KNOWLEDGEFLOW
CYBERSAFETY FOUNDATION

A Guide to Digital Self-Defense: Cybersafety for Personal Safety

Contents

Chapter 1:

Introduction

This toolkit is a comprehensive guide to help individuals and organizations to recognize, be more aware of, and to respond to instances of technology abuse. In the modern era, technology has become an essential part of our daily lives which helps us to connect and communicate with people around the world. However, technology can be misused as a tool to control, intimidate, and harm people. The types of misuse range from cyberstalking and harassment to financial exploitation and it can have serious consequences for its victims. This toolkit is designed to provide information, resources, and strategies to empower individuals and organizations to recognize, prevent, and respond to technology abuse. The toolkit will provide valuable insights and tools to assist you with navigating complex issues.

Resources in Canada

Immediate help that is available at the following national hotlines. All services are provided 24/7 and are free.

Government of Canada

https://www.canada.ca/en/public-health/services/mental-health-services/mental-health-get-help.html

Victim Services in Ontario

- https://www.ontario.ca/page/victim-services-ontario#:~:text=Victim%20Services%20Directory%20and%20Support%20Line&text=call%20the%20Victim%20Support%20Line,a.m.%20%E2%80%93%209%20p.m.%20Eastern%20Time
  - Sheltersafe.ca – map for shelters
  - Youth and Young Adults
    - Kids help assistance either call 1-800-668-6868 or text message CONNECT to 686868. 24/7 service.
  - Indigenous People
    - 1-855-242-3310 (toll-free) 24/7.
  - Ontario
    - Victim 24/7 Support Line: 1-888-579-2888
    - Assaulted Women's Helpline: 1-866-863-0511
  - Older Adults
    - Canadian Network for the Prevention of Elder Abuse (CNPEA)
    - https://cnpea.ca/en/

Additional Resources:

- Women's Shelters
  - https://sheltersafe.ca/
- Ontario Network of Sexual Assault and Domestic Violence Treatment Centers
  - https://www.sadvtreatmentcentres.ca/find-a-centre
- Talk4Healing for Indigenous Women
  - https://www.beendigen.com/programs/talk4healing/
- Trans Lifeline
  - https://translifeline.org/
- Nisa Helpline for Muslim Women

  - https://nisahelpline.com/
- Fem'aide for French-speaking women
  - www.femaide.ca
- Assaulted women's hotline
  - www.awhl.org/home

Federal government website that offers general information on family violence. https://justice.gc.ca/eng/cj-jp/fv-vf/help-aide.html

List of community services by the Federal government. https://women-gender-equality.canada.ca/en.html

Supporting the Victim of Tech Enabled Abuse

- **Be aware of the risks.**
  - Many victims are being monitored by their abusers so be careful when reaching out. They may be tracked through social media, phone calls/messages/ or email. Leaving a voicemail or reaching out may put the victim in more danger.
- **Ensure your own safety.**
  - Do not do anything that may put yourself in danger or an unsafe situation such as confronting the offender.
- **Find resources.**
  - Before speaking with the victim, find resources such as local shelters, crisis lines, or any other services that specialized in victims of abuse.
- **Be aware of the time and place to help.**
  - Be wise about the location and time you speak with the victim. Choose a time when you will not be overheard, seen, or interrupted.

Reminder: If someone is in immediate danger, call 911.

Services:

- Crisis Lines
  - Ontario
    - Victim 24/7 Support Line: 1-888-579-2888

Victim’s Rights

https://victimsfirst.gc.ca/serv/vrc-dvc.html

On July 23, 2015, the Victims Bill of Rights Act came into force.

The Bill outlines the rights that victims of crime have:

- Right to Information
- Right to Protection
- Right to Participation
- Right to seek Restitution

Right to Information

Victims have the right to get information about how the justice system works and services/programs that are available to them. Also, victims have the right to be given any information regarding the progress of a case, this includes information about the investigation, prosecution, and sentencing of the person who had caused harm to them.

- Information the victims may request:
  - The criminal justice system and their role of being a victim.
  - The available services/programs (restorative justice, shelter)
  - Their right to make a complaint if they feel their right has not been respected.
- Also request information about the case
  - The status/outcome of an investigation.
  - Scheduling, progress, and outcome of criminal proceeding.
  - Any review of the offender’s conditional release, timing, and condition.
  - A copy of any orders regarding bail, conditional sentence, and probation.
  - Information about the accused who has been found unfit to stand trial or found to be not responsible due to mental disorder while that person is under jurisdiction of a court/review board.

Information for Registered Victims

Victims who have been registered with the Correctional Service of Canada or the Parole Board of Canada could receive information on:

- Status of the offender and the progress on their correctional plan
- Offender’s release date, destination, and conditions unless the information is harmful to the public safety.

- Copies of the Parole Board of Canada verdicts.
- Victim-offender mediation services.

Right to Protection

Victims have a right to their security and privacy and it is considered at various stages of the criminal justice process. They should also have reasonable and necessary protection from intimidation or possible retaliation from the offender. Also, victims have the right to ask for a testimonial aid at their court appearance.

Security and Privacy

Canadian Victims Bill of Rights provides the victims:

- Having security and privacy considered by the criminal justice personnel.
- Be protected from offenders who try to intimidate or retaliate.
- Request the courts for their identity not to be released to the public.

Victims have the right to ask for testimonial aid when they are testifying in court. It is also now easier for courts to order testimonial aids. The court's consideration includes a number of factors, security, and protection of witnesses, and decide whether to allow victims to give their testimony by closed-circuit tv, behind a screen, or with a support individual close by. Under 18 years old can request, and publication bans are mandatory.

Victims of sexual assault cases are protected under the amendments to the Criminal Code. They have since changed how the third-party records are handled.

The Crown now has the ability to request the spouse to testify in all cases to help ensure the prosecutors have access to all significant evidence.

Right to Participation

Changes to the Laws

Victims now have a role in the criminal justice system through meaningful participation in the parole and conditional release system.

