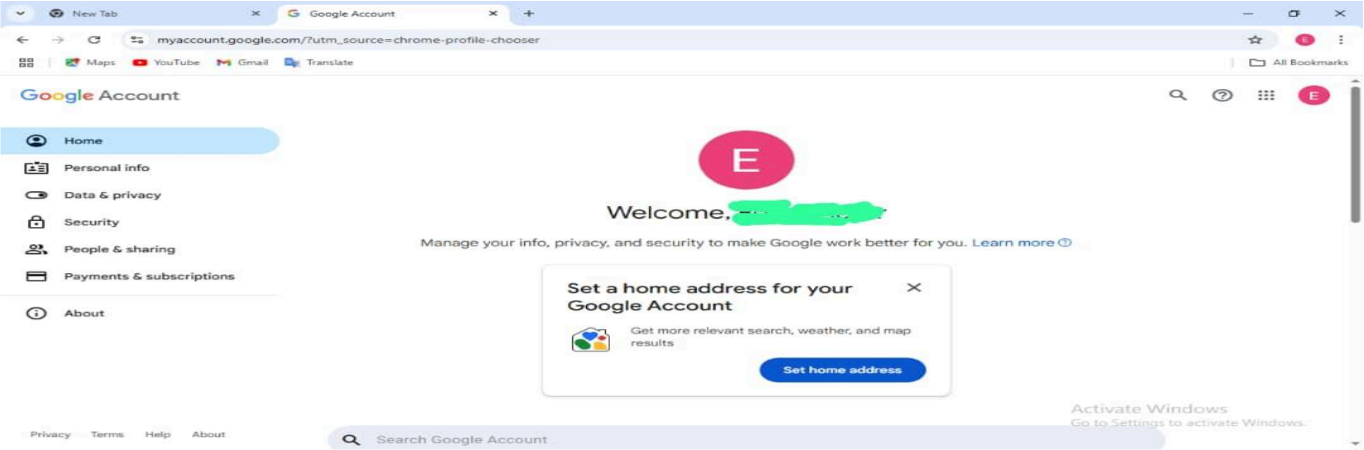
Implementation of Multi-Factor Authentication (MFA) on My Google Account

Steps followed to enable MFA:
Step1: I opened my browser and logged into my Google Account.
Step2: I clicked on security in the left-hand menu and located the signing in to Google section.
Step3: I Clicked on 2-Step Verification and I followed the prompts. I entered my password and proceeded.
Step4: I selected Text Message or Voice Call and entered my phone number.
Step5: I completed the setup by entering a code sent to my phone number and Google confirmed that MFA has been successfully enabled.
Step6: I logged out and logged in back, it shows I have to follow the MFA prompt. Access was granted to me after completing the second authentication step.

Chosen Authentication Method: Text Message or Voice Call

ScreenShot of Setup:

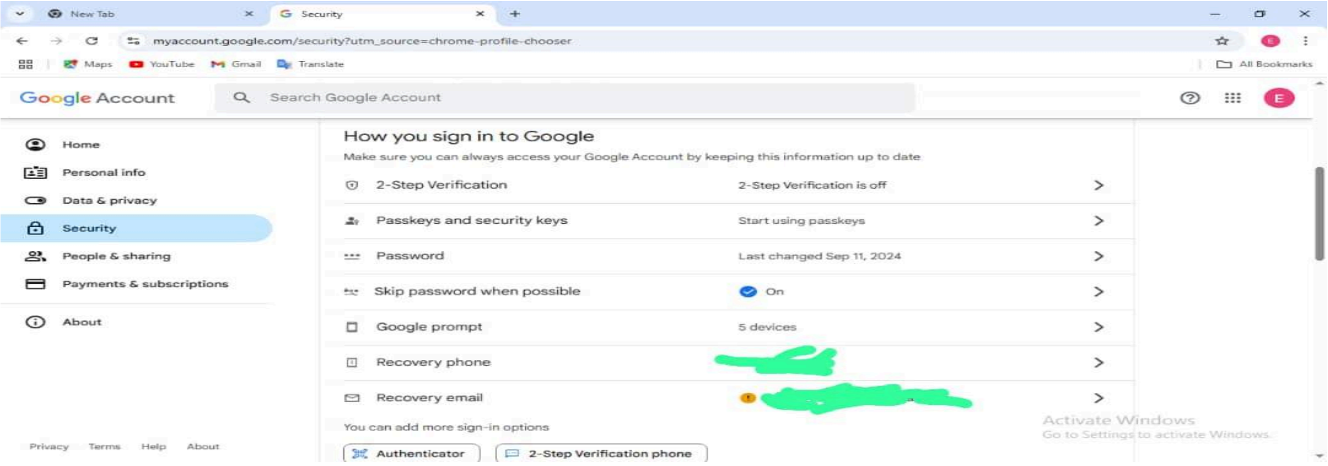


Welcome, [redacted]

