

SKIOVOX exploit for ChromeOS

Exploit originally found by @AkaButNice

Exploit expanded by @Bypassi

Guide written by @Bypassi

What is it?

An exploit that allows for browsing within a completely unblocked Chrome browser. It works on ChromeOS 118 and a wide range of previous versions.

- Skiovox utilizes a bug in kiosk apps
- Very similar to a bug from 3 years ago

Within the unblocked browser, you can

- Install extensions
- Bypass pretty much all blocks



Kiosk apps

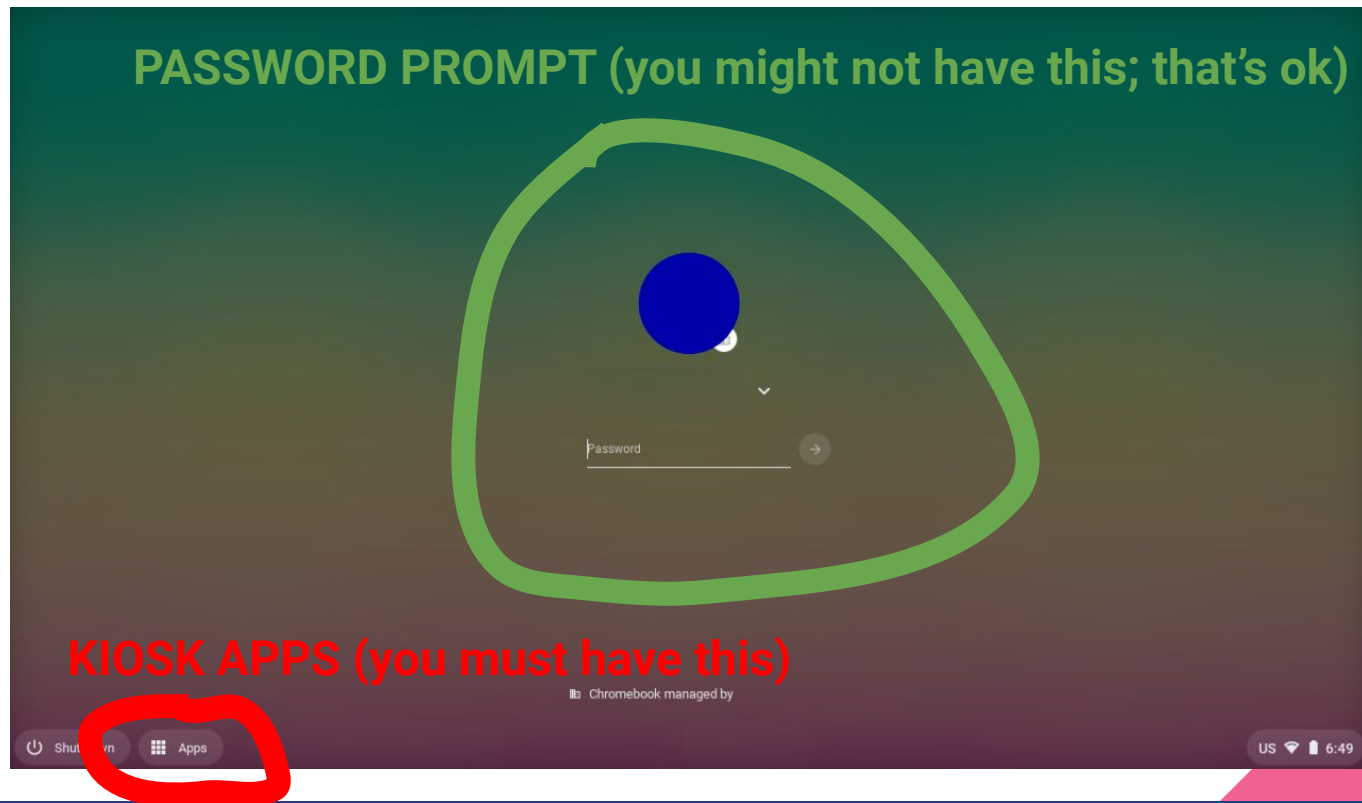
- A district-controlled app available from the login screen
- Most districts use them for standardized tests

These are required for this exploit. You cannot install these; only your school can!

See the following slide for a picture of what your Chromebook should look like when you shut it down and turn it back on.