These changes include:

- Requires the judge to include in the record of the bailing process that they have considered the victim's safety and security.
- Include that they acknowledge the harm that has been done to the victim and the community as the sentencing objective under the Criminal Code

- Allow the victim to use a testimonial aid when they are presenting the Victim Impact Statement in court.
- Also, allow the victim to bring a photograph of the victim to court when they are giving their Victim Impact Statement
- Provide a standardized form for the victims and the community to ensure consistency in how impactful the crime has been to the victims including physical/emotional harm, property damage or financial loss.
- Allow the victims to include a picture/drawing if it helps them express the impact of the crime.
    - The VIS can be used by the Review Board when concluding about the accused individual found to be not criminally responsible due to conditions including mental disorder.

Corrections and Conditional Release

- Victims have the ability to listen to the audio recording of the hearing for victims that could not make it to the parole hearing.
- They can designate a person to represent them to receive information on their behalf.
- If victims choose to, they have the ability to waive access to information about their offender through the Correctional Service of Canada and the Parole Board of Canada.

Right to Seek Restitution

Victims have a right to have the court think about restitution orders and enforce any unpaid restitution order through a civil court.

Changes made to the Criminal Code

- Victims can voice the losses they have occurred due to the harm they have received because of the crime at the sentencing.
- Standardized form is available for victims to help claim their losses. Easy to calculate and based on records of financial loss. The amount lost is calculated up to the date the offender is sentenced.
- Courts need to consider any ordering restitution for all offences.
- An offender’s ability to pay the restitution is not a factor when the court orders the restitution.
- The courts can include information about the payment schedule in their judgement.

Financial Losses

Restitution can be ordered with financial losses related to:

- Damaged or lost property from the crime.
- Physical or psychological harm from the crime.
- Physical injury from the arrest or during the attempted arrest of the offender.
- Costs for temporary housing, food, childcare, and transportation due to the moving out of the offender's household.
- Costs that the victim of identity theft had to pay to re-establish their identity, and to correct any credit history/rating.

Chapter 2:

Technology Safety Information

This chapter will provide information about technology abuse including general technology safety, the misuse of technology, stalkerware, tracking devices, etc. As we all are becoming more aware, technology has drastically changed how we live and work. There are many benefits and conveniences, but it has also made us more vulnerable to technology misuse. This chapter will provide some tips and strategies for staying safe online and protecting your personal information.

Technology Safety

https://www.techsafety.org/resources-survivors/technology-safety-plan

Prioritize Safety

1. If the person causing harm has had access (physical or remote) to your computer, tablet, or phone then you will have to assume that it is being montirored. Use a deviceg that the individual would not have had physical access or remote access in the past or present. This way you can communicate safely without that person monitoring.
2. Find a Victim Advocate to help you create a plan for your well-being.
3. Trust your instincts. If you think the individual causing harm knows too much about you then they could be receiving that information from a couple of sources such as online accounts, tracking your location, or gathering your information online.
4. Have a Strategic Plan. The initial reaction of wanting the offender to stop is either to throw away the device or delete online accounts. This could lead the offender to increase or escalate their dangerous behaviour. Think about a safety plan for yourself if you remove devices like a hidden camera or GPS tracking devices. Consider reporting these found devices to the police.

Identify the Source of Tech Abuse (if possible)

1. Think about the potential technology that might be used to stalk, monitor, or harass you. Does the individual causing harm only show up when you are at home? Check for hidden cameras. If you notice that you are being followed often, then they might have a tracking device on your car/phone. Find the potential sources, document, and report the abuse.

Documentation Tips

- Keep track of all the incidents including the date, time, and the suspected technology used. If it is reported to police then take note of the officer’s name and any witnesses if available. Take a photo or screenshot of emails, text messages, or voice mails. Sometimes the other party can manipulate messages and delete them. Stay safe and do not let the offender know that you are gathering information about the instances. They may try to escalate the situation and cause more harm if they find out.

- Document call logs, phone calls (check if you can record the phone call through local police), social media, emails, texts.
- Do not delete the evidence as some things like emails could be used to find the possible location of the sender.

Ways to Increase Security

- Change your passwords and usernames. Once you have changed the password/username, be careful accessing these accounts on devices you may suspect of being monitored. Do not use information that may give away your identity when creating new profiles or updating. Do not use the same password for multiple accounts.
- Check your devices & settings to confirm your devices/accounts are not connected to others. For example, Bluetooth, turn it off when you are not using it. Delete apps if you are not familiar with them.
- For more serious instances where you may suspect your device is being monitored. The best option is to get a new device. When you get the new device do not connect your old accounts such as Google or Apple that the individual causing harm may have access to. Turn off the location tracking and Bluetooth. A possibility is keeping your old device so the individual may suspect you are still using the device and do not attempt to track the new device.
- Protect your location by turning off any trackers through your phone or vehicle. If there is a concern about a location tracker on your car then contact the local police, an investigator, or a mechanic. Document any evidence before removing such devices.
- Beware of gifts from the individual as they could contain hidden cameras.

Steps to Increase Privacy

- Protect your address by telling your friends and family not to share your address especially if you move to a new location. Be careful when you are giving out your address to local businesses. Check to see if your local municipality has an address confidentiality program.
- Limit the information you put out there when making a purchase or creating an account online. This information is sold to other parties so people can have

access to them. Minimize any information collection and provide only the necessary.

- The person causing harm could use the victim’s phone or through a shared account gain access to their health status, location, messages, internet searches, or calls.

Location Privacy

- Try not to search for locations or make plans through your phone, email, internet browser, or messaging apps.
- Pay cash or one-time passes instead of transit passes connected to your name.
- Search your car/belongings to see if there are any devices that are tracking you.

Communication/Information Privacy

- Use a library or public computer but do not log into any shared or monitored accounts.
- Use a web form to send messages.
- Set up new accounts using fake information and do not use devices that are possibly compromised by previous physical or remote access by the persona causing harm.