Manage your info, privacy, and security to make Google work better for you. Learn more

Set a home address for your Google Account

Get more relevant search, weather, and map results

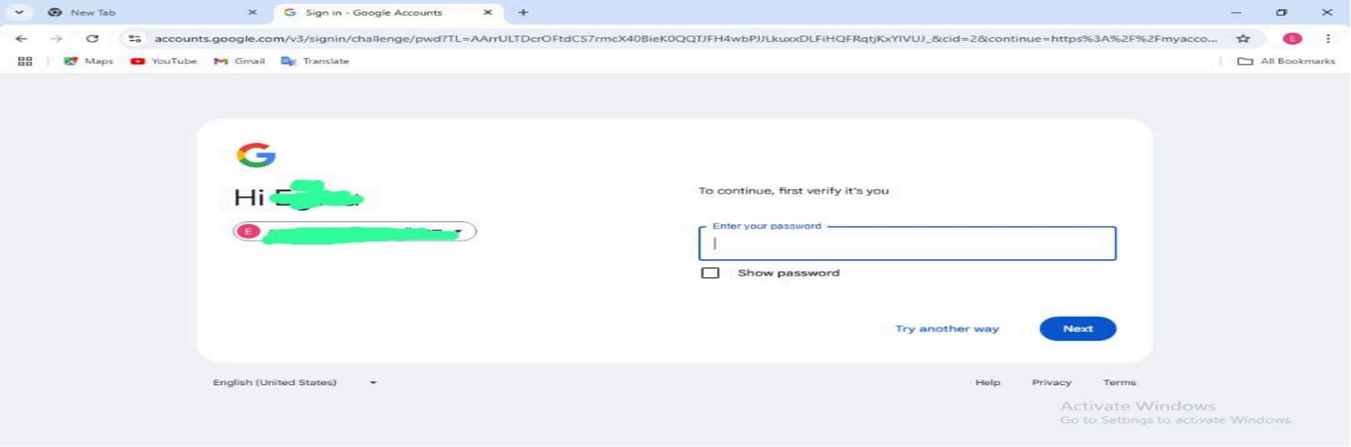


How you sign in to Google

Make sure you can always access your Google Account by keeping this information up to date

2-Step Verification	2-Step Verification is off
Passkeys and security keys	Start using passkeys
Password	Last changed Sep 11, 2024
Skip password when possible	✓ On
Google prompt	5 devices
Recovery phone	[redacted]
Recovery email	[redacted]

You can add more sign-in options


New Tab
Sign in - Google Accounts
accounts.google.com/v3/signin/challenge/pwd?TL=AArrULTDcrOFtdCS7rmcX40BieK0QQTJFH4wbPJJLkuxxDLFiHQFRqtjKxYIVUJ_&cid=2&continue=https%3A%2F%2Fmyacco...
Maps
YouTube
Gmail
Translate
All Bookmarks

Hi [redacted]

[redacted]