The login screen anatomy



Disclaimer

This exploit may not work for you! **I do not care**, so please don't bother me.

It's also possible that it may be patched by the time you try it. I do not plan on updating these instructions.

Also, it's recommended to **open these instructions on another device**, as you won't be able to see them on your Chromebook while doing the exploit.



Stage 1

Starting the exploit

Note

Before you start, you must be properly connected to a WiFi network.



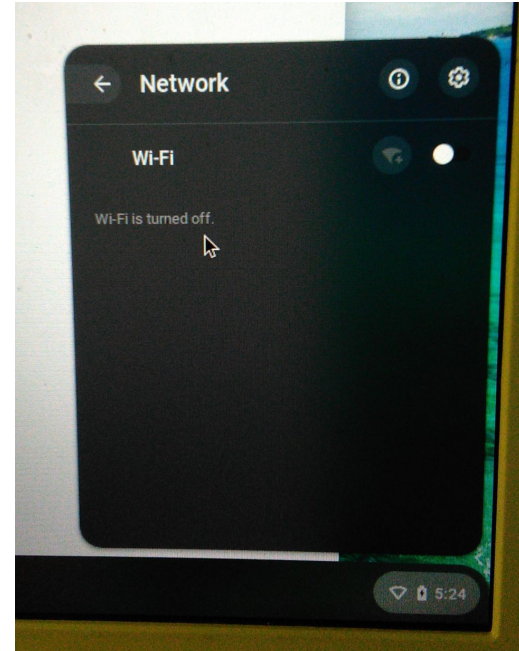
Step 1.1

First, sign out or restart your Chromebook to get to the login screen.

Then, turn **off** your Wi-Fi using the control panel in the bottom right.

Don't forget or disconnect from any networks, just turn it off completely.

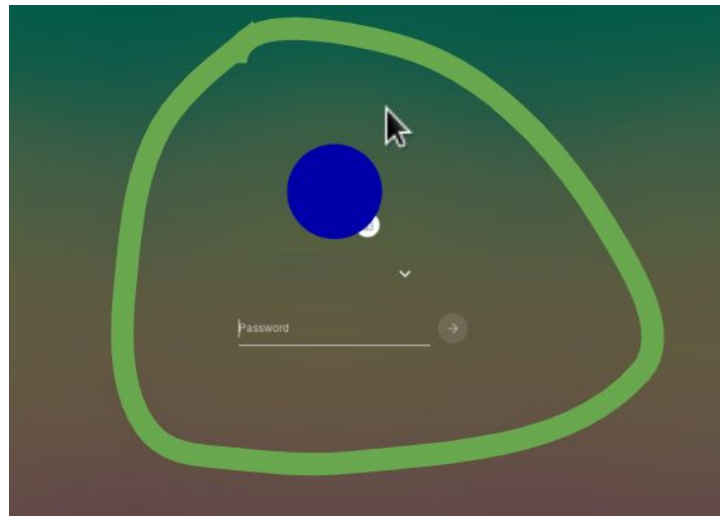
This may not work while at school.



Step 1.2

If you have a password input like the one in the image, type in your password but **do not** press enter.

If you don't have one, you can skip this step.



Step 1.3

Click on one of the apps in the “apps” section.

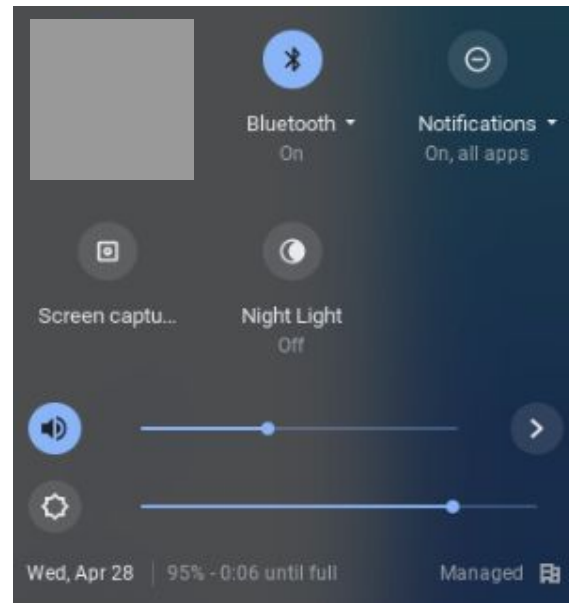
- Most of them work with this exploit
- Use the same app every time to save data

Instantly after you click on the app, **run [alt+shift+s]**.
(NOT ctrl+alt+s)

If you did it fast enough,
a toolbar should appear.