Disconnecting From the Person Causing Harm

https://www.ceta.tech.cornell.edu/_files/ugd/c4e6d5_20fe31daffd74b2fb4b4735d703dad6a.pdf

Before disconnecting, consult with a case worker for domestic violence and seek support. It will be obvious when changes are made to any shared accounts. Be aware the persona causing harm will know. Use the appropriate resources/organizations to create a safety plan.

Please note this section will briefly go over some ways to increase safety on your devices. There are more detailed sections within this toolkit in chapters 3 and 4.

Checklist

1. Make a list of the devices that you connect to like phones, laptops, tablets, then change the passcode to access each device.
2. Create a list of all your online accounts and how you log into those accounts.
3. Can you delete any of those accounts and create new ones? Are any of the accounts shared? Can any of those be deleted? Change the password on all accounts possible.
4. Remove saved passwords on any web browsers.
    a. For Google Chrome.
        i. Settings
        ii. Passwords
    b. Firefox
        i. Preferences
        ii. Privacy
        iii. Scroll to find Logins and Passwords
        iv. Saved Logins
    c. Safari
        i. Preferences
        ii. AutoFill
        iii. Edit
5. Change your passwords and create a strong password. This should be long with a mix of capital/lowercase letters, and use symbols and numbers.
    a. Use something the person causing harm would not guess so do not include birthdays, or names.
    b. When setting up a security question to log into an account, do not use answers that could be guessed. Make up fake answers to questions like "the name of the street you grew up on".
    c. Password manager programs can keep track of your passwords and the fake information you provide to security questions.
6. Check which apps have access to your location, contacts, microphone, camera, etc..
    a. iPhone
        i. Settings
        ii. Privacy. A list of the apps will show up.
        iii. Click on each app to see the permission granted.
    b. For Androids
        i. Settings
        ii. Apps

iii. Settings

iv. Applications. Click on each individual app to see Permissions.

7. Check your phone’s location setting.
   a. For iPhone,
      i. Settings
      ii. Privacy
      iii. Location Services.
         1. This will show you the apps that have access to your location. You can decide which apps can track you.
   b. It is recommended as well on iPhones to check the Share My Location,
      i. Settings
      ii. Privacy
      iii. Location Services
      iv. Share My Location.
      v. You can check who has access to your location and you could also decide if you want to turn off Find My iPhone.
   c. For Android
      i. Settings
      ii. Location
      iii. App Permission. If that does not work then,
      iv. Apps
      v. Settings
      vi. Applications. Click on each individual app to see Permissions. Check the location.
8. Check each social media account’s privacy and security settings.
9. Photo Settings
   a. iPhone
      i. Settings
      ii. Apple ID
      iii. iCloud
      iv. Photos.
      v. Check to see if Shared Albums is turned off. If you had shared with someone previously you can remove the person or delete the shared album. To delete someone/album, Open the Shared Album>People>Remove Subscriber/or/Delete Shared Album.
   b. Android Users
      i. Google Photos

        ii. Sharing
        iii. More
        iv. Stop sharing your library.
    c. To remove
        i. Sharing
        ii. Name
        iii. More
        iv. Settings
        v. Remove Partner
        vi. Remove.

10. You can check if others are logged into your Google account by going to https://myaccount.google.com. And entering your email. Security>Your devices.
    a. You can log them out of the devices by they may be notified so be careful when doing this step.
11. Check location settings on other devices such as smartwatches, tablets, etc.
12. Privacy settings on web browsers,
    a. Turn on the 2-Factor Authentication if possible.
13. Check all applications on your devices and see if you recognize all of them. If you do not recognize any you should delete them.
14. If you have any children and you are afraid that the person causing harm may have access to those devices, repeat the steps with those devices.

Some categories of shared accounts to verify.

- Food
    - UberEATS
    - Door Dash
    - SkiptheDishes
- Music
    - Spotify
- Smart speakers
    - Google Home
- Banking and Financial
    - Online banking
    - Stocks
    - PayPal
    - Credit cards
    - Cash Apps

    - Retirement Accounts
- Phone
    - Shared Plans
- Car
    - GPS
    - Apps (Waze)
- Home Technology
    - Ring
    - Nest
    - Alarm System
    - Smart door locks
- TV
    - Netflix
    - Disney
    - Amazon Prime
- Shared Car Rides
    - Uber
    - Lyft
- Traveling
    - Trivago
    - TripAdvisor
    - Airlines
- Utilities
    - Cable/Internet
    - Water/Gas
- Workout Apps
    - Garmin
- Cloud Storage
    - Dropbox
    - Amazon/Google Drive

Stalkerware & Location Tracking

https://www.certosoftware.com/insights/how-a-little-known-iphone-feature-is-opening-the-door-for-cyberstalkers/

The Overview of Stalkerware

The introduction of spyware and Stalkerware have made it easier for offenders to track, monitor, and harass their victims. They can use spyware to secretly monitor what the individual is doing on their mobile device. If you are concerned about spyware, be careful when searching on your device as the abuser can see what you are doing. Try using a new device or another one the abusive person is not monitoring. Trust your instincts and look for patterns to understand what the abuser might be doing.

What is Spyware or Stalkerware?

Spyware or Stalkerware can be applications, a software program, or a device that will give another person (abuser) the ability to secretly monitor and record activity about another person's computer/phone. These tools are intrusive and one of the more dangerous forms of misuse through technology. Spyware provides remote access to conduct surveillance, harassment, abuse, stalking, and/or violence without the user's consent. The software could be hidden on a device and does not provide persistent notification that it is installed. Difficult to detect and remove. There are other features on a phone such as "Find my Phone" or family locater services which raise a concern as well.

Generally, Spyware is illegal. It is illegal to monitor and set up surveillance of another person without their permission or knowledge. This violates laws from stalking or harassing to illegal access to a device.

Almost all Stalkerware requires physical access to the device to install it. It will run in stealth mode without any notifications, so it makes it difficult to detect.