To continue, first verify it's you

Enter your password

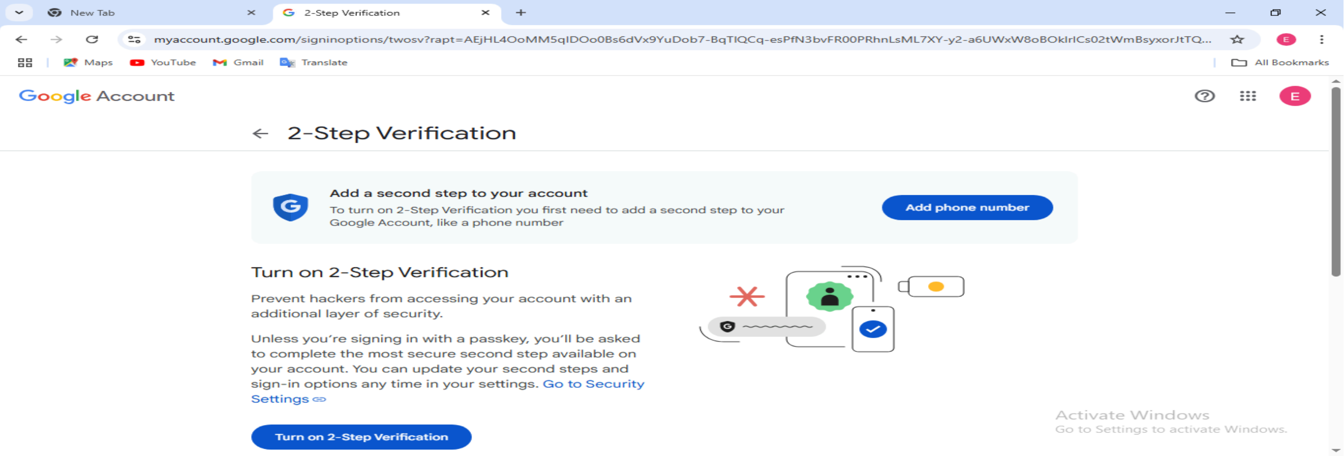
□ Show password

Try another way

Next

English (United States)

Help Privacy Terms


New Tab
2-Step Verification
myaccount.google.com/signinoptions/twosv?rapt=AEjHL4OoMM5qIDOo0Bs6dVx9YuDob7-BqTIQCq-esPfN3bvFR00PRhnLsML7XY-y2-a6UWxW8oBOklrlCs02tWmBsyxorJtTQ...
Maps
YouTube
Gmail
Translate
All Bookmarks
Google Account

← 2-Step Verification

Add a second step to your account

To turn on 2-Step Verification you first need to add a second step to your Google Account, like a phone number

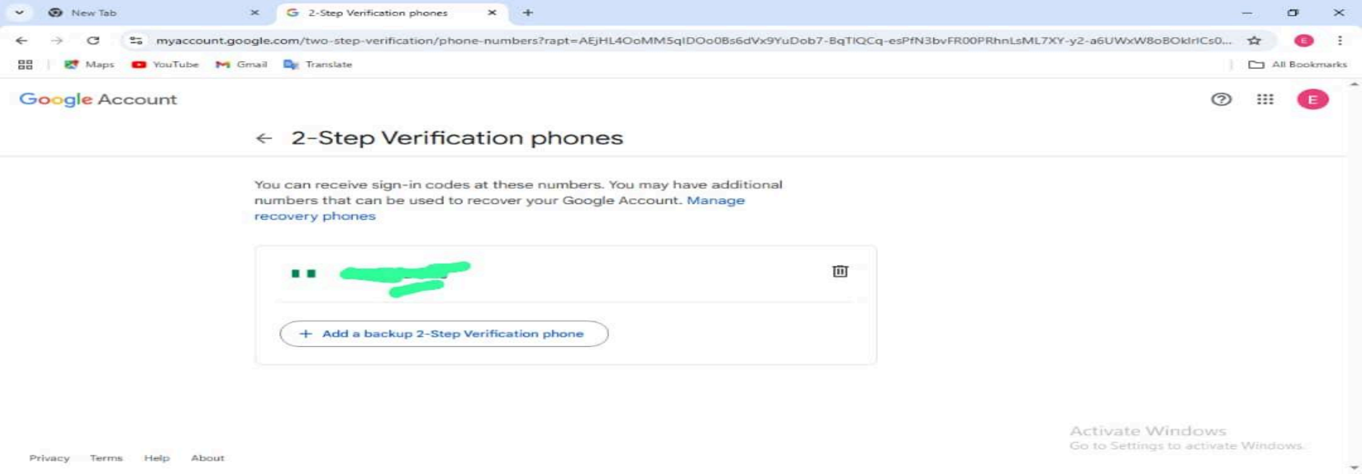
Add phone number

Turn on 2-Step Verification

Prevent hackers from accessing your account with an additional layer of security.