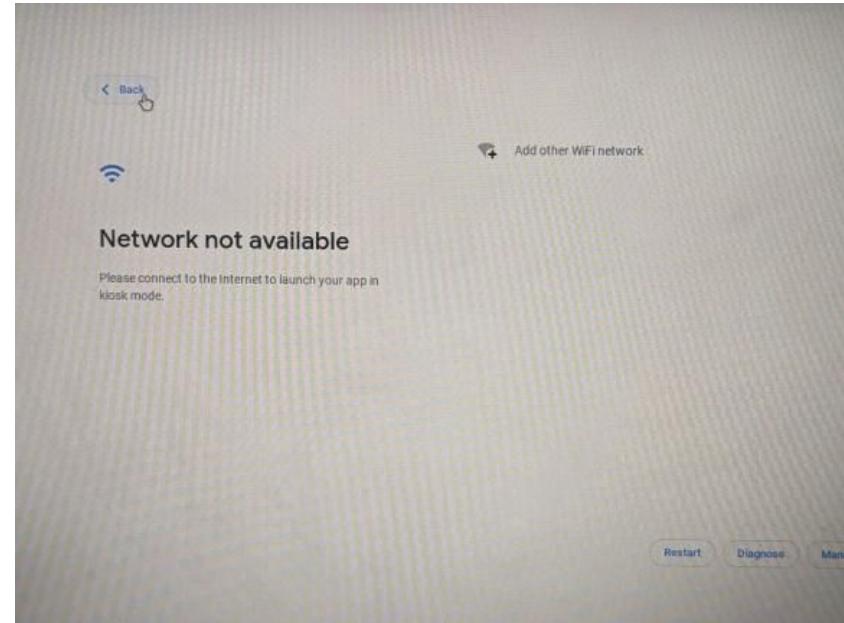
If it didn't, restart the steps.



This should show up

Step 1.4

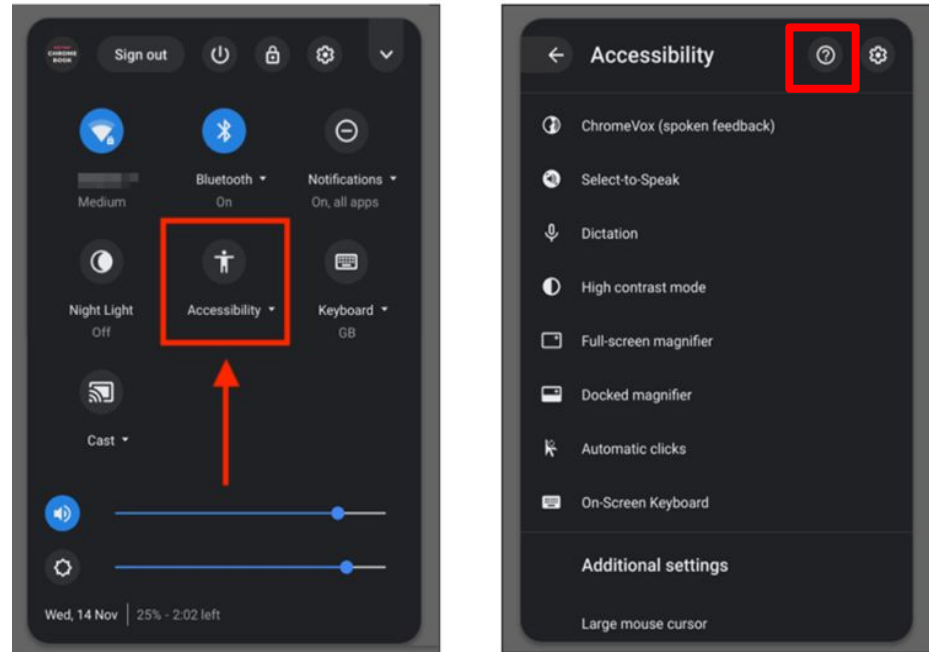
Wait until you get a “network unavailable” screen.