Phone Stalkerware & Safety for Survivors

Detecting stalkerware can be difficult but look out for signs like your battery rapidly draining, your device turning on and off, and spikes in data usage. The most common sign though is the person's suspicious behaviour. They may know too much information about your phone activities so trust your instincts and look for patterns. Have a professional check your phone. Before removing apps like stalkerware think about your safety. Sometimes the abuser may escalate their behaviour because it is removed. Create a safety plan through resources provided to assist with the process.

Document all the things you are experiencing.

To remove stalkerware, you can do a factory reset on your phone but be careful when reinstalling apps or files from a backup as it can re-load it onto the device again. Create a new iCloud or Google account for your device.

Preventing Stalkerware

- **Consider access**. Beware of new gifts from an abuser. Be careful when giving your phone to someone else. Stalkerware is quick to install.
- **Update accounts**. Change your passwords and set up 2-step authentication when it is available.
- **Lock your phone.** Setting up a password for your phone will minimize the risk as they require physical access to the device.
- **Use anti-virus and anti-stalkerware protection.** Download security apps for your device so they can scan your phone for potential malware or stalkerware apps.
- **Use security features.** Review your security features on the device. Android phones have the option to allow installation from "unknown sources", confirm that it is not turned on. Always install the latest updates on your phone.
- **Do not root or jailbreak your personal phone.** Rooting or jailbreaking means that you are removing the operating system limitations in order to allow third-party installations. This will be impactful on the built-in security features that protect the device. Many stalkerware features do not work unless there is a vulnerability by the manufacturer.

If an individual has access to your physical phone or your cloud account they may not need any spyware apps. They may also use friends and families to gain information about you. Look for patterns in what the person may know and where they could get that information from.

Computer Stalkerware & Safety for Survivors

Spyware on the computer can keep track of almost everything you do on your computer. Some spyware could give the abuser access to your webcam/microphone, take screenshots, and shut down or restart the computer.

This can be installed remotely by sending an email or message with an attached file or link. Be aware, it can automatically install when you open an attachment or click on any links. If you are ever suspicious, do not open links even if they are from friends. They can also be sent through instant messages, computer games, or other ploys to get you or your children want to click on the link.

Responding to Spyware

- **Safety first.**
  - The abuser may escalate their abusive behaviour if they suspect the victim is removing the spyware and cutting their access. Create a safety plan before cutting off access and reach out for help.
- **Gather evidence.**
  - Gather and preserve evidence of all your activities so law enforcement can analyze the information. This can lead to taking a criminal investigation.
- **Remove spyware.**
  - Difficult to remove spyware, you can consider wiping and rebuilding the computer by reinstalling the operating system. This is not a guaranteed procedure that will work. Get a replacement hard drive for the computer or get another computer. Be careful copying files from the infected computer to the new computer.
- **Use devices that aren't monitored.**
  - Use a computer or device that the individual in question does not have physical access to do research. Reminder, the person can see all activities including, online chat, emails, and web searches. You may want to use a library computer or a friend's device.
- **Update accounts.**
  - Consider resetting your passwords on different devices and no longer accessing certain accounts from your computer.

Preventing Spyware

- **Consider access.**
  - Be suspicious if someone is suggesting installing a new keyboard, cord, or software to your computer to "Fix" it. Beware of gifts for you or your children.
- **Create separate users or guest accounts.**
  - Create guest accounts that have settings that do not allow software or apps to be installed without the admin's login. This can prevent accidentally installing any spyware/malware.
- **Use anti-virus and anti-spyware protection.**

  - Install anti-virus and anti-spyware programs and regularly scan your computer. These programs can help prevent the programs from being installed. They would be best before the computer has been compromised.

Reminder if a person has physical access to your computer, they may not need to install spyware. They can also remotely receive information if they already have access to your accounts.

Location Tracking

Location privacy is important to safety. Sometimes phones and apps can track your location without your knowledge. There are also tracking devices such as the GPS in your car that can be misused to monitor your location. Location tools can also be beneficial. They could be used to gain information about where your children are or to find lost phones or keys or to identify if an offender is close.

Step 1: Prioritize your Safety.

- **Get more information.** Professionals can assist with creating a safety plan. See local resources.

Step 2: Narrow down potentials for how you might be getting tracked.

- Are there patterns to what the abuser may know? Do you think you are being tracked in real-time or only where you have been previously?
- Do you share any accounts with anyone else? Does anyone have access to your phone or have information to log in to your accounts?
- Are you using apps that share your location?
- Could your friends and family share your location? Sometimes location can be shared through social media posts.

Step 3: Learn more about how technology works.

Phones & Mobile Devices

- Phones can be tracked by your location through built in GPS, Wi-Fi connections may reveal your location, and cell towers which connects the phone and your cellular carrier. The location on your phone can be turned off but the emergency services and phone companies will have access to your location when your phone is on.

- Phones can connect from your Apple or Google account that has features like help find your lost phones. People who have access to your account can see the location of your phone.
- Phones, tablet, or laptops keeps a history of past Wi-Fi networks you have access to and you can delete that.

Apps & social media

- Check your location and privacy settings for apps.
- Camera and photo apps can also store the location where the photo was taken. Location settings can be turned off in your phone settings.
- Friends and family might share your information through social media. Check when they are mentioning you in a post. Check your app to see if you can set up notifications when they mention you or if it is available to change your privacy settings to not allow others to share your location.
- Some apps request your locations such as shopping apps, ride-share services, or food-delivery services.
- Spyware (Stalkerware) could also be installed on your phone without your knowledge.

Global Positioning System (GPS)

- Many cars have GPS built in and store your location history.
- These devices can also be placed on a vehicle or personal belongings to track someone. They can be hidden very easily because they are tiny and hard to find.
- These devices can be in real-time, sharing the data directly with the abuser.

Location Trackers

- Newer devices can be small and can be hidden in a bag or in gifts.
- Unlike, GPS devices, these do not need to be connected to a power source.
- They are connected to an app or online account.
- They use a combination of GPS, active RFID (Radio Frequency Identification), Bluetooth LE(low energy), and Wi-Fi networks.

