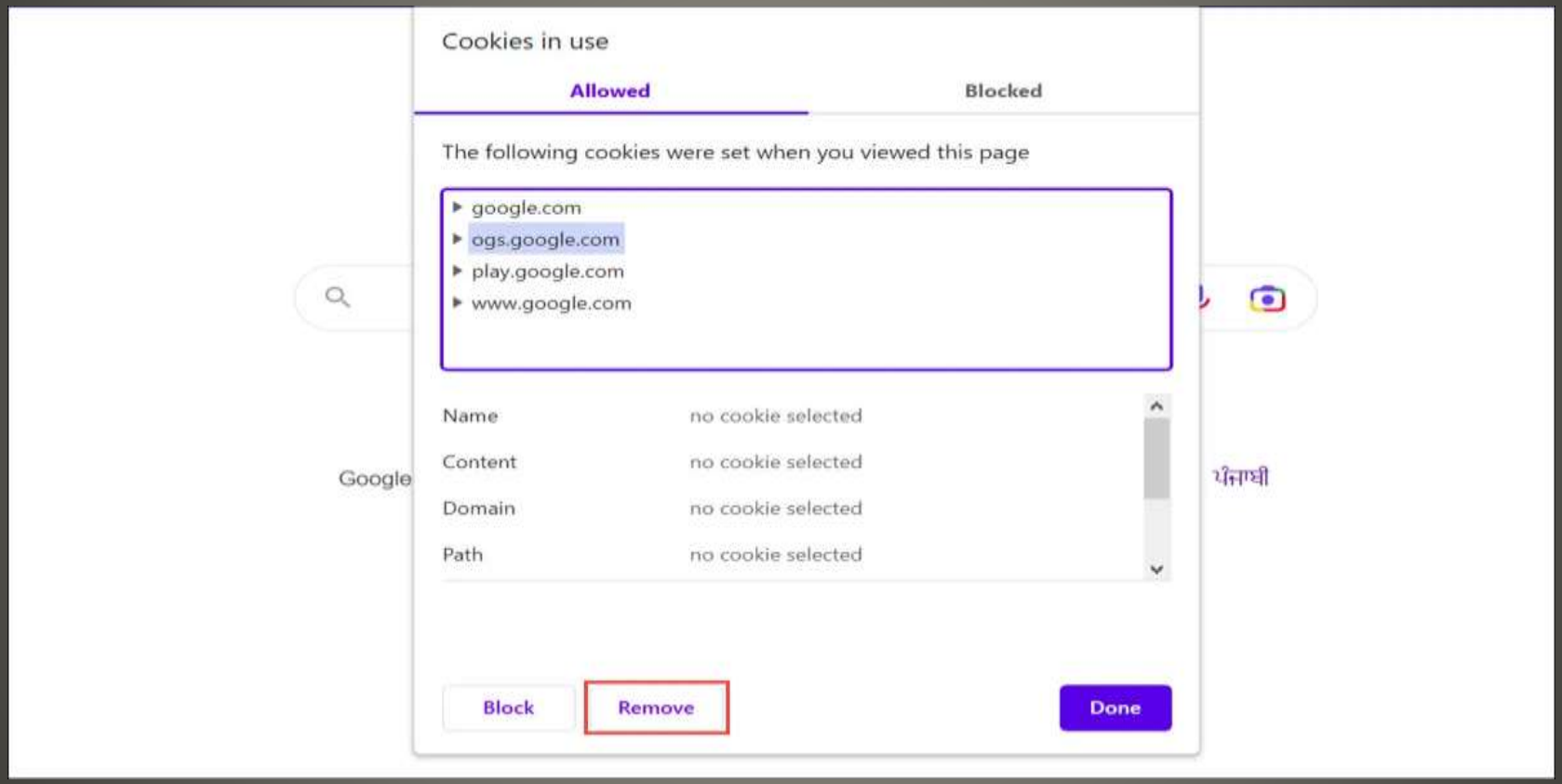

**Not really need**

- Chrome



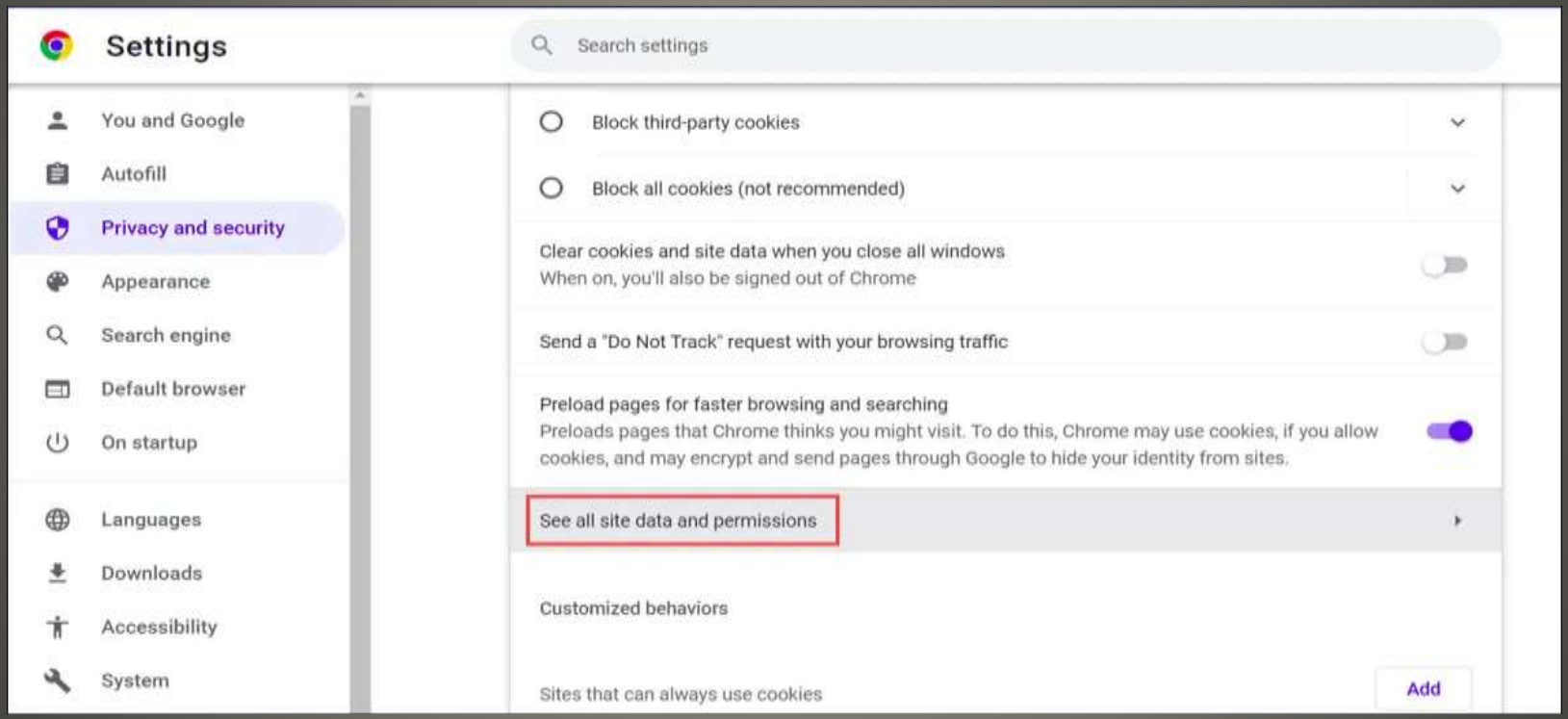

# Clear cookies per site

- Chrome



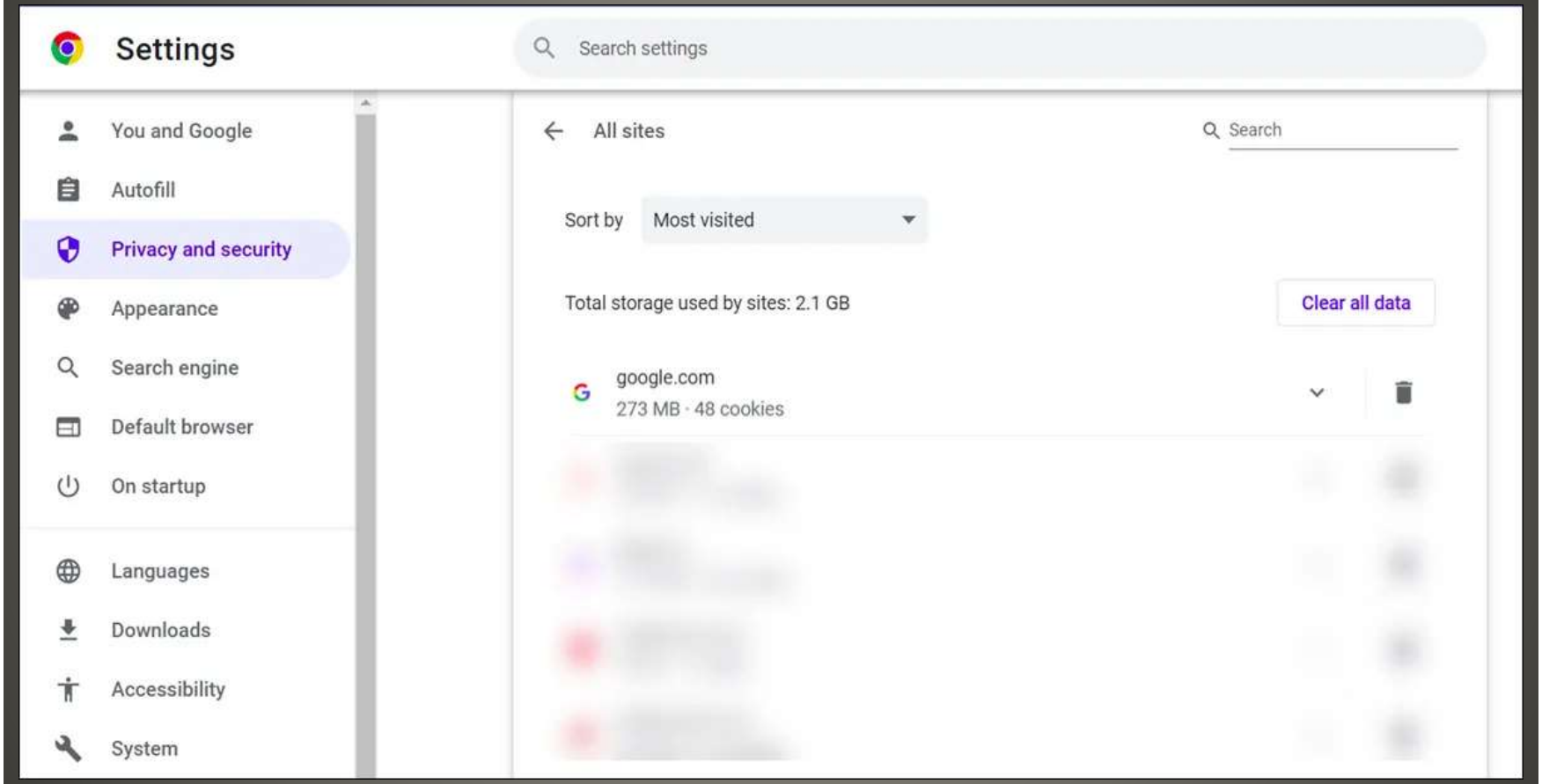

# Clear Cookies per site

- Chrome
  chrome://settings/cookies



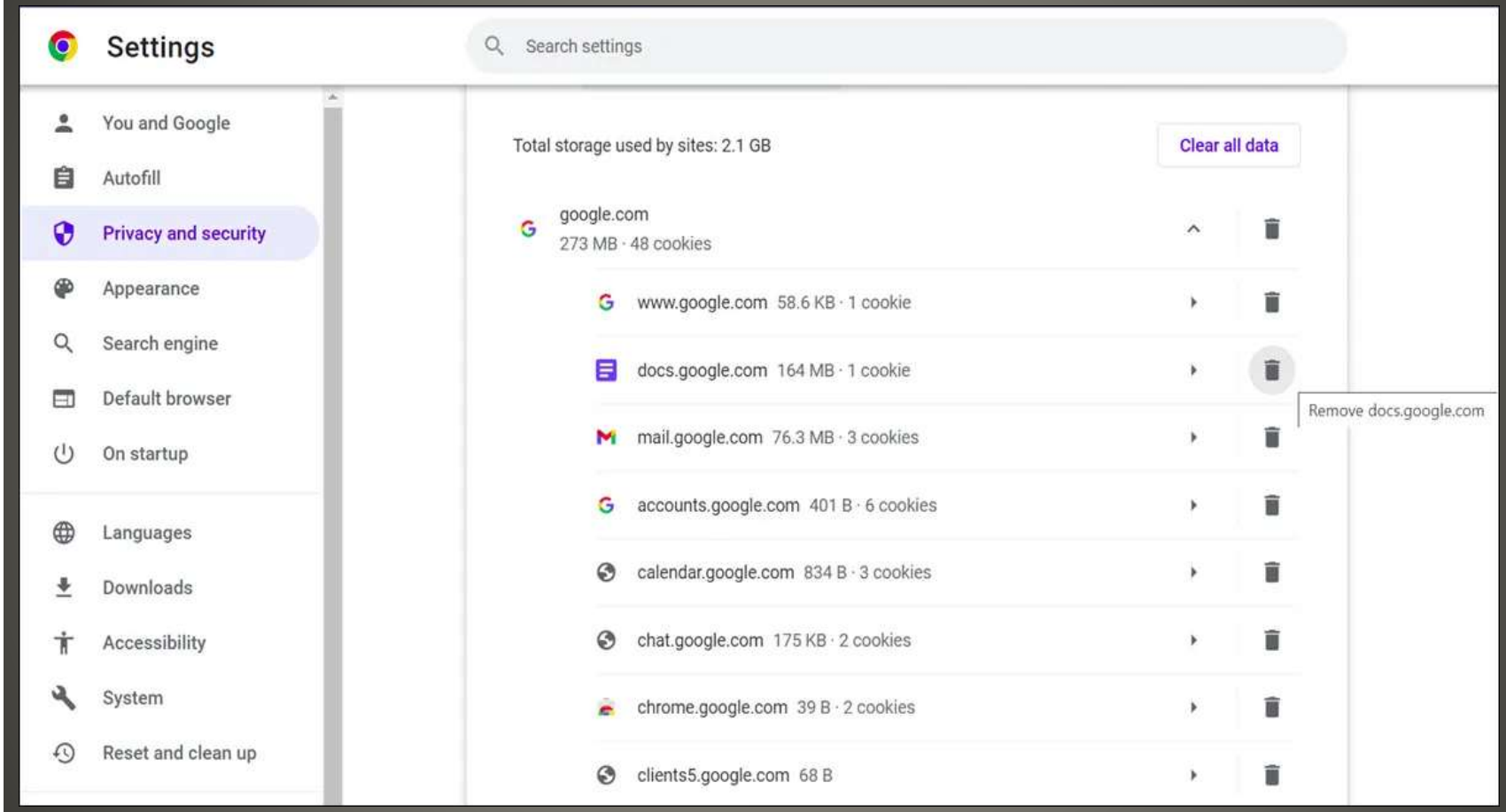

# Clear cookies per site

- Chrome



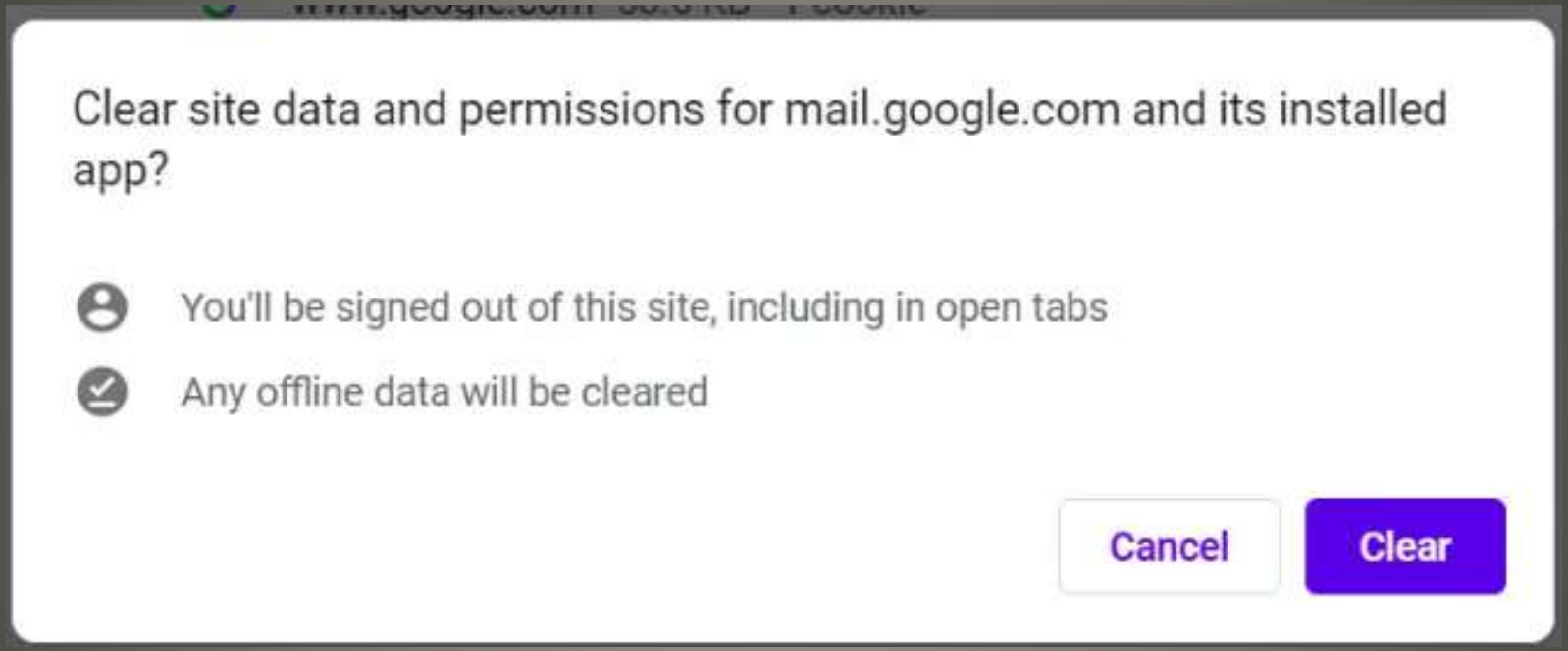