Step 1.5

The toolbar should still be open. Click accessibility, then click the question mark. The toolbar will now close.

If you couldn't do this step, try again with another app.



Next...

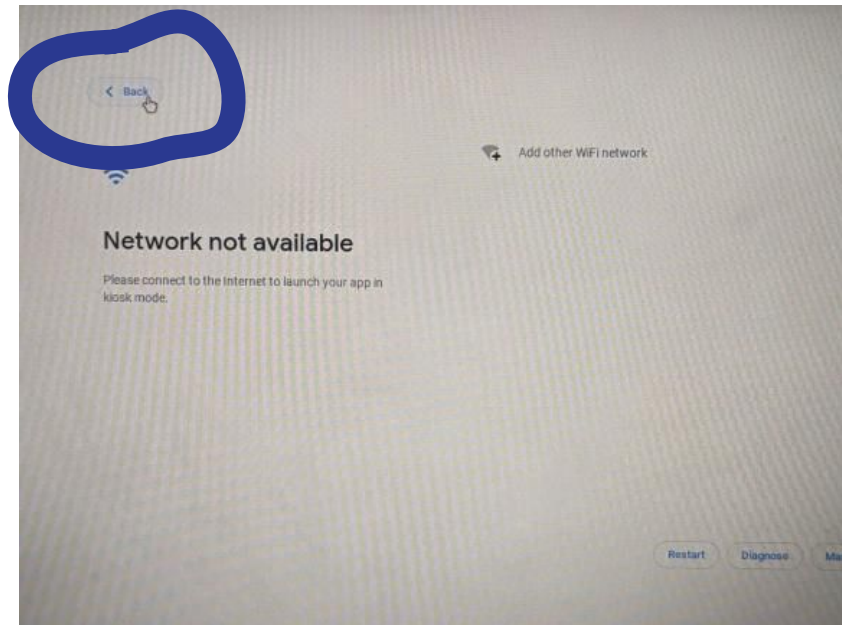
If you see a “back” button on the network error page:

- **Go to stage 2A**

Otherwise:

- **Go to stage 2B or 2C**

They have different steps!



Stage 2A

For users with a back button

Note

You should have already typed in your password (step 1.2) by the time you're here.

Remember that the steps in stage 2A are only for users who see a back button on the network error page.

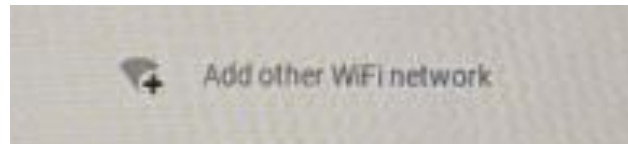


Step 2A.1

Click “add other WiFi network”.

Don’t type anything in.

Instead, immediately:



- **Press the escape key twice**, which should bring you to the login screen with your password still typed in
- **Press enter** to log in

These steps must be done within ~4 seconds after pressing the “add network” button.

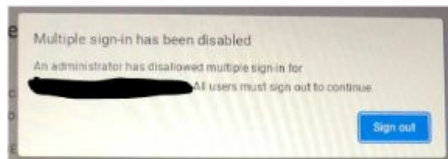


Step 2A.2

You may see a screen saying “multiple sign-in is disabled.” If you get this, simply press the escape key on your keyboard to bypass it.

WHO WOULD WIN?

Google's well-programmed
feature to enforce a policy



Step 2A.3

There may be an open window belonging to your school profile. This window will have your filter extensions installed.

Close this window if you like. There should be another one behind it.

