

Google Security Checkup

BACKGROUND

If you have a Gmail account and/or are a regular user of Chrome, then you'll be able to increase your security game by running the Google Security Checkup. Google makes it easy to make sure your passwords are safe, you know where you are logged in, and you know what apps have access to what information.

DESCRIPTION

This exercise will walk you through a routine security check offered by Google for your Google account.

REQUIREMENTS

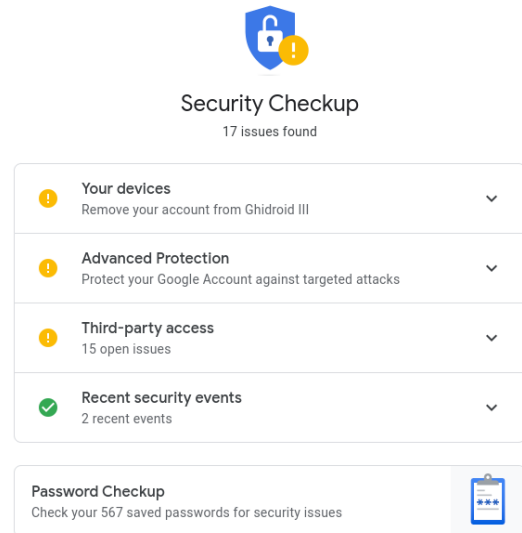
A web browser (preferably Chrome).

PART I: Initiate the Security Checkup

1. Make sure you are logged into Google.
2. Go to the Security Checkup website.
 - a. <https://myaccount.google.com/intro/security-checkup?hl=en-US>

PART II: Check devices you are currently logged into

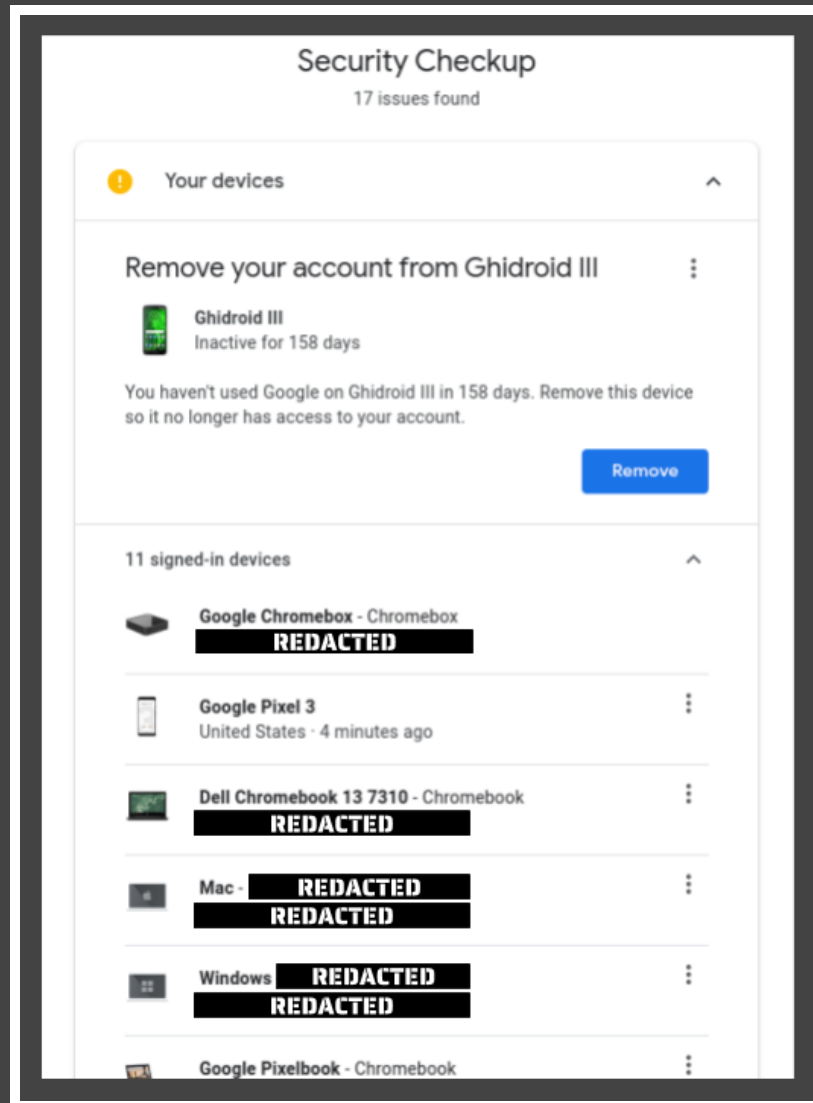
1. You might be logged into your Google account on different devices. For instance:
 - a. If you use the Gmail app on your phone (Android or iOS), you are logged in.
 - b. If you use Chrome on different devices, you are logged in.
 - c. If you use Google Docs on different devices, you are logged in.
2. To see what devices you are logged in on, you should click on the "Your Devices" section and review all the devices. You might be surprised at how many devices you are logged



in on (home computers, work computers, school computers, old phones, etc.).