Step 4. Safety & Privacy Settings.

Be aware making these changes could alert the abuser. This may also erase the evidence.

- Documentation.

    - Even without knowing how you are tracked. Indicate when the abusive person knows your location. Take note of when and where they have appeared when you least expected them to be there.
- Finding the device or service
    - Check your car, in the trunk, under the hood, inside the bumper, under or between your seats.
    - Check your belongings, look for items that do not belong to you.
- Reporting the abuse
    - Victim services and advocates can help you.
    - Notify law enforcement.
    - Get legal aid.
    - Contact the company to request the abusive person not have access to your location.
- Removing, blocking, or jamming.
    - When it is safe remove the device or turn off location sharing.
    - As part of the safety plan, sometimes people leave the tracking on to gather evidence.
    - Some counter-surveillance may jam or stop the communication of the location- tracking device.

The Internet of Things

https://thewhitehatter.ca/digital-inoculation-guide-to-taking-back-control-leaving-abusive-relationships-steps-to-protect-yourself-from-tech-abuse/

Replace your home router, establish a guest network for smart/connected devices and reset all devices:

Cameras:

- **Nest**: https://support.google.com/googlenest/answer/9252162?hl=en#zippy=
- **Logitech Circle:** https://support.logi.com/hc/en-ca
- **NetgearArlo:** https://kb.arlo.com/1057976/How-can-I-reset-my-Arlo-SmartHub-or-base-station-to-the-default-values
- **Ring Stick Up:** https://support.ring.com/hc/en-us/articles/115000125926-Stick-Up-Cam-Setup-Mode

- **Ring Spotlight:** https://support.ring.com/hc/en-us/articles/115003835483-Spotlight-Cam-Setup-Mode
- **Amazon Cloud:** https://www.amazon.com/gp/help/customer/display.html?linkCode=w61&imprToken=gaX.lG7AS6v6wGWZYX62bQ&slotNum=0&ascsubtag=e99519292933a52d5c1bdf4f4b176faebf364aaa&nodeId=202161680&tag=lifehackeramzn-20
- **Blink**: https://support.blinkforhome.com/categories/how-to-videos-BkFoXlQIB

Thermostats:

- **Nest Thermostat**: https://support.google.com/googlenest/answer/9247296?hl=en
- **Ecobee Thermostat**: https://support.google.com/googlenest/answer/9247296?hl=en
- **Honeywell Thermostat**: https://www.honeywellhome.com/en/questions/how-do-i-complete-a-factory-reset-on-the-lyric-round-thermostat

Light Switches:

- **Lutron Caseta dimmers:** https://www.wink.com/help/products/lutron-caseta-in-wall-dimmer-and-pico/
- **Echobee Switch**: https://support.ecobee.com/hc/en-us/articles/360026508712
- **TP-Link Switch**: https://www.tp-link.com/us/support/faq/265/
- **Insteon Switch**: https://www.insteon.com/support-knowledgebase/2016/2/24/factory-resetting-insteon-hub

Lights:

- **Philips Hue**: https://labs.meethue.com/support
- **LIFX**: https://support.lifx.com/hc/en-us/articles/200468240-Hardware-Resetting-your-LIFX
- **Cree Connect**: https://support.smartthings.com/hc/en-us/articles/204258280-Cree-Connected-LED-Bulb

Doorbells:

- **Ring**: https://support.ring.com/hc/en-us/articles/115000125086-Ring-Video-Doorbell-Setup-Mode
- **Skybell**: https://skybelltechnologies.zendesk.com/hc/en-us/articles/203317075-SkyBell-HD-Device-Reset

Home Hubs:

- **Samsung SmartThings**: https://support.smartthings.com/hc/en-us/articles/204936890-How-do-I-factory-reset-the-Hub-delete-a-Location-
- **Iris Smarthub**: https://www.irisbylowes.com/support?guideTitle=I-have-a-new-hub-that-I-can't-add-to-my-Iris-account.&guideId=137aff1c-a4a5-404a-8c58-1320cb59f312
- **Apple Home**: https://support.apple.com/en-ca/HT204893

Smart locks:

- **August Smart Lock**: https://support.august.com/how-do-i-factory-reset-my-lock-BkH1D8y0uG
- **Schlage Sense**: https://www.schlage.com/content/dam/sch-us/documents/pdf/installation-manuals/Schlage-Sense-User-Guide-P516-991.pdf
- **Schlage Encode Smart Wifi Deadbolt**: https://www.schlage.com/en/home/support/faqs/schlage-encode.html
- **Nest X Yal**: https://support.google.com/googlenest/answer/9218474?co=GENIE.Platform%3DAndroid&hl=en
- **Lockly Secure Plus**: http://www.support.lockly.com/article/how-to-do-a-factory-reset/
- **SimplySafe Smart Lock**: https://support.simplisafe.com/hc/en-us/articles/360033366692-Smart-Lock-Setup-Updating-your-system-before-installing

Children, Teens & Tech

https://www.techsafety.org/survivor-toolkit/teens-and-technology

Use and Misuse of Popular applications

It is important for adults to understand popular apps and their function of those apps. A general understanding of the apps can help relate to young people and support their positive use of technology. Most social media apps are similar, and they are used to build connections.

- YouTube

    - Used to share and create videos, watch videos, show creative talent, gaming, product review, and earn money.
    - Types of misuse are creating false video names, bullying, harassment in comments, and harmful prank videos.
- Instagram
    - Used for posting photos/videos, liking and sharing other content, selling products, raising awareness, creating boards, and empowering hashtags.
    - Misuse can be through bullying, harassment, fake profiles, face tuning, stalking, etc.
- Snapchat
    - Used to create videos/photos with the use of possible filters, showing talent, connecting with others through geotagging, and having “streaks”.
    - Misuses are revenge porn, taking screenshots of private messages, being always visible on the map, and disappearing messages.
- TikTok
    - Used for sharing talents, gaining knowledge, dance challenges, and creating content.
    - Misuses are location tracking, harming others for views/likes, dangerous challenges, disclosing abuse (trends), promoting violence, and peer pressure.
- Yubo
    - Used to meet new people, create a sense of community, live streams, sharing content.
    - Misuses include providing false information, harassment, bullying, demanding explicit photos and videos.