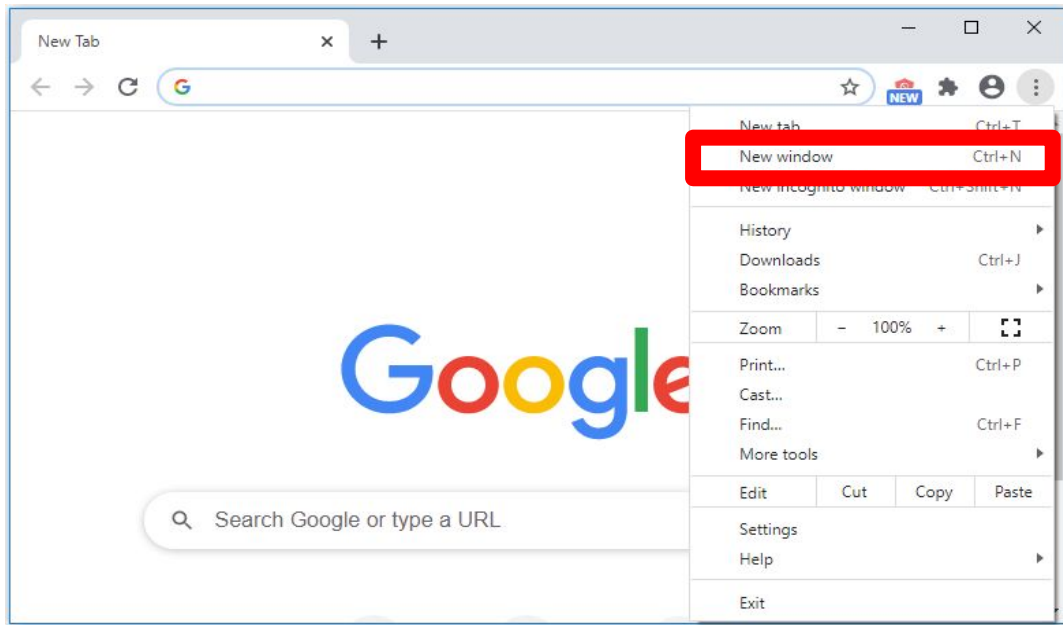


Step 2A.4

You should be able to see a window with no managed extensions installed.

This window is slightly bugged. To fix this, click the three dots in the upper right corner of Chrome and select “new window”.

Use this window instead.



Next...

If this is your first time setting up the exploit, do Stage 3. Otherwise, you're done.



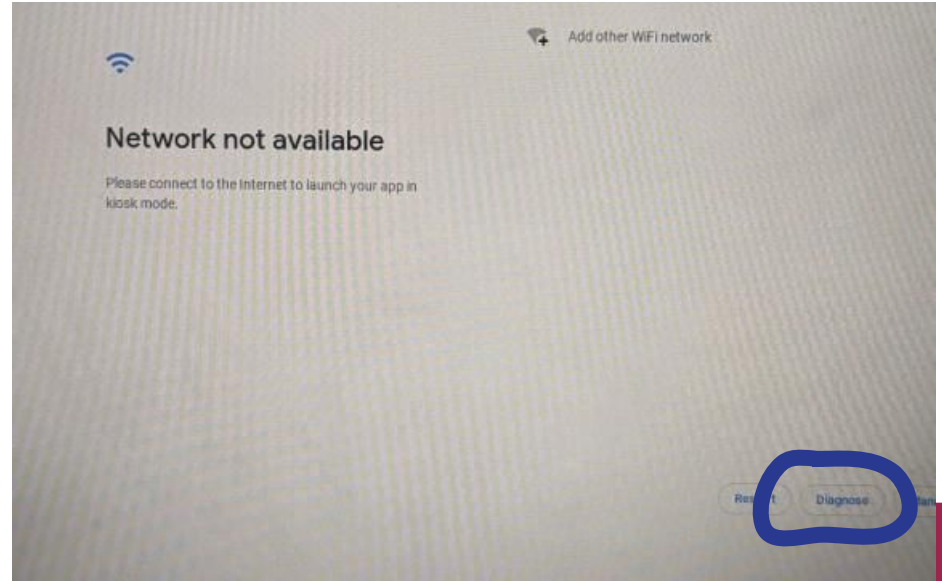
Stage 2B

For users without a back button

Step 2B.1

Press the “diagnose” button.