# Clear cookies per site

- Chrome



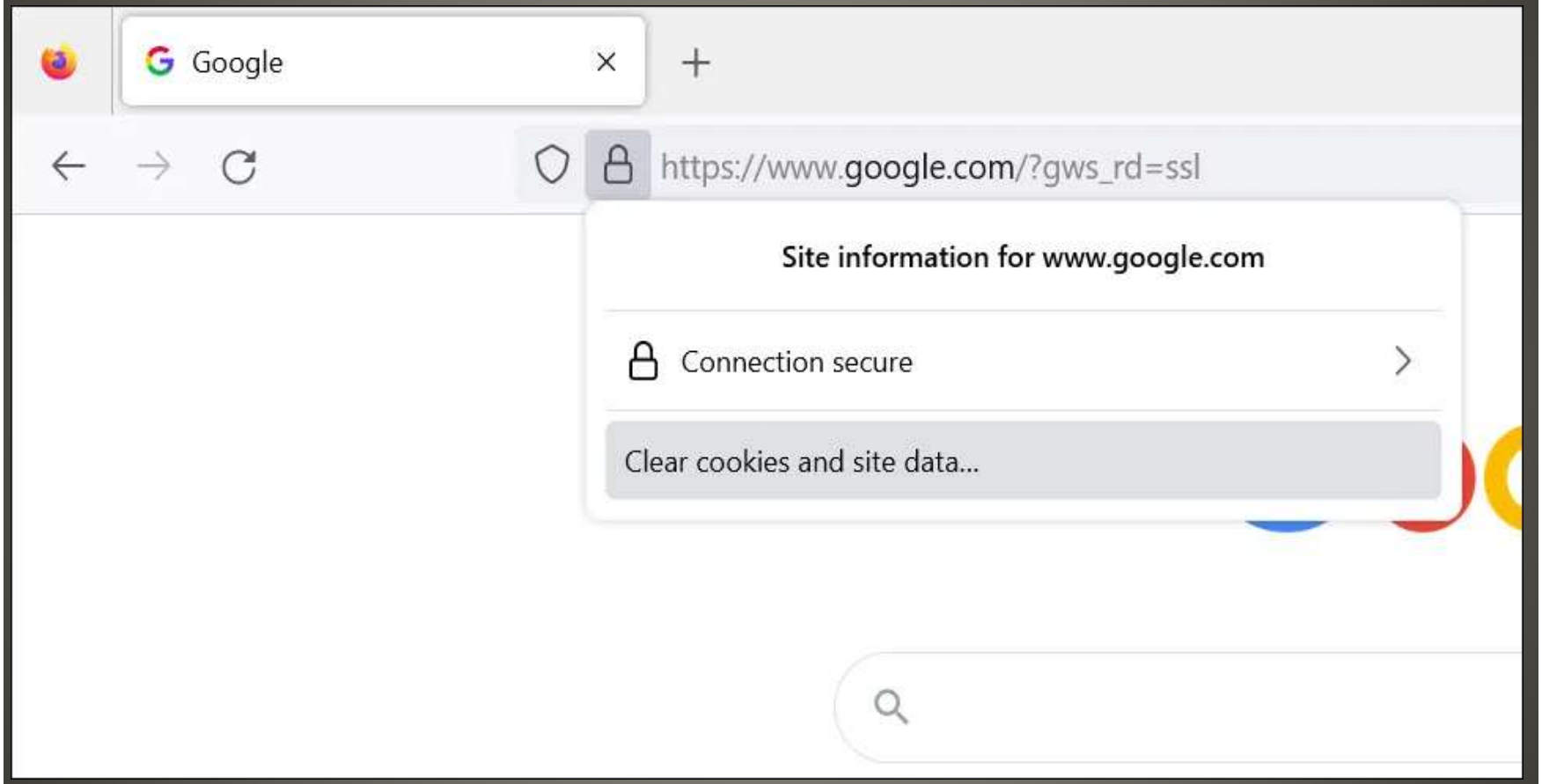

# Clear cookies per site

- Chrome



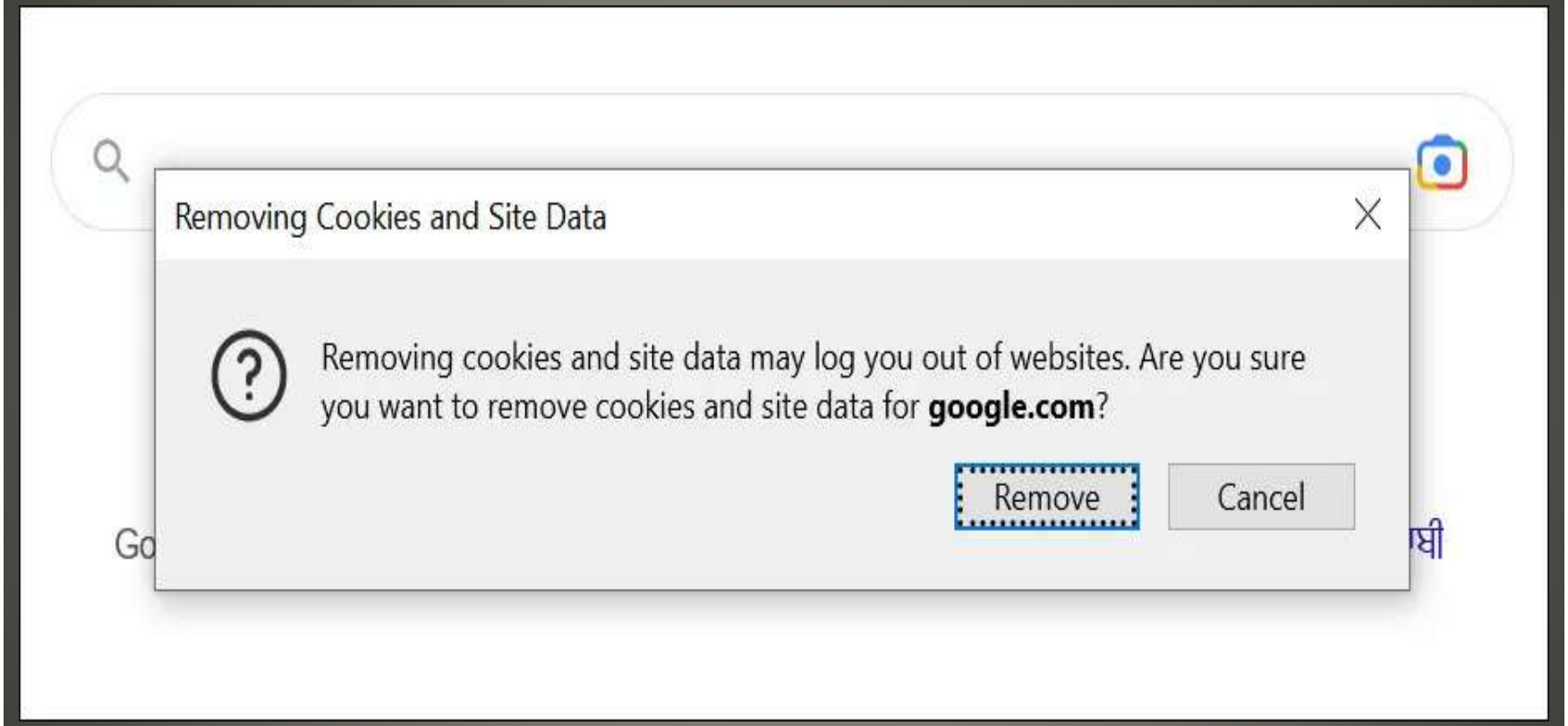

# Clear cookies per site

- Firefox




# Clear cookies per site

- Firefox



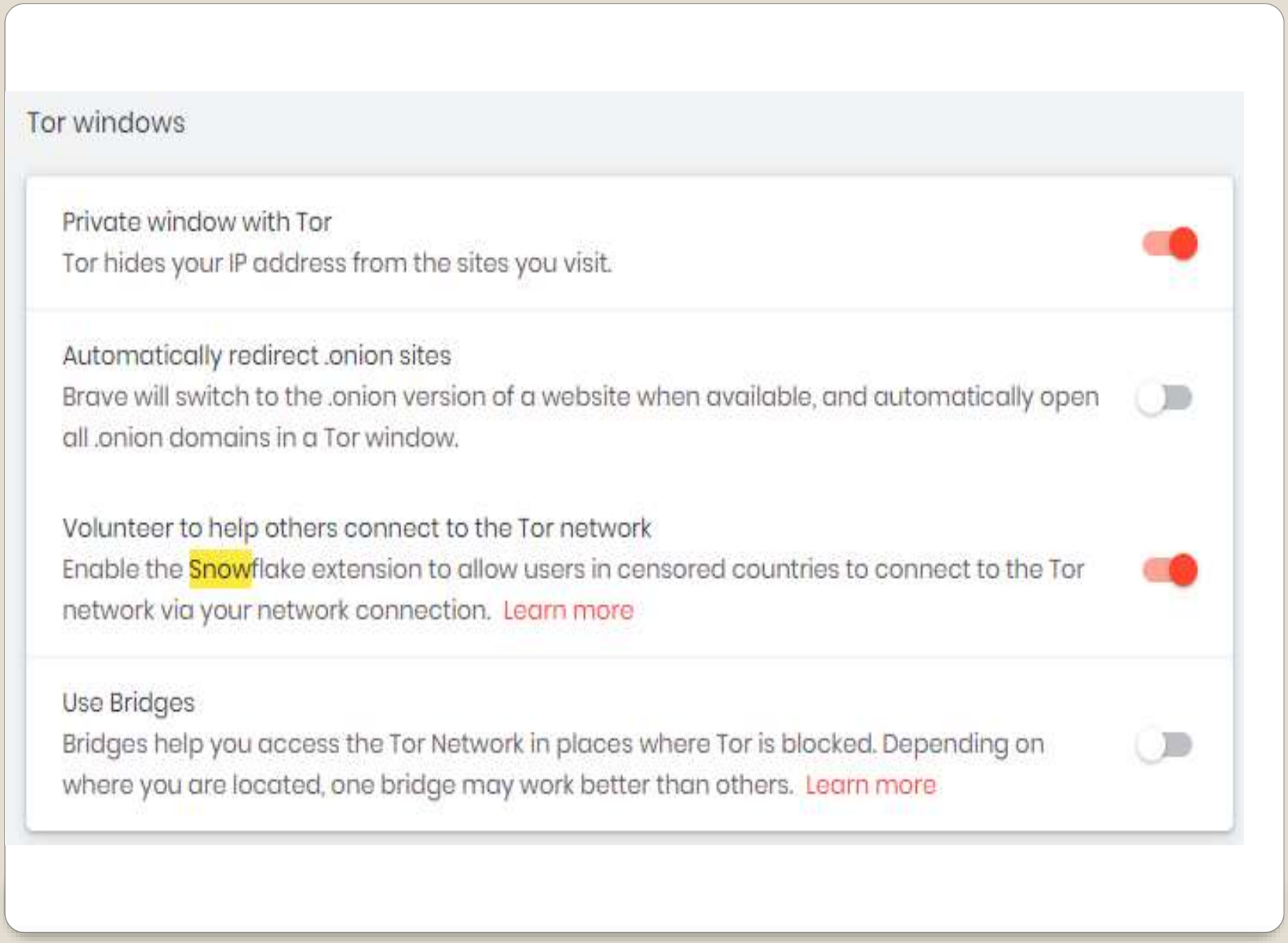

# Clear cookies per site

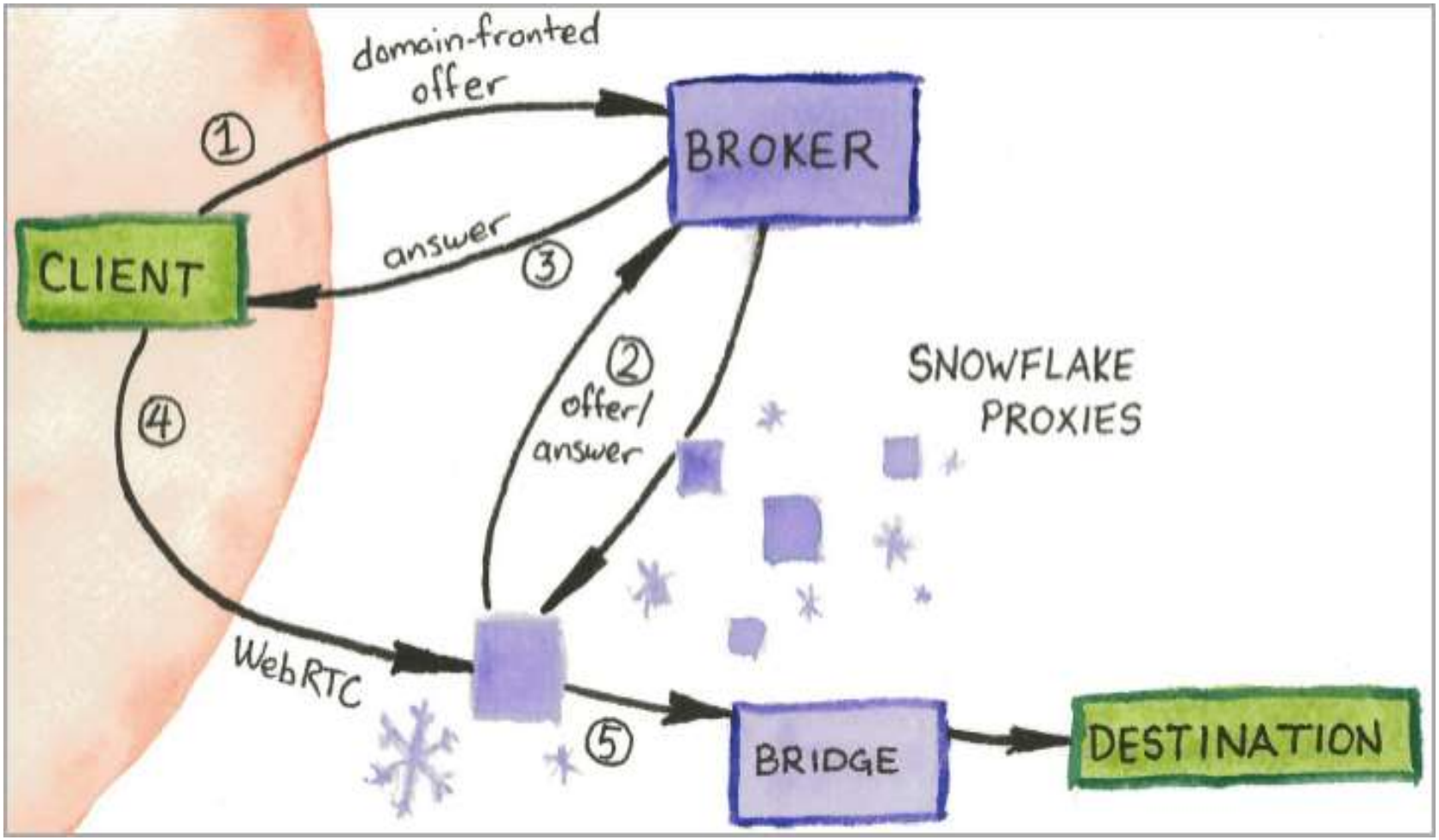
- Helpful <-> Harmful