Unless you're signing in with a passkey, you'll be asked to complete the most secure second step available on your account. You can update your second steps and sign-in options any time in your settings. Go to Security Settings

Turn on 2-Step Verification


New Tab
2-Step Verification phones
myaccount.google.com/two-step-verification/phone-numbers?rapt=AEjHL4OoMM5qIDOo0Bs6dVx9YuDob7-BqTIQCq-esPfN3bvFR00PRhnLsML7XY-y2-a6UWxW8oBOklrlCs0...
Maps
YouTube
Gmail
Translate
All Bookmarks
Google Account

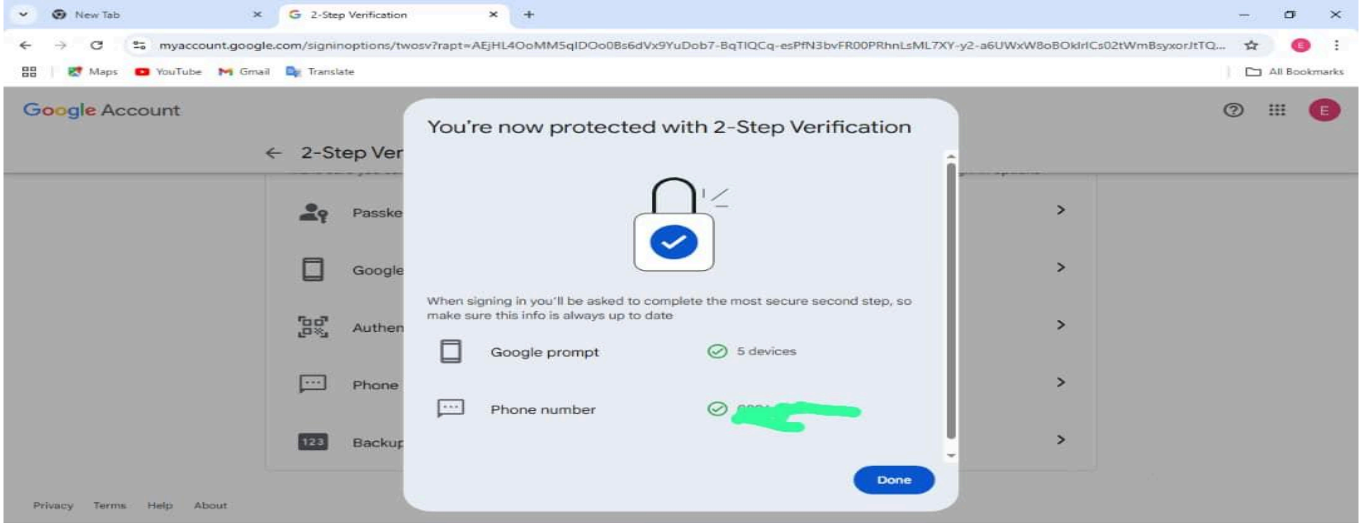
← 2-Step Verification phones

You can receive sign-in codes at these numbers. You may have additional numbers that can be used to recover your Google Account. Manage recovery phones

[redacted]