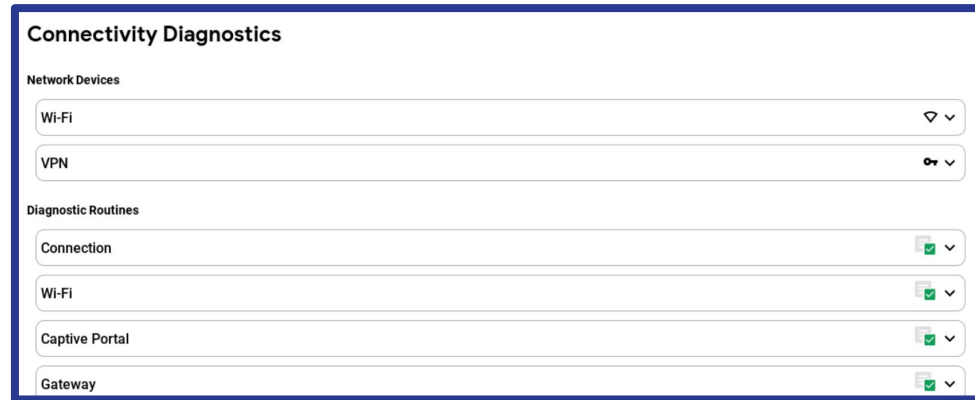
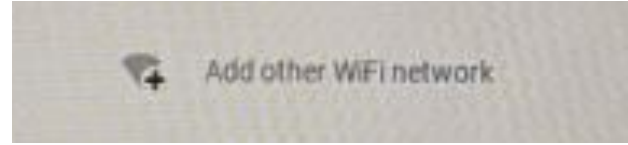
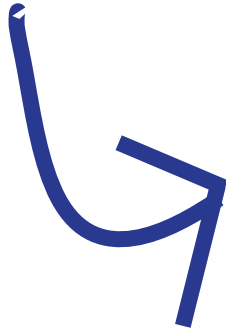
The diagnostics window will now open, although you shouldn't be able to see it.



Step 2B.2

Click “add other WiFi network” to turn your WiFi back on. Don’t type anything in, just **wait until the diagnostics page shows up.**

This is known to be inconsistent; try a few times with a few apps or try 2C.



Step 2B.3

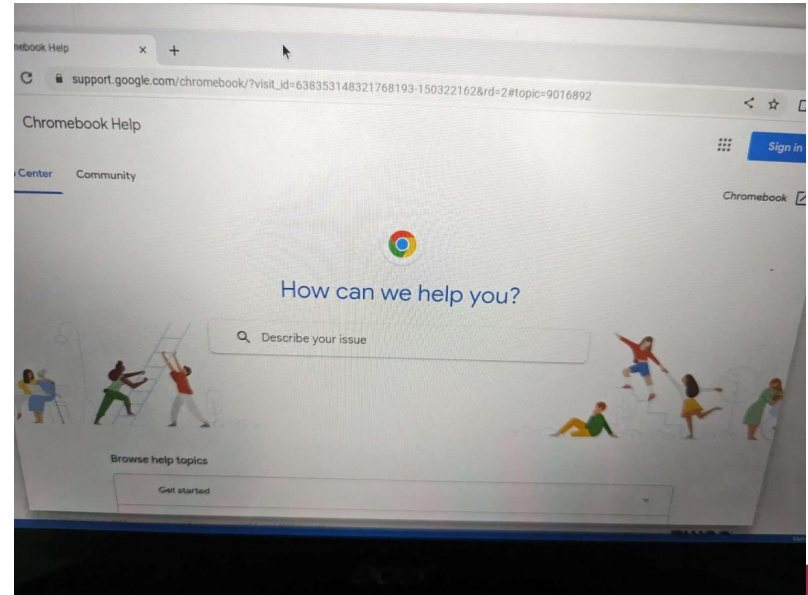
Click WiFi, then click the settings link. Settings should now open.



Step 2B.4

Close the settings window. There's nothing useful that you can do from device settings, as device policies still apply.

Once you've closed it, you should be focused on a Chrome window. This window shouldn't have any of your district's extensions installed.



Next...

If this is your first time setting up the exploit, do Stage 3. Otherwise, you're done.

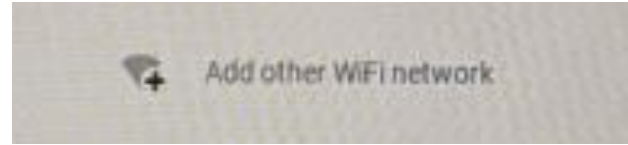


Stage 2C

Also for users without a back button

Step 2C.1

Click “add other WiFi network” to turn your WiFi back on. Don’t type anything in, just **wait until the kiosk app loads**.