# Clearing cookies per site

- Snowflake extension
- Tor Bridges
  - Built-in
  - torproject.org
  - trusted source

# Brave Browser 1.47


Tor windows
Private window with Tor
Tor hides your IP address from the sites you visit.
Automatically redirect .onion sites
Brave will switch to the .onion version of a website when available, and automatically open all .onion domains in a Tor window.
Volunteer to help others connect to the Tor network
Enable the Snowflake extension to allow users in censored countries to connect to the Tor network via your network connection. Learn more
Use Bridges
Bridges help you access the Tor Network in places where Tor is blocked. Depending on where you are located, one bridge may work better than others. Learn more

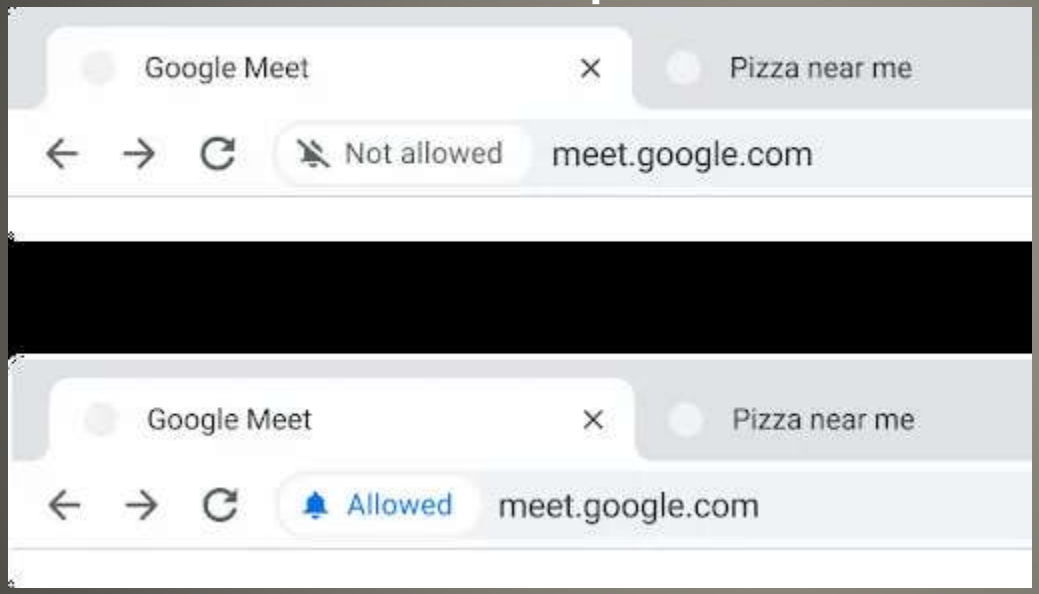

