Tips for using Google Password Manager safely

If you're using Google Password Manager, use these tips to keep your passwords safe and away from the bad guys.

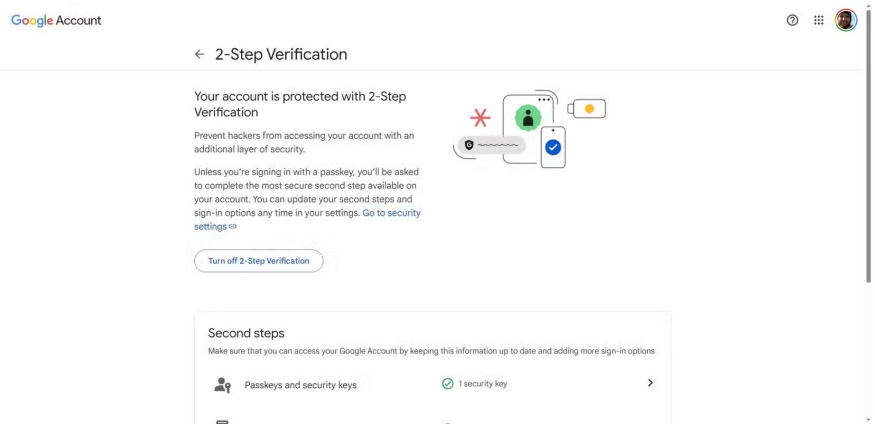
Many people have relied on Google Password Manager for years to keep their digital lives organized, but convenience can sometimes come at the expense of security. So if you're using Google Password Manager, use these tips to keep your passwords safe and out of reach of the bad guys.

7. Use a strong Google account password

If you sync Google Password Manager (GPM) with your Google account, your account password acts as the key to access your stored passwords. Therefore, GPM is only as secure as the password protecting your Google account. For this reason, it is important to use strong and unique passwords .

There are many ways to make your password more secure, but you can use a passphrase if you want it to be easier to remember.

6. Turn on two-factor authentication (2FA) for your Google account



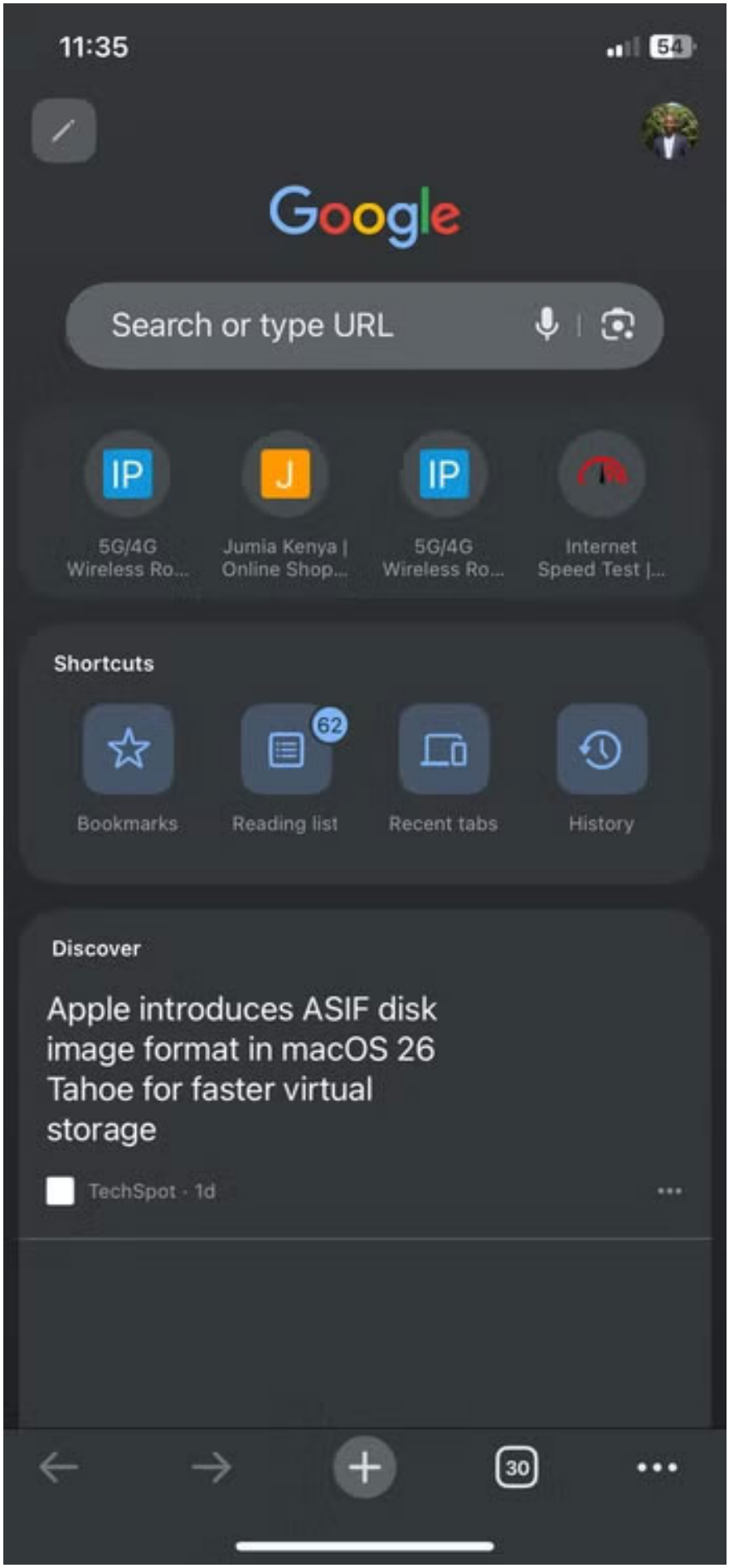
It's no secret that even the strongest passwords can be compromised. That's why enabling two-factor authentication (2FA) is a must for any online account, not just your Google account. 2FA adds an extra layer of protection, requiring you to provide both your password and a second verification step. The second verification step can be a code sent to your phone via SMS or generated by an authenticator app.