3. Take a screenshot and include it below. Make sure to redact personal information (for instance, location). Note that in my example, I have an old phone that has been inactive for 158 days that I'm still logged in on! Don't worry - that's my backup phone and it's kept in a safe. You should remove any device that is a security concern.

EVIDENCE #1



PASTE THE IMAGE OF THE RESULTS OF "Your Devices"

PART III: Consider enrolling in Advanced Protection (if possible)

1. You may be offered the "Advanced Protection" option. If you use Google a lot and have a

big threat surface, Google may offer you this service:

The Advanced Protection Program is designed to safeguard the accounts of anyone at risk of targeted online attacks. It provides industry-leading protection against ever-changing threats like phishing and malware.

- *Google's strongest defense against phishing*
- *Safeguard your data by limiting access to it*
- *Block fraudulent account access with extra verification*

2. If you are curious about this service, check out the [explainer video](#).
3. Note that there is no requirement for this lab to enroll. But you should totally do it if you can. It's awesome (although it may require a physical key if you don't have compatible devices).

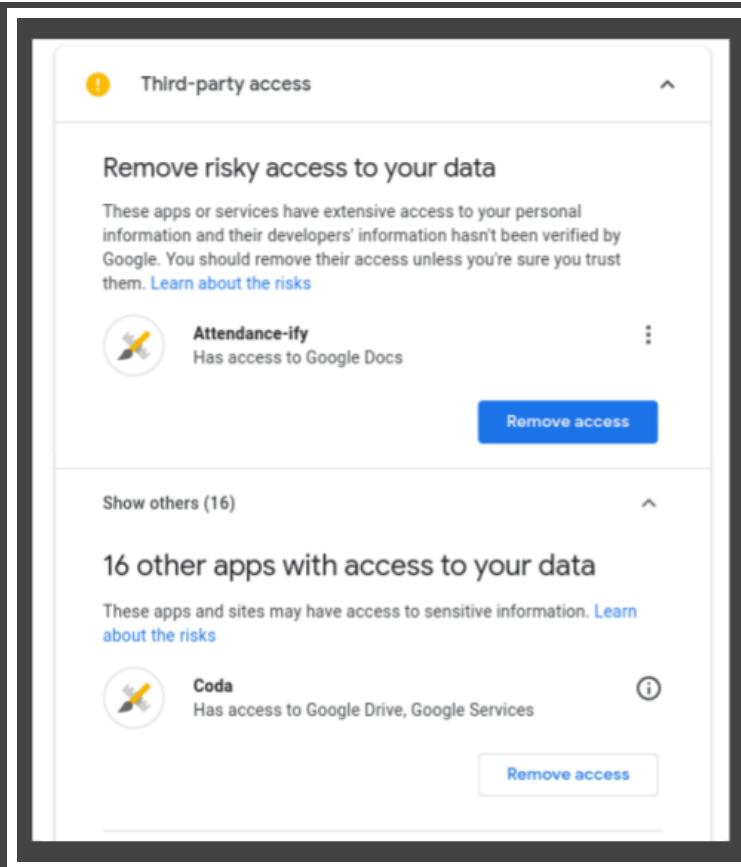
PART IV: Third-party access

1. Third-party access to your Google account can occur in a few different ways. If you have a script in any of your Google Sheets or Google Docs documents, you've granted some level of third-party access. This isn't something that happens on accident; you need to be pretty intentional about giving third-party access to Sheets or Docs. You can also grant access to your Google account through various apps and extensions.

You can see in my example below that I have a script ("Attendance-ify") that has access to Google Docs and an app, "Coda", that has access to Google Drive and services. I have vetted both these applications, so I know they are safe. But you could (and should!) revoke access to any app that you think is suspect.

2. Take a screenshot that captures some of these issues. Redact any information you wish to keep private.

EVIDENCE #2



PASTE THE IMAGE OF THE RESULTS OF "Third-party access"