domain-fronted
offer
1
BROKER
CLIENT
answer
3
2
offer/
answer
SNOWFLAKE
PROXIES
4
WebRTC
5
BRIDGE
DESTINATION

- Peer-to-Peer network
- WebRTC protocol
- Automatically add ephemeral Tor Bridges
- Your leanings may vary

# Brave Snowflake extension

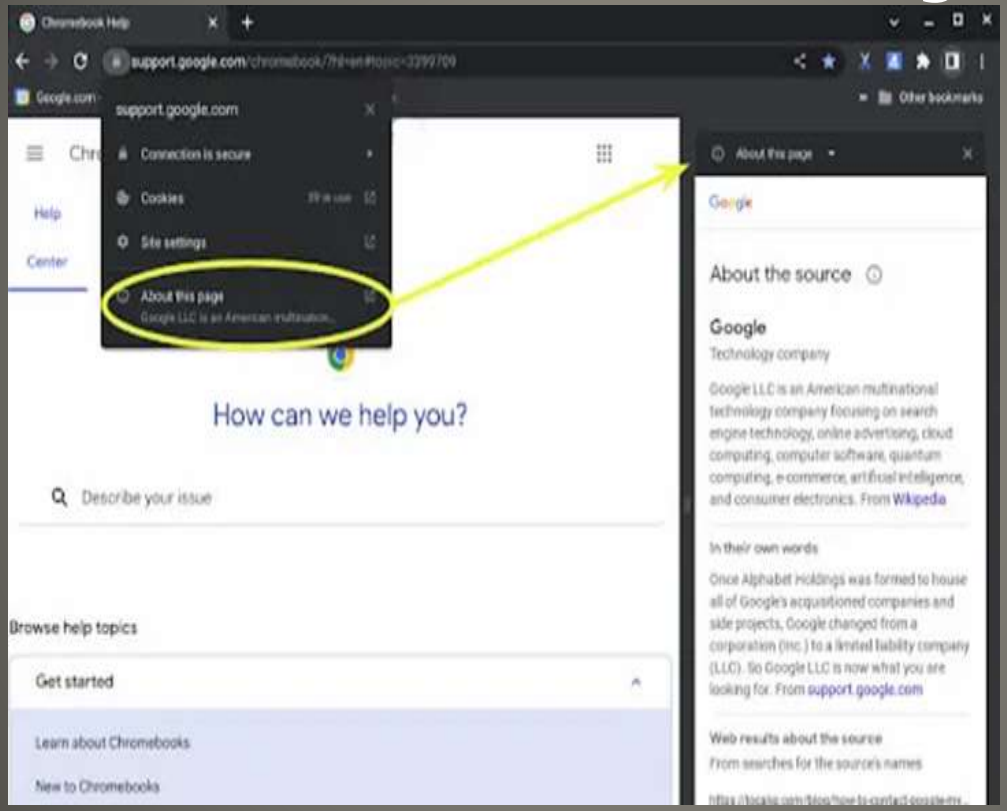
# Chrome 109

- Tuesday January 10, 2023
- 17 security fixes
- Permission “chips” to address bar