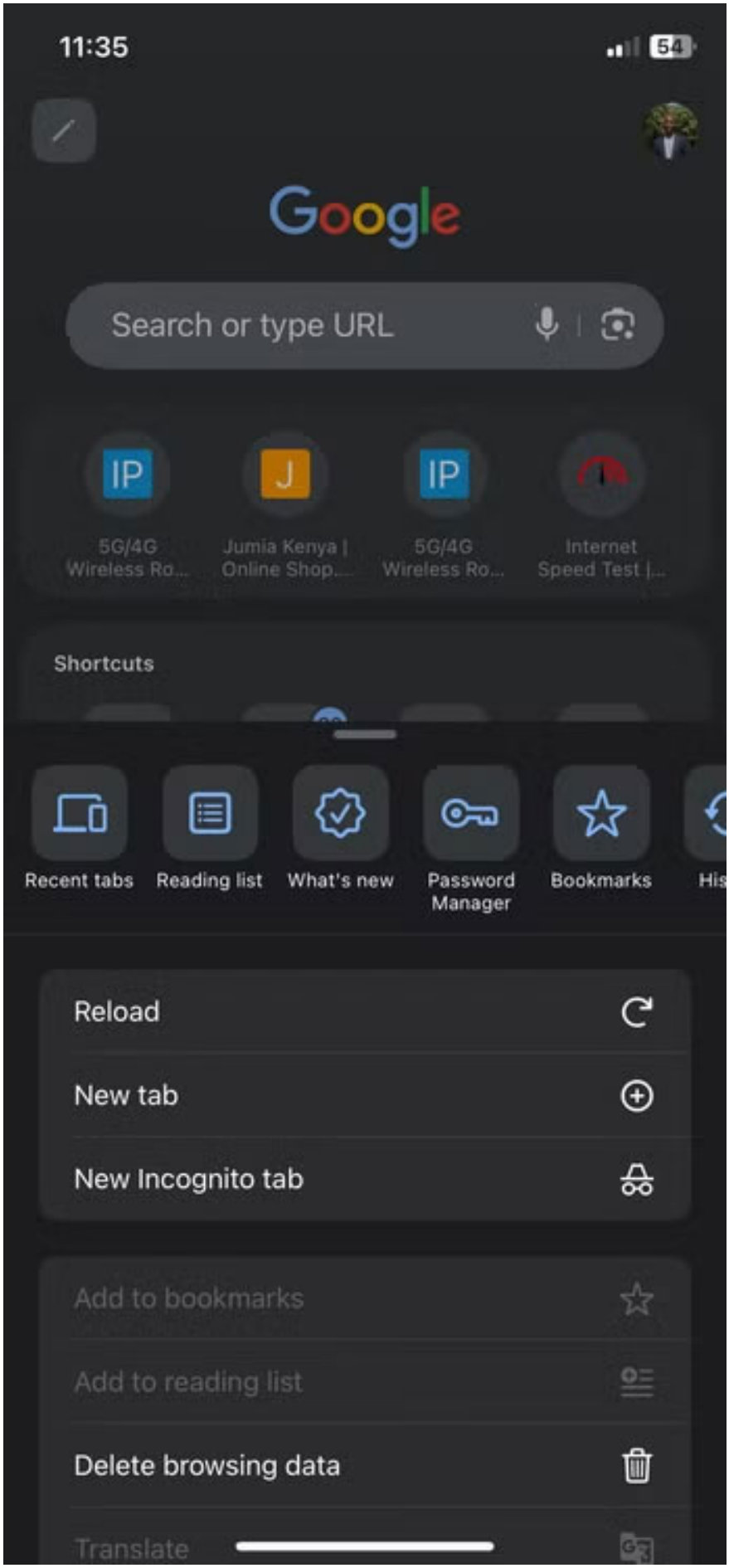
This extra layer ensures that even if your password falls into the wrong hands, your account won't be compromised without the second factor. Google offers three 2FA options, including text messages, authenticator apps, and even physical security keys. You can use any of these three options, but for optimal security, you should avoid SMS verification because it's vulnerable to SIM swapping and other attacks.