Chapter 3:

Safety Guides Android and iOS

In this chapter, we will be discussing Android and iOS Safety guides. Smartphones and other mobile devices are normal parts of our lives and it is essential to ensure these devices are secure and protected from cyber threats. Android and iOS are the two most popular operating systems for mobile devices. They do have built in security features but are still vulnerable to hacking, malware, and other cyber-attacks. This chapter will discuss the steps to secure your devices including setting strong passwords, enabling two-factor authentication, and keeping your device up-to-date. It is important to be aware of risks and take the necessary steps to protect yourself and your information.

Android Safety Guide

https://www.ceta.tech.cornell.edu/_files/ugd/9e6719_4db0b8e8154844bf84665ad3f04ec6c6.pdf

Android phones are phones that use an operating system developed by Google. Phone manufacturers include Samsung, LG, Motorola, Blackberry, Nokia, and more. If it is not an Apple phone, then most likely you will have an Android phone.

Shared Phone Plans

Please note, if you share a phone plan with someone else, they will have access to information about what you are doing on your phone. It will be easier to access that information especially if they are the account holder. They can view information about call logs, phone numbers of people who call/text you, and other potential information. The increased security guide below will not prevent information that is being accessed through a shared plan.

You could use your phone without a Google account, but most times users will have a registered account with Google/Gmail that is connected to the phone. It is important to know the Google accounts that are connected to your phone.

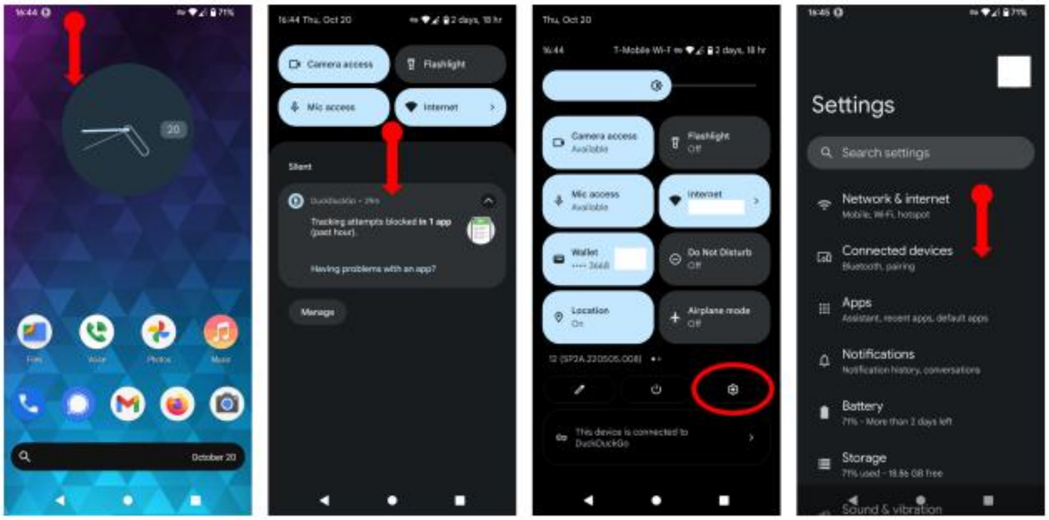
Google/Gmail Safety

Check the Google/Gmail Safety to understand whether an account is set up.

https://www.ceta.tech.cornell.edu/_files/ugd/9e6719_4db0b8e8154844bf84665ad3f04ec6c6.pdf#page=3&zoom=100,96,524

How to check which Google accounts are connected your Android.

First, go to the main Setting page.



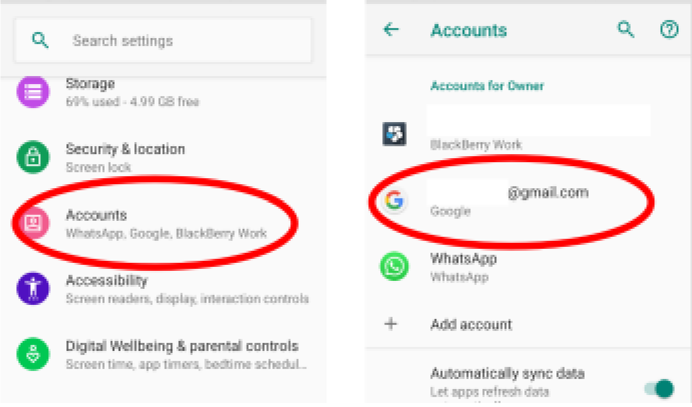
Option #1

1. Press on the notification bar at the top of the screen and pull down to find quick settings.
2. You may have to pull down again to view more settings.
3. You should look for the small gear icon and click on it to go to the main settings.

Option #2

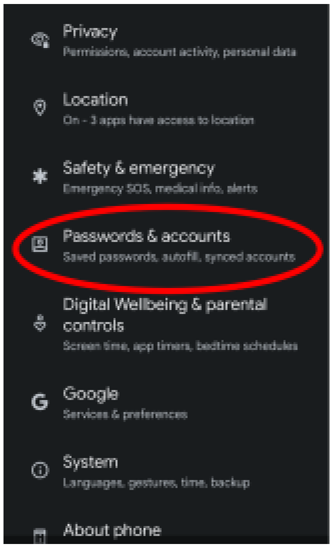
1. Go to **All Apps**, either tapping on it or swiping up.
2. Find **Settings** and click on it.

Android version 11:



On versions 11 or older on Android, scroll through the settings and click on **Accounts.** You will then see the list of Google/Gmail accounts connected to the phone.