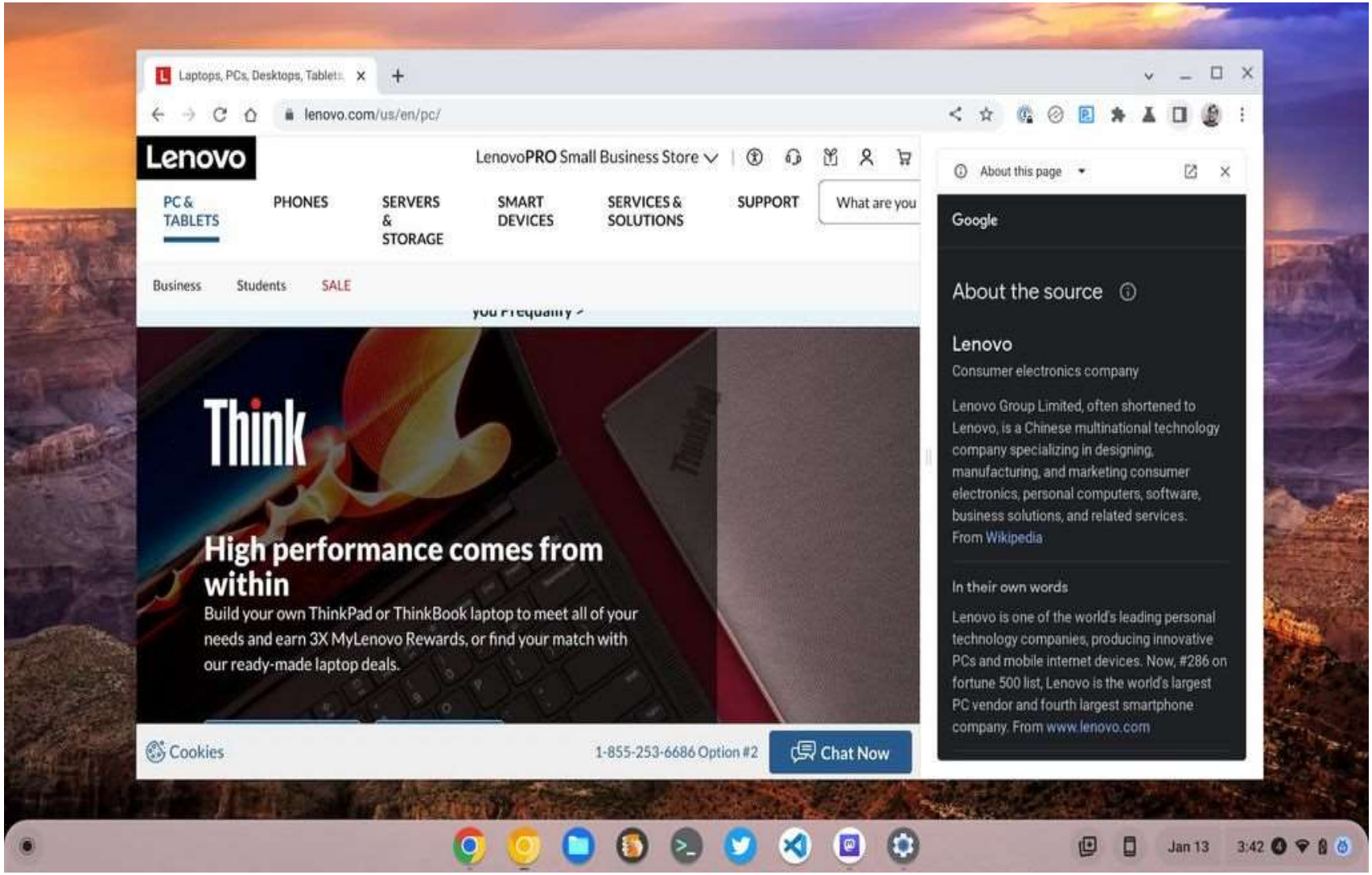



- Be quick

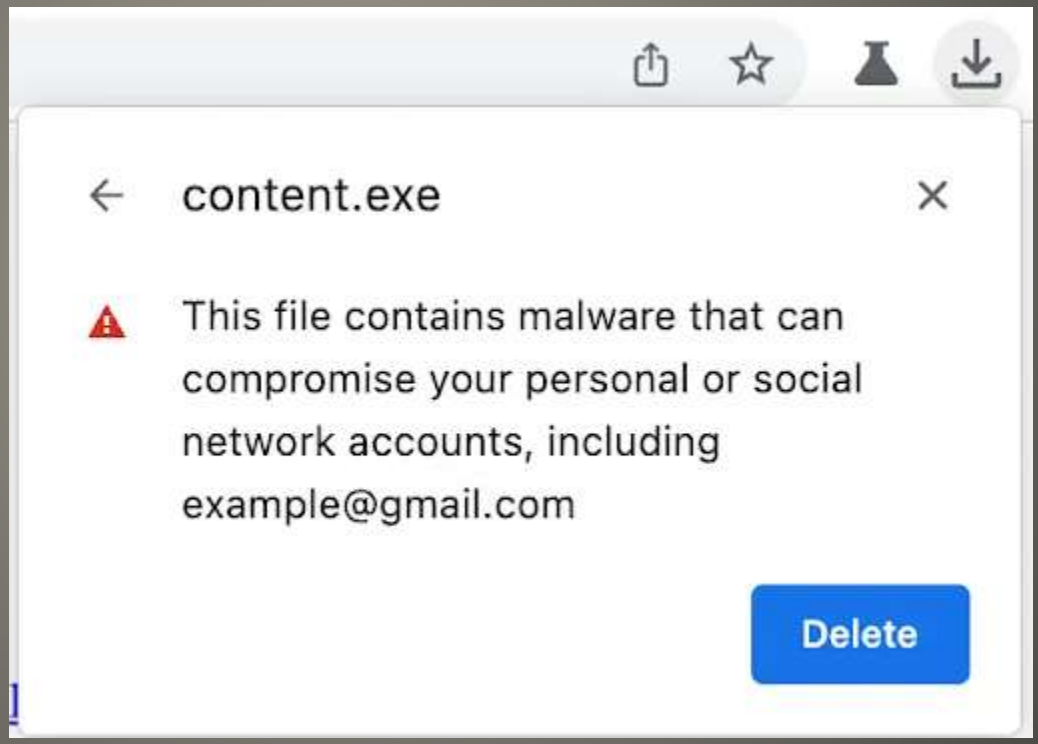
- More information about web sites
- *Make searches and browsing better*