+ Add a backup 2-Step Verification phone

Privacy Terms Help About

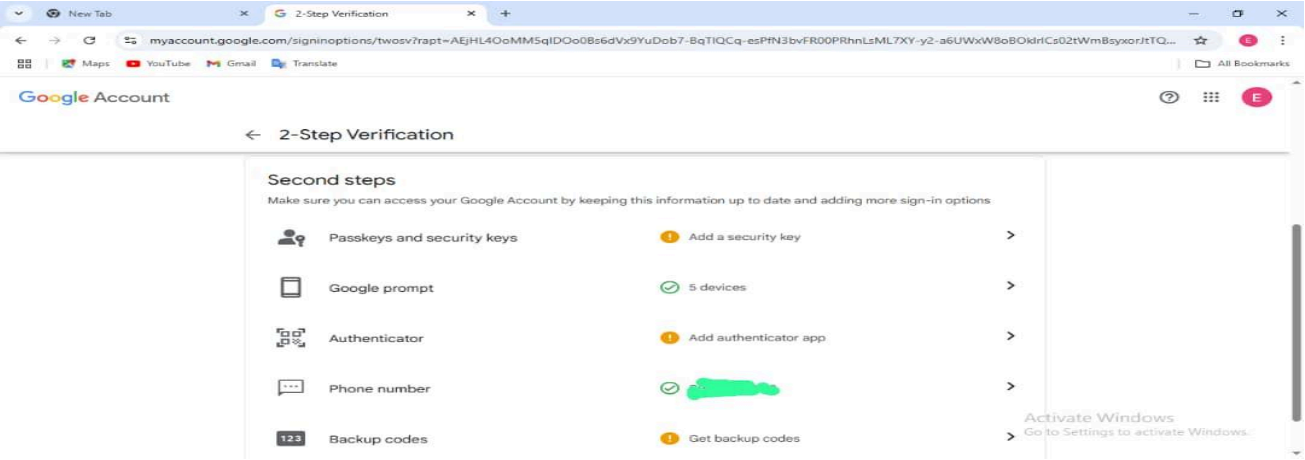


New Tab
2-Step Verification
myaccount.google.com/signinoptions/twosv?rapt=AEjHL4OoMM5qIDOo0Bs6dVx9YuDob7-BqTIQCq-esPfN3bvFR00PRhnLsML7XY-y2-a6UWxW8oBOkIrICs02tWmBsyxorJtTQ...
Maps
YouTube
Gmail
Translate
All Bookmarks
Google Account
2-Step Ver
Passke
Google
Authen
Phone
Backup
Privacy
Terms
Help
About

You're now protected with 2-Step Verification

When signing in you'll be asked to complete the most secure second step, so make sure this info is always up to date

Google prompt	✓ 5 devices
Phone number	✓ [redacted]



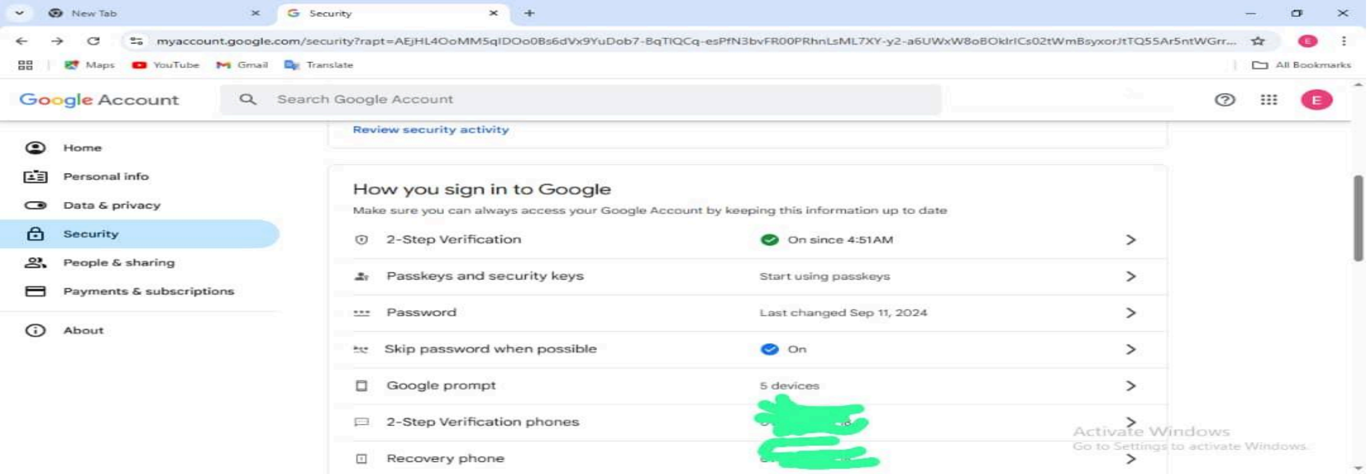
New Tab
2-Step Verification
myaccount.google.com/signinoptions/twosv?rapt=AEjHL4OoMM5qIDOo0Bs6dVx9YuDob7-BqTIQCq-esPfN3bvFR00PRhnLsML7XY-y2-a6UWxW8oBOkIrICs02tWmBsyxorJtTQ...
Maps
YouTube
Gmail
Translate
All Bookmarks
Google Account
Activate Windows
Go to Settings to activate Windows.

2-Step Verification

Second steps

Make sure you can access your Google Account by keeping this information up to date and adding more sign-in options