Android version 12+:



Privacy
Permissions, account activity, personal data

Location
On - 3 apps have access to location

Safety & emergency
Emergency SOS, medical info, alerts

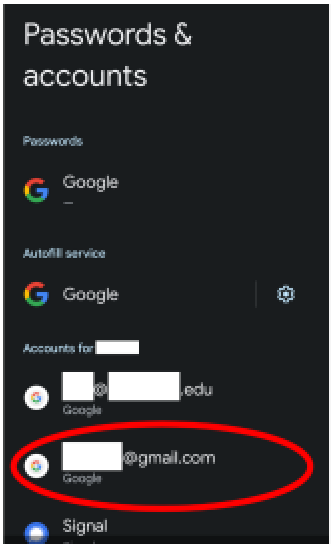
Passwords & accounts
Saved passwords, autofill, synced accounts

Digital Wellbeing & parental controls
Screen time, app timers, bedtime schedules

Google
Services & preferences

System
Languages, gestures, time, backup

About phone



Passwords & accounts

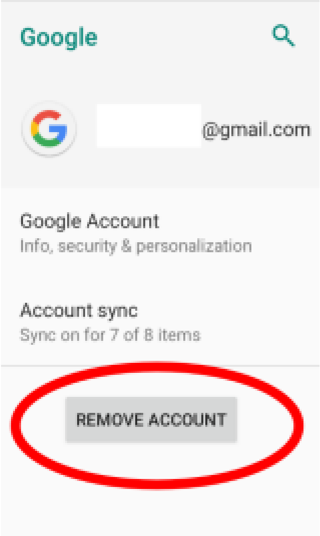
Passwords
Google

Autofill service
Google

Accounts for [redacted]
[redacted]@[redacted].edu
Google
[redacted]@gmail.com
Google
Signal

On version 12 or later, scroll through the settings and go to **Passwords & Accounts**. You will be able to view the list of accounts connected to the phone.

Remove any accounts that you do not recognize. Be aware the owner of those accounts may know when the account is removed. Have a plan in place when you remove the accounts.



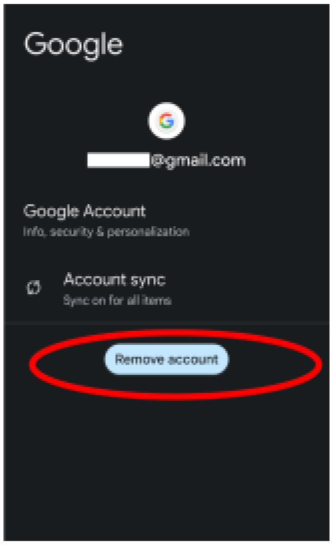
Google
[redacted]@gmail.com

Google Account
Info, security & personalization

Account sync
Sync on for 7 of 8 items

REMOVE ACCOUNT

Android 11



Google
[redacted]@gmail.com

Google Account
Info, security & personalization

Account sync
Sync on for all items

Remove account

Android 12+

To remove the accounts, click on a certain account and you will see an choice to remove it. Speak with a trained advocate who is helping you through this matter if you are concerned about any retaliation.

Find and Securing Backups.

What is a backup?

A backup application is software that will automatically save a copy of information from a device from another location. It will make a copy and store the data for cases when the original data is lost or damaged. Although there are benefits to a backup, it is important to know who has access to the backups. Any unauthorized users can use the backups to find information including text, emails, and photographs.

Many Android phones may have the backup application pre-installed. They may use Google One or different manufacturers like Samsung may use Samsung Cloud.

Backups may include information such as old text messages, photos, and videos even when it is deleted from your phone. It can be helpful if you need to get back old information but harmful if an abusive person can see the information you have deleted.

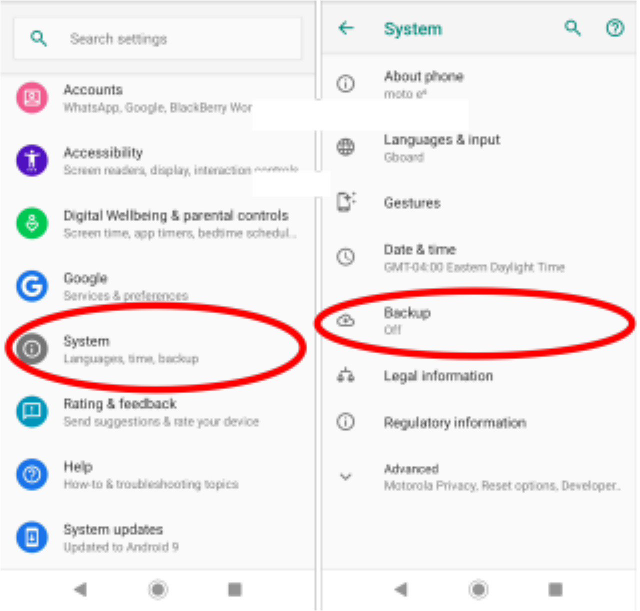
Google One:

official document
https://support.google.com/android/answer/2819582?hl=en#zippy=%2Cwhat-gets-backed-up

The following information can be backed up through Google One:

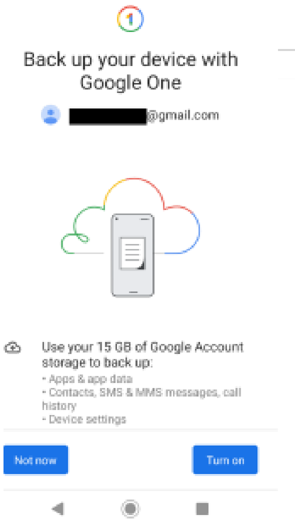
- Apps
- Call History
- Device Settings
- Contacts
- Calendar
- SMS (Short Message Service) messages. These are short messages up to 160 characters.
- Photos & Videos
- MMS (Multimedia Message Service) messages. These are text that includes files, photos, videos, emojis, or attached websites.

Check if your backup (Google One) is turned on.