# Chrome 109

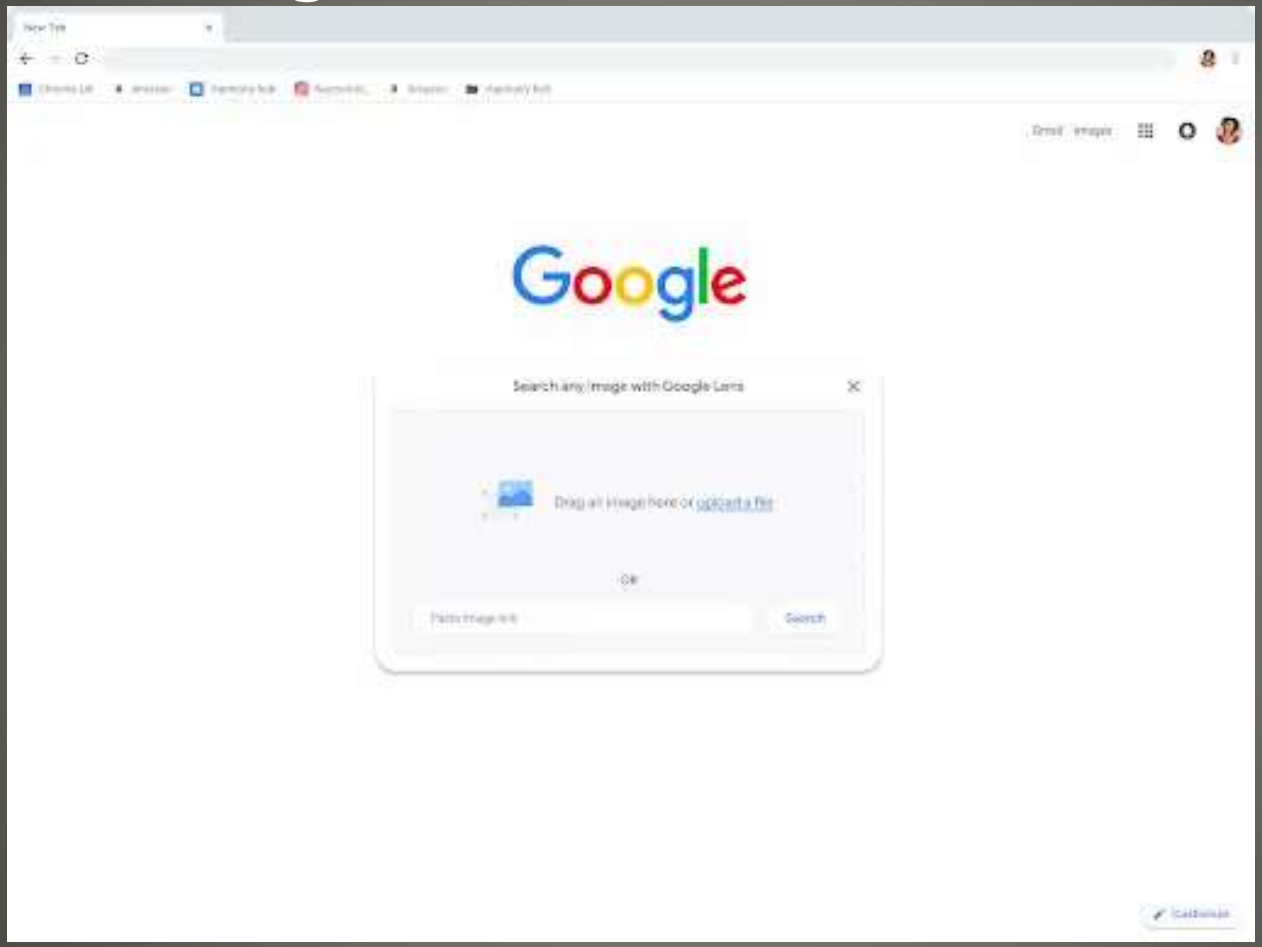

Laptops, PCs, Desktops, Tablets
lenovo.com/us/en/pc/
Lenovo
LenovoPRO Small Business Store
PC & TABLETS
PHONES
SERVERS & STORAGE
SMART DEVICES
SERVICES & SOLUTIONS
SUPPORT
What are you
Business
Students
SALE
Think
High performance comes from within
Build your own ThinkPad or ThinkBook laptop to meet all of your needs and earn 3X MyLenovo Rewards, or find your match with our ready-made laptop deals.
Cookies
1-855-253-6686 Option #2
Chat Now
About this page
Google
About the source
Lenovo
Consumer electronics company
Lenovo Group Limited, often shortened to Lenovo, is a Chinese multinational technology company specializing in designing, manufacturing, and marketing consumer electronics, personal computers, software, business solutions, and related services. From Wikipedia
In their own words
Lenovo is one of the world's leading personal technology companies, producing innovative PCs and mobile internet devices. Now, #286 on fortune 500 list, Lenovo is the world's largest PC vendor and fourth largest smartphone company. From www.lenovo.com
Jan 13
3:42

- Warning: Possible malware
- With Safe Browsing feature unpack 7z archives locally