Step 2C.2

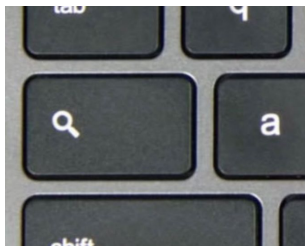
Press [ctrl+alt+z] to open text-to-speech. This may be blocked for you.

Note that a noise will likely be made when you run this shortcut.

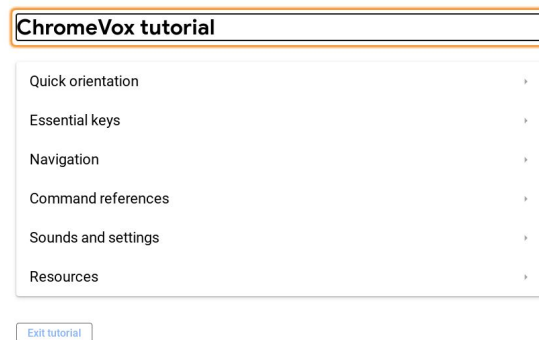


Step 2C.3

Hold the search key. Press the O key, then the T key.



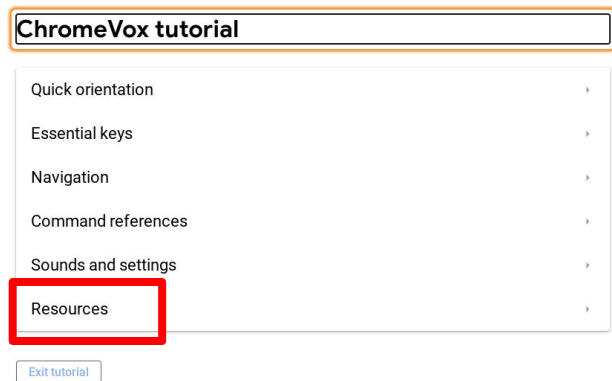
A tutorial window should appear:



Step 2C.3

Click “resources”. **Three links will show up**; you can click any of them.

Your browser should now open.



Next...

Once your browser is open, you can turn off TTS by running [ctrl+alt+z] again.

If this is your first time setting up the exploit, do Stage 3. Otherwise, you're done.



Stage 3

Making the experience smoother

Issues with this exploit

- It's unclear how to add a Google account and install extensions
- Most keyboard shortcuts don't work
- It's hard to move or resize the window(s)

-



The solution

The **Skiovox Helper** extension restores all of this functionality:

Find it on the skiovox page

In this section, I'll explain how to install it.

You only have to set this up once! (per app)




Step 3.1

A zip file of the extension is available On the skiovox page.

Find a way to **download this zip file** in your unblocked browser.

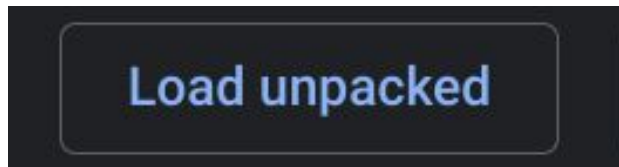
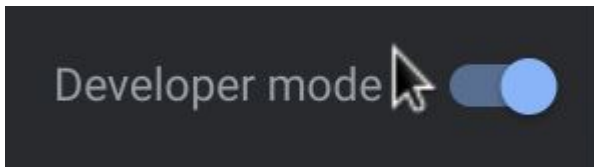
If you got here from stage 2A, make sure the following settings in `chrome://settings/downloads` is turned **off**:

Ask where to save each file before downloading



Step 3.2

- Go to `chrome://extensions`
- Ensure that the developer mode switch in the top right is turned on
- Click “load unpacked”
- A file prompt should now appear



If you don't get a file upload dialog, make sure you didn't skip step 2A.4.

Step 3.3

- Find the zip file from step 3.1 in your Downloads section
- Right-click it and press “extract all”
- Double-click the newly created folder
- Press “open”

The extension should now install.