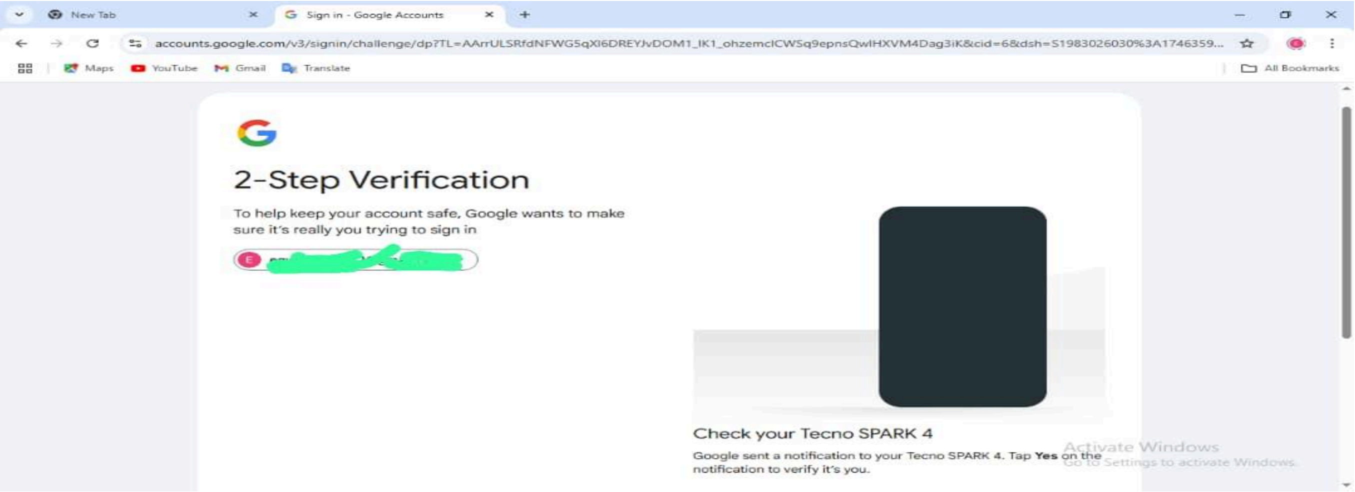
Passkeys and security keys	! Add a security key
Google prompt	✓ 5 devices
Authenticator	! Add authenticator app
Phone number	✓ [redacted]
Backup codes	! Get backup codes



How you sign in to Google

Make sure you can always access your Google Account by keeping this information up to date

2-Step Verification	✓ On since 4:51AM
Passkeys and security keys	Start using passkeys
Password	Last changed Sep 11, 2024
Skip password when possible	✓ On
Google prompt	5 devices
2-Step Verification phones	[redacted]
Recovery phone	[redacted]


New Tab
Sign in - Google Accounts
accounts.google.com/v3/signin/challenge/dp?TL=AArrULSRfdNFWG5qXI6DREYJvDOM1_IK1_ohzemclCWSq9epnsQwlHXVM4Dag3iK&cid=6&dsh=S1983026030%3A1746359...
Maps
YouTube
Gmail
Translate
All Bookmarks
Activate Windows
Go to Settings to activate Windows.