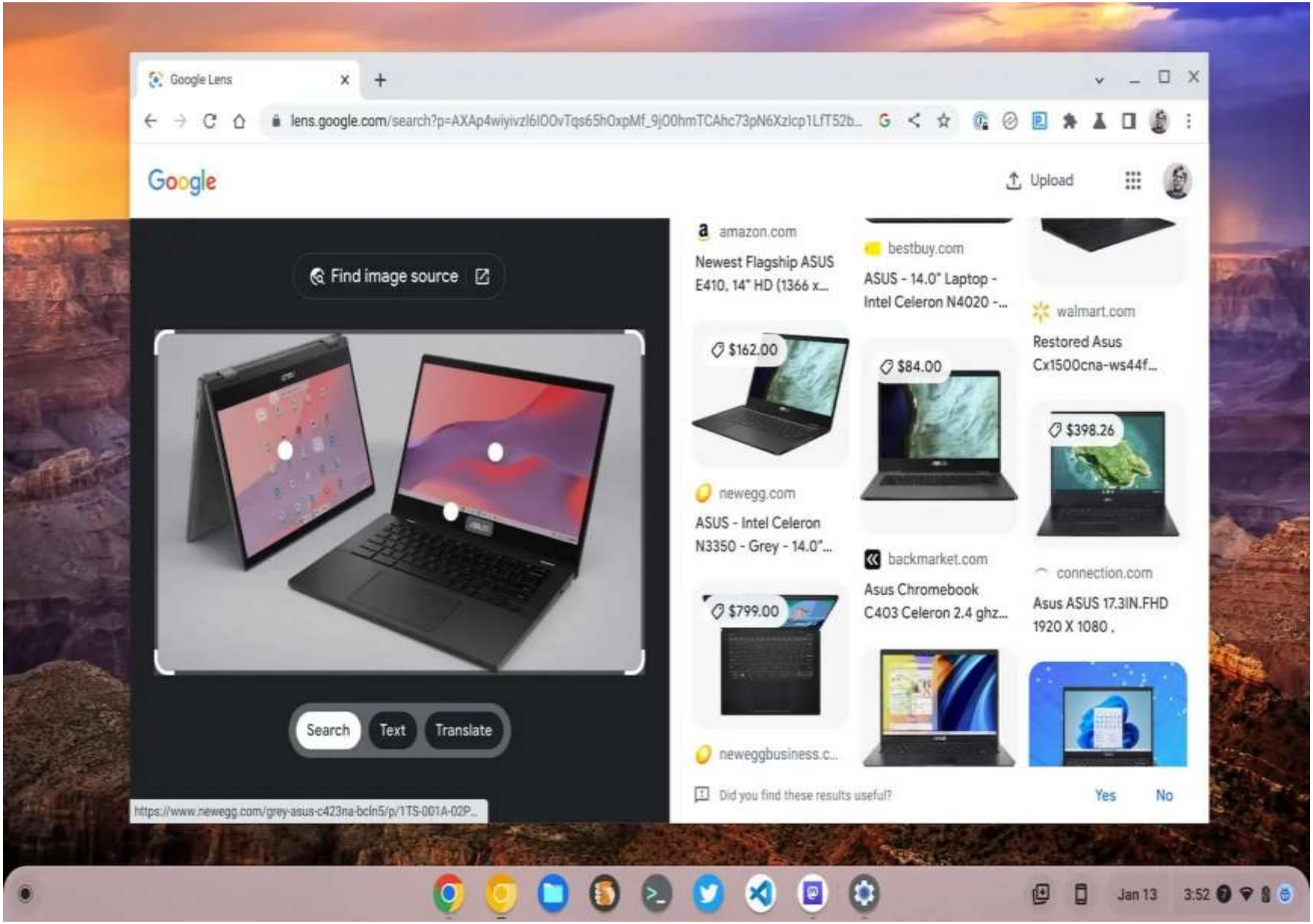



# Chrome 109

- Lens image search




# Chrome 109

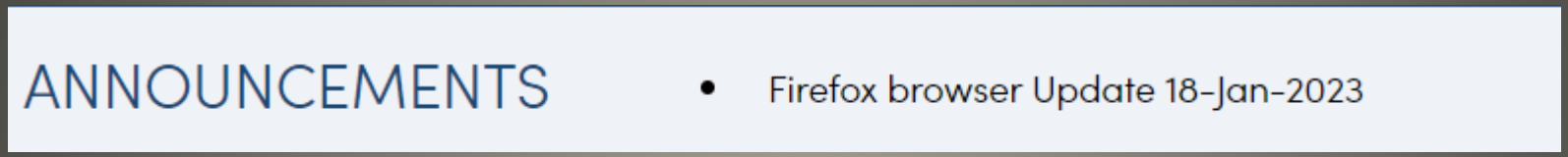

Google Lens
lens.google.com/search?p=AXAp4wiyivzl6lOOvTqs65hOxpMf_9jO0hmTCAhc73pN6XzIcp1LfT52b...
Google
Upload
Find image source
Search
Text
Translate
https://www.newegg.com/grey-asus-c423na-bcln5/p/1TS-001A-02P...
amazon.com
Newest Flagship ASUS E410, 14" HD (1366 x...
bestbuy.com
ASUS - 14.0" Laptop - Intel Celeron N4020 -...
walmart.com
Restored Asus Cx1500cna-ws44f...
$162.00
newegg.com
ASUS - Intel Celeron N3350 - Grey - 14.0"...
$84.00
backmarket.com
Asus Chromebook C403 Celeron 2.4 ghz...
$398.26
connection.com
Asus ASUS 17.3IN.FHD 1920 X 1080 ,
$799.00
neweggbusiness.c...
Did you find these results useful?
Yes
No
Jan 13
3:52

# Chrome 109

- 17 Security fixes
- SymStealer  symbolic links
  Digital wallet, keys , credentials
- ChromeOS 109

# Browser and Extensions update

- Expect chromium browsers to update soon



- Extensions button
- Unified extensions via Manifest Version 3
- Continued support for WebRequest function
  Ad blocker

# Firefox 109 Update

- YouTube channel
  channel SpaceXMission
  Elon Musk offering crypto coins
  iff you send him crypto coins
  Yup, they are doing it again
  During video QR code displayed


# Flipper Zero

# Flipper Zero

- SCAMS
- $170
- Criminal Activity is Criminal Activity!

- Read/Copy/Emulate NFC/RFID/IR
- Learning tool

- Wi-Fi development board

# Flipper Zero

- Wi-Fi dev board
- Flash firmware on Wi-Fi dev board
- New firmware on Flipper Zero
- Wi-Fi marauder on Flipper Zero


Select
Clear List
Attack
Targeted Deauth station
rickroll
FLIPPER
RESET
X3

# Flipper Zero

- Ooops

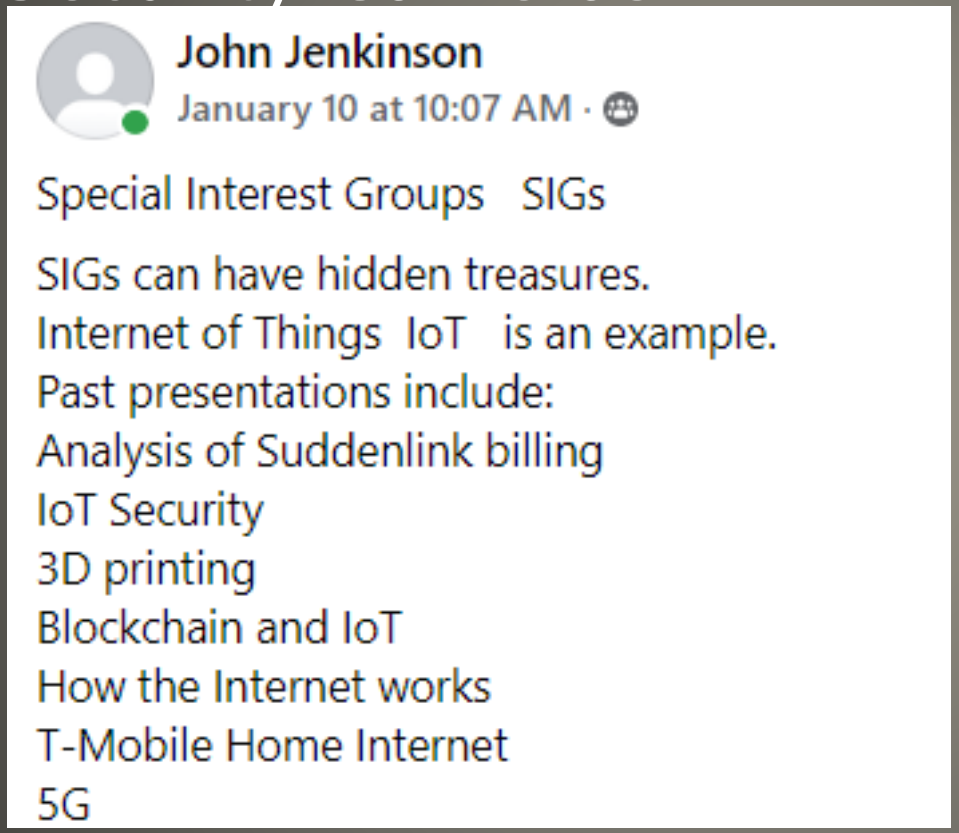
  crash wi-Fi, disable car key fob, …
- Alternative

  Kali Linux

  ALPHA AWUS036ACH dual-band USB Wi-Fi card


enter
return
Remove Ads
Do This To Remove Annoying Ads
Ad
Total Adblock

- IoT SIG
  Security Cameras




# SIGs

- Special Interest Groups
- Past Presentations

# SIGs

# iDevices

- Needs leader(s)
- Some content in MUG Mac Users Group
- News
- Beta Tests for iPhone, iPad, watch, mac
- Products starting to blend
- Contribute  Hints & Kinks

- Interim attempt at iDevice news
  Beta tests iPhone, iPad, watch, macOS
  iDevice user input requested
  Keep the group going until SIG revival

iOS 16.3 iPad16.3 watch 9.3 macOS 13.2
Bug fixes
Security keys for Apple IDs
New HomePod support

Monterey 12.6.3

# MUG Mac Users Group


A collision has been detected
Your vehicle has detected a collision on
17.01 at 07:15.
Please check this area for damage.
OK

- Helpful < - > Harmful
- Awareness, Preparedness, Understanding

Computer Club, Help Center, SIGs, Presentations, FirstTime, classes
Cyber Security SIG meetings, NEWSBLOG
Internet

- Questions, suggestions, comments?

**SCCCCyber@gmail.com**