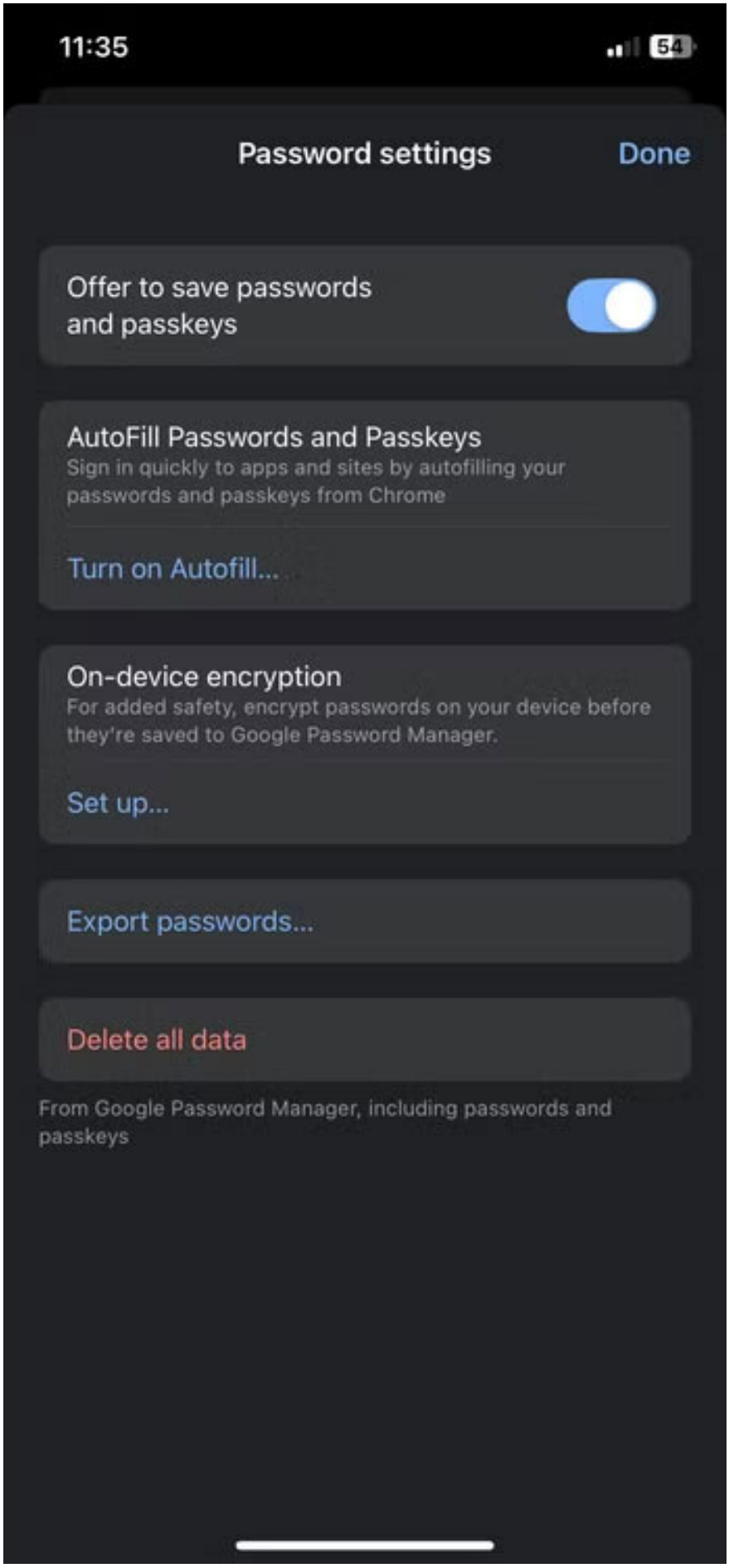
5. Turn on device encryption in Google Password Manager

Another lesser-known way to increase the security of your saved logins is on-device encryption. When on-device encryption is enabled, your logins are encrypted and decrypted only on your device. This adds an extra layer of protection to your saved passwords, ensuring that no one, not even Google, can access them.