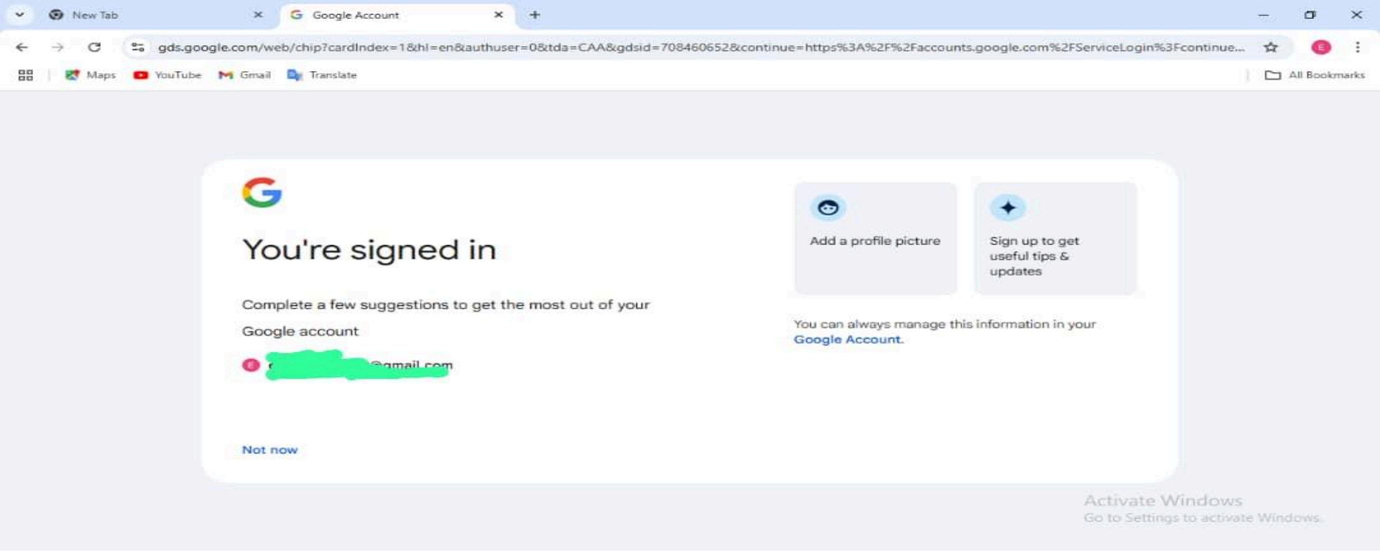
2-Step Verification

To help keep your account safe, Google wants to make sure it's really you trying to sign in

[redacted]

Check your Tecno SPARK 4

Google sent a notification to your Tecno SPARK 4. Tap **Yes** on the notification to verify it's you.


New Tab
Google Account
gds.google.com/web/chip?cardIndex=1&hl=en&authuser=0&tda=CAA&gdsid=708460652&continue=https%3A%2F%2Faccounts.google.com%2FServiceLogin%3Fcontinue...
Maps
YouTube
Gmail
Translate
All Bookmarks
Add a profile picture
Sign up to get useful tips & updates
Not now
Activate Windows
Go to Settings to activate Windows.

You're signed in

Complete a few suggestions to get the most out of your Google account

[redacted]@gmail.com

You can always manage this information in your Google Account.

Observations and Importance:

Multi-factor authentication (MFA) on Gmail is crucial for enhanced security, acting as an extra layer of protection against unauthorized access, even if a password is compromised. The process involves verifying user identity through multiple factors, typically including a password and a second verification method like a code from a phone or a security key.

Enhanced Security:

MFA significantly reduces the risk of unauthorized access, making it much harder for malicious actors to gain access to a Gmail account even if they have obtained the password.

Protection Against Phishing and Password Reuse:
MFA safeguards against phishing attacks where users are tricked into revealing their credentials and prevents the impact of password reuse, where the same password is used across multiple accounts.

Compliance with Regulations:
Many organizations and individuals are required to implement MFA for compliance with security regulations and industry standards.

User Trust and Confidence:
By demonstrating a commitment to security through MFA, organizations can build trust with users and demonstrate that they prioritize the protection of sensitive data.

Recommendations:
To maintain Gmail account security, it's crucial to use a strong, unique password, enable two-factor authentication, and regularly review security settings. Additionally, be cautious about suspicious emails and links, and update your software and devices.

Here's a more detailed breakdown:

1. Strong and Unique Passwords:

- **Create a strong password:** Avoid using personal information like birthdays, addresses, or nicknames. Use a combination of upper and lowercase letters, numbers, and symbols.
- **Use a password manager:** This helps you generate and store unique passwords for each account.
- **Avoid reusing passwords:** Using the same password across multiple accounts increases the risk if one account is compromised.

2. Two-Factor Authentication (2FA):

- **Enable 2FA:** This adds an extra layer of security by requiring a code from your phone or another trusted device in addition to your password.
- **Keep 2FA enabled:** Don't disable it after setting it up.

3. Security Checkup:

- **Run a security checkup:**
  Google's Security Checkup provides personalized recommendations for your account,

including adding recovery options, verifying your account, and reviewing security settings.

- **Review security activity:**
  Regularly check your recent security activity to identify any suspicious sign-ins or unauthorized access attempts.

4. Be Wary of Phishing and Spam:

- **Be cautious about suspicious emails:** Don't click on links or open attachments from untrusted senders.
- **Report suspicious emails:** Report spam and phishing attempts to help Google improve its detection capabilities.
- **Don't share personal information:** Never share your password or other sensitive information with anyone, including Google.

5. Software and Device Updates:

- **Keep your devices and software up-to-date:**
  Updates often include security patches that protect against known vulnerabilities.
- **Install security software:**
  Consider using antivirus and anti-malware software to protect your device from malware and viruses.

6. General Security Practices:

- **Secure your internet connection:** Use strong passwords for your Wi-Fi network and be cautious about using public Wi-Fi, which may not be encrypted.
- **Use a strong computer password:** Protect your device with a strong password and use a screen lock.
- **Sign out of your account when using public computers:** Always sign out of your Gmail account when using public or shared computers to prevent unauthorized access.
- **Update your account recovery options:** Ensure your recovery phone number and email address are up-to-date.