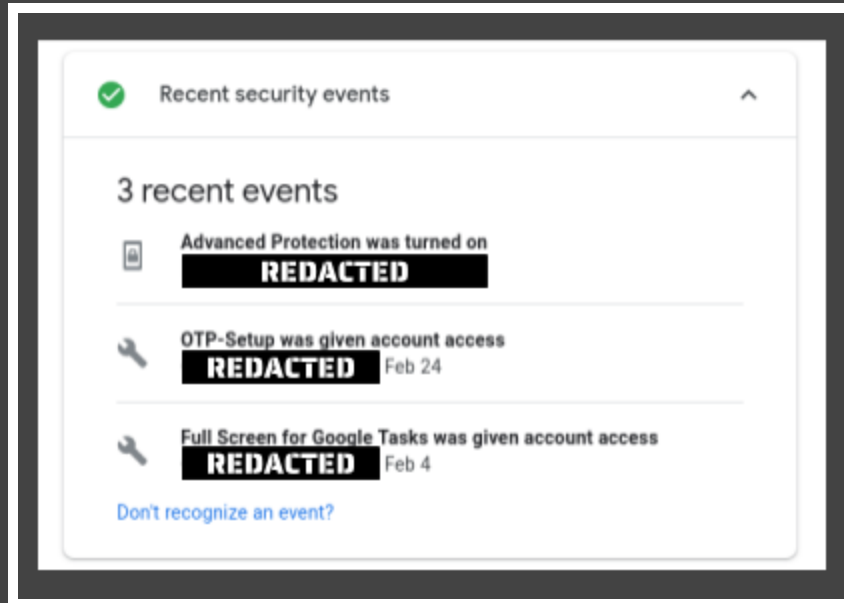
PART V: Recent Security Events

1. Google will help you understand recent events that may affect your account. For instance, if you have given an app or extension the ability to access your Google account or if you have logged in on another device.

Note that you can't dismiss these event notifications; that is for security. Let's say that a bad actor infiltrated your account and installed a malicious extension or logged on to their device with your account. Both those activities would trigger a Security Event notification. If they had access to your account, they could dismiss the notification and you wouldn't know. But since Google doesn't allow notification dismissals, you will know recent security events if you check this frequently.

2. Take a screenshot of your recent security events, redact any personal information (like location or security events you want to keep private).

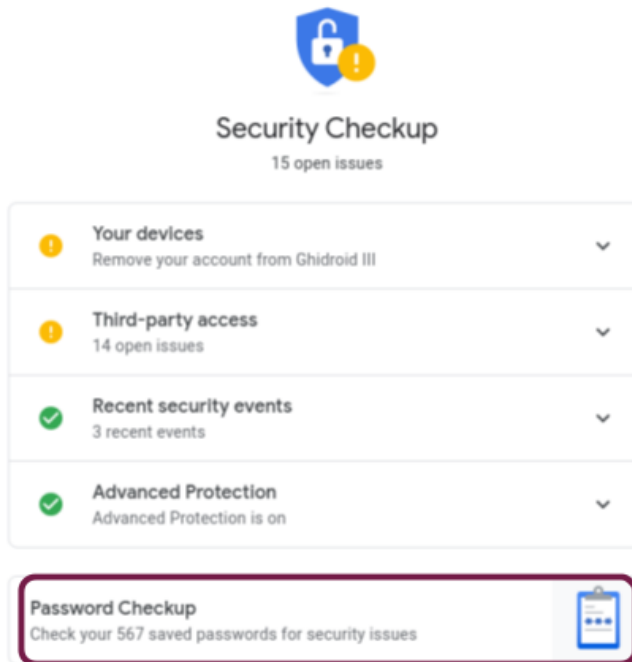
EVIDENCE #3



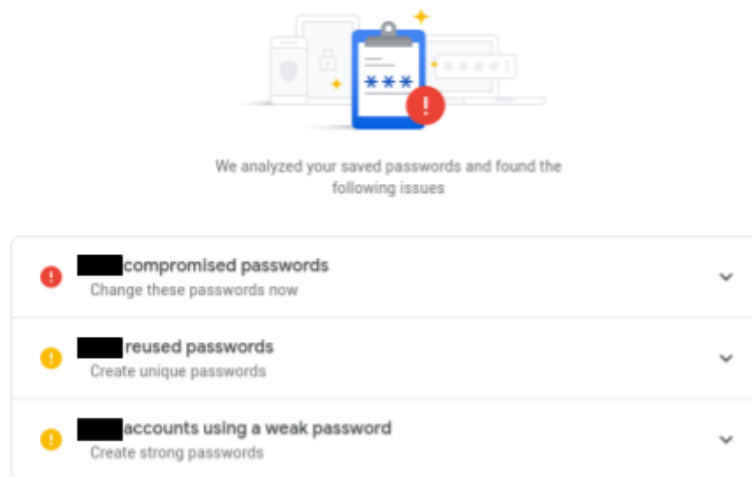
PASTE THE IMAGE OF THE RESULTS OF "Recent Security Events"

PART VI: Password Checkup

1. Google also has an onboard password manager. Some of the benefits of the password manager are that it will help you:
 - a. See accounts where you've used the same password
 - b. Alert you to breaches
 - c. Help you create secure passwords
2. From the Security Checkup main screen, click on the "Password Checkup" link:



- Note that this portion of the lab is not assessed, but you should spend some time understanding this tool and also ensuring that your passwords are safe. It would be a good idea to fix any issues (compromised passwords, duplicate passwords, and weak passwords).



See personalized security recommendations for your Google Account in the Security Checkup. [Get started](#)