The downside is that since you hold the keys to decrypt your passwords, you can't recover them unless you have access to your device or have set up recovery options. But that's the whole point. If you're serious about password security, enabling on-device encryption in Google Password Manager is a logical next step.


11:35
54
Google
Search or type URL
IP
5G/4G Wireless Ro...
J
Jumia Kenya | Online Shop...
IP
5G/4G Wireless Ro...
Internet Speed Test |...
Shortcuts
Bookmarks
62
Reading list
Recent tabs
History
Discover
Apple introduces ASIF disk image format in macOS 26 Tahoe for faster virtual storage
TechSpot · 1d
30


11:35
54
Google
Search or type URL
IP
5G/4G Wireless Ro...
J
Jumia Kenya | Online Shop...
IP
5G/4G Wireless Ro...
Internet Speed Test |...
Shortcuts
Recent tabs
Reading list
What's new
Password Manager
Bookmarks
Reload
New tab
New Incognito tab
Add to bookmarks
Add to reading list
Delete browsing data
Translate


11:35
54
Password settings
Done
Offer to save passwords and passkeys
AutoFill Passwords and Passkeys
Sign in quickly to apps and sites by autofilling your passwords and passkeys from Chrome
Turn on Autofill...
On-device encryption
For added safety, encrypt passwords on your device before they're saved to Google Password Manager.
Set up...
Export passwords...
Delete all data
From Google Password Manager, including passwords and passkeys

4. Secure your device with biometrics, PIN, or password

Even with a secure Google account, your device needs to be protected, as everything will be compromised if someone can easily unlock it. When using Google Password Manager, it is essential to secure your device with a PIN, password, or strong biometric authentication (like a fingerprint or facial recognition), as these act as a gateway to your passwords.

For optimal security, avoid leaving your device unprotected or using a weak screen lock mechanism that can be easily bypassed. Facial recognition can be used for convenience, but a PIN should be used as a backup. You can also use biometric authentication and have a PIN as a backup in case the first method fails due to physical damage or any other reason.

3. Only log in on trusted devices

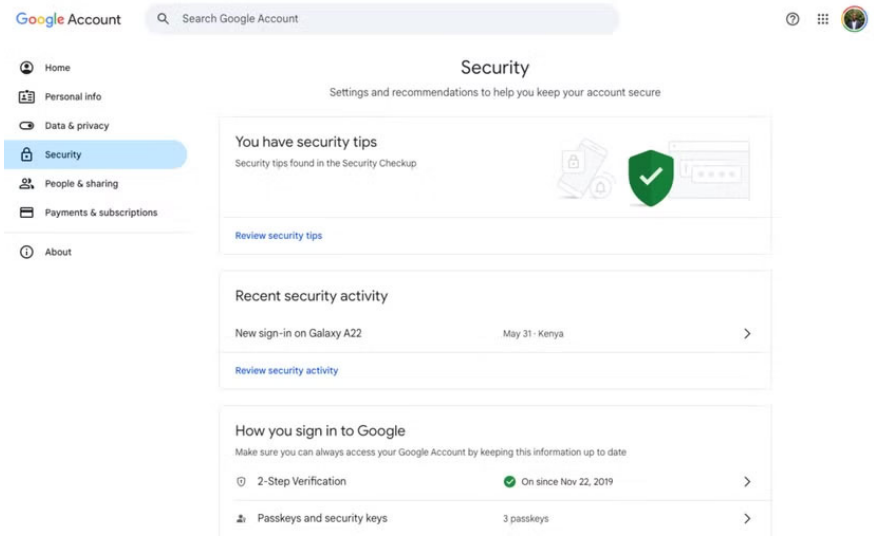
Since your Google account gives you access to all your saved logins, only sign in on trusted devices. Only sign in to your account on devices that are shared, public, or borrowed, as anyone else using them could access your saved logins.

However, if you must use someone else's device, use Chrome's Incognito or Guest Mode and always sign out when you're done. That way, you can be sure the device owner won't be able to access your saved passwords and any other personal data in your Google account after you're done.

2. Track Google account activity

You should also monitor your account activity to spot any suspicious activity early, such as if someone else has access to your password. Thankfully, Google lets you do this directly in your account management. However, the best option is to enable notifications so you can receive these security alerts in real time on your device.

Additionally, you can check the same information in your Google account by selecting the account profile icon and navigating to **Manage your account > Security > Recent security activity** .



1. Update your device regularly

Software updates are an important part of keeping your device secure. Even if you follow all of the recommended steps above, vulnerabilities in your operating system or applications can still leave your saved credentials vulnerable. Regular updates will patch these vulnerabilities before hackers can exploit them.

That's why it's a good idea to install updates as soon as they're available. It's also important to keep your apps up to date, and most importantly, your Chrome browser, since GPM integrates directly with it.