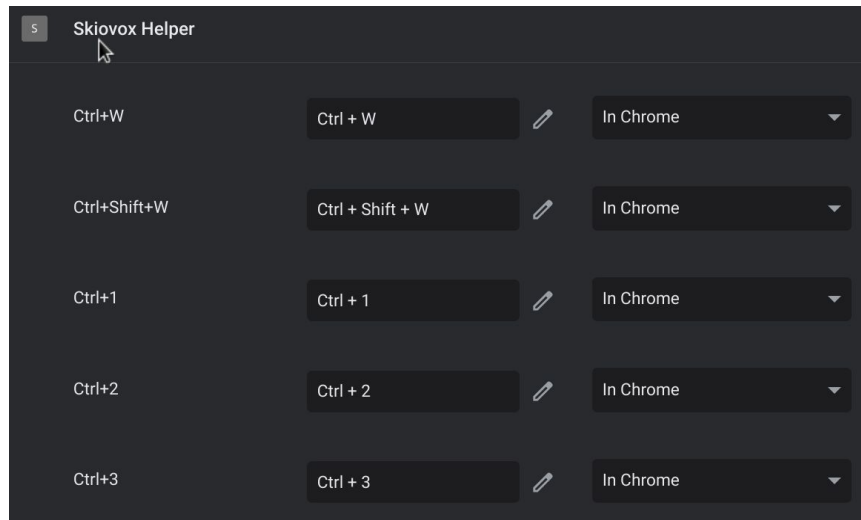
Step 3.4

Upon the first install, the extension will open a page where you can configure your browser shortcuts.

For each shortcut shown:

- Press the edit icon
- Type the command shown in the caption

You can now use most Chrome commands (ctrl+T, ctrl+W, etc)

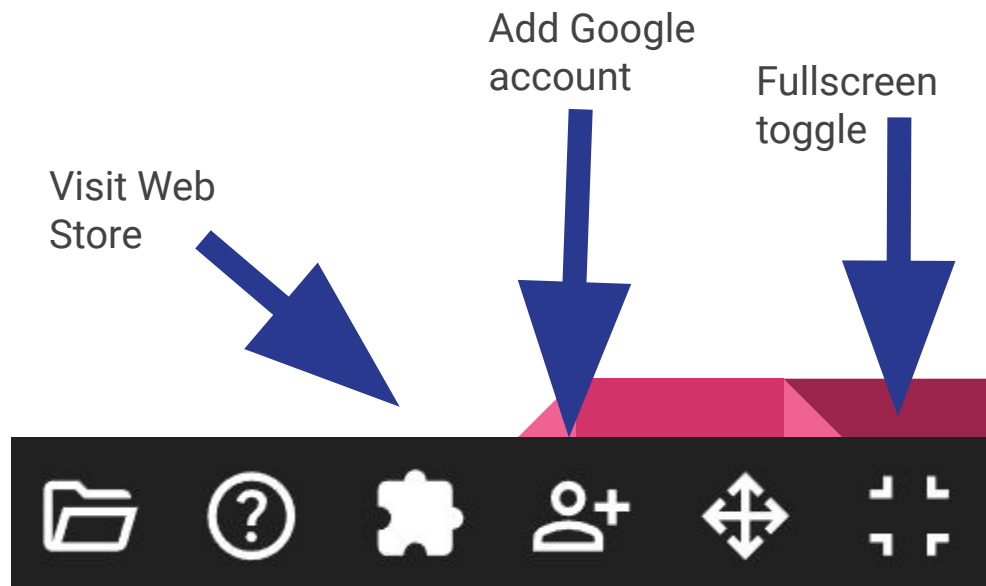


Step 3.5

The Skiovox Helper replaces the new tab page. **Open a new tab** to see its main menu. Try playing around with the buttons in the top right.

The web store only works on recent ChromeOS versions.

You can use it to install VPN extensions that bypass your school's internet filtering.



Other notes


The main difference between the stages is:

- 2A can open multiple windows
- 2B and 2C can not

If your screen keeps falling asleep after five seconds, try using another kiosk app.

Every app has its own extensions, history, settings, etc.

It's possible that google.com might be blocked for some users; we're looking into this.



Opening device settings

If you only want to edit network settings, try `chrome://network#select`.

Again, device settings are mostly useless because device policies still apply, but...

If using 2A:

- Click the settings icon instead of the help icon on step 1.5

If using 2B or 2C:

- Simply go to `chrome://os-settings`



Exiting the exploit

To exit the exploit, either:

- Hold down on your power button (and sign out)
- Type “chrome:quit” into a new tab





That's all!

Exploit originally found by @AkaButNice
Exploit expanded by @Bypassi