Search settings
Accounts
WhatsApp, Google, BlackBerry Wor
Accessibility
Screen readers, display, interaction
Digital Wellbeing & parental controls
Screen time, app timers, bedtime schedul...
Google
Services & preferences
System
Languages, time, backup
Rating & feedback
Send suggestions & rate your device
Help
How-to & troubleshooting topics
System updates
Updated to Android 9
System
About phone
moto e⁶
Languages & input
Gboard
Gestures
Date & time
GMT-04:00 Eastern Daylight Time
Backup
Off
Legal information
Regulatory information
Advanced
Motorola Privacy, Reset options, Developer..

1. Go to **Settings.**
2. Scroll through and tap on **System.**
3. Find and click on **Backup.**

If the Backup (Google One) is turned off:



Back up your device with Google One

[redacted]@gmail.com

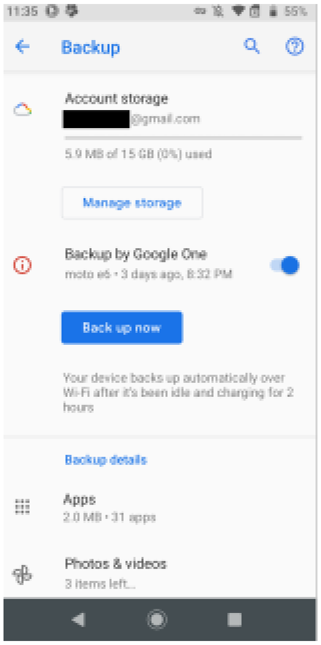
Use your 15 GB of Google Account storage to back up:
- Apps & app data
- Contacts, SMS & MMS messages, call history
- Device settings

If Google One is turned off then you may see the above screen and have the ability to turn it on. There are benefits to turning on the backup such as freeing up space on your phone and recovering information if your device might be damaged or lost.

It is important to ensure the Google account you are using to connect to Google One is an account that only belongs to you. Ensure no one else that has access to that account.

Confirm that you have secured your account. https://www.ceta.tech.cornell.edu/_files/ugd/9e6719_4db0b8e8154844bf84665ad3f04ec6c6.pdf#page=3&zoom=100,96,524

If the Backup (Google One) is turned on:



Account storage
[redacted]@gmail.com
5.9 MB of 15 GB (0%) used

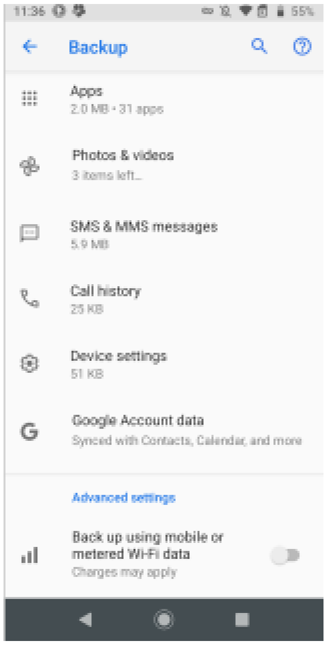
Backup by Google One
moto e6 • 3 days ago, 8:32 PM

Your device backs up automatically over Wi-Fi after it's been idle and charging for 2 hours

Backup details

Apps
2.0 MB • 31 apps

Photos & videos
3 items left...



Apps
2.0 MB • 31 apps

Photos & videos
3 items left...

SMS & MMS messages
5.9 MB

Call history
25 KB

Device settings
51 KB

Google Account data
Synced with Contacts, Calendar, and more

Advanced settings

Back up using mobile or metered Wi-Fi data
Charges may apply

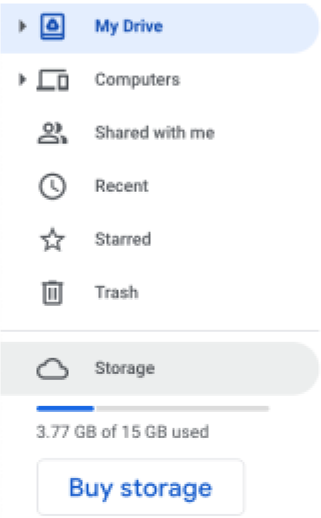
If the Backup is turned on, you have the option to turn it off by toggling the blue button.

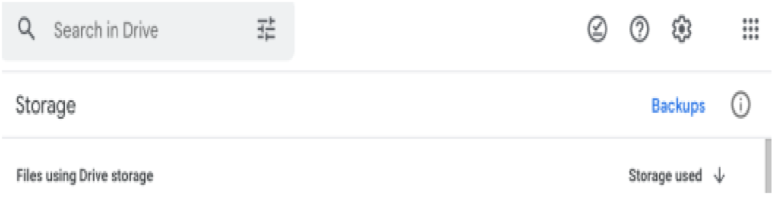
Warning: This may notify any users who have access to that account.

Please note, turning off the backup will not delete any data that has been backed-up before. You can delete backed up data by selecting and tapping delete.

Managing Backups Through Google Drive on a laptop or desktop.

Backups can be managed through Google Drive. Open a web browser and enter the following link, https://drive.google.com. Log in to your Google Account that is linked to your Android device. Use the email and password of the address you want to backup.





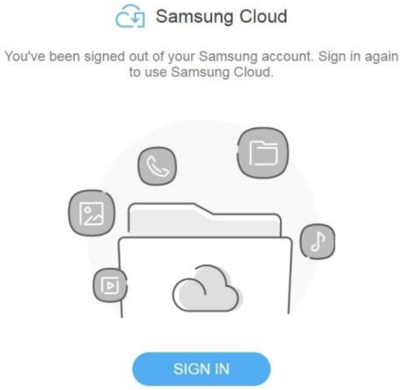
1. On the left side menu, click on **Settings.**
2. At the top right, click on **Backups**. You will see a list of backups for your device.

Ensure that you turn on extra security for Google Cloud Drive. https://www.ceta.tech.cornell.edu/_files/ugd/9e6719_4db0b8e8154844bf84665ad3f04ec6c6.pdf#page=3&zoom=100,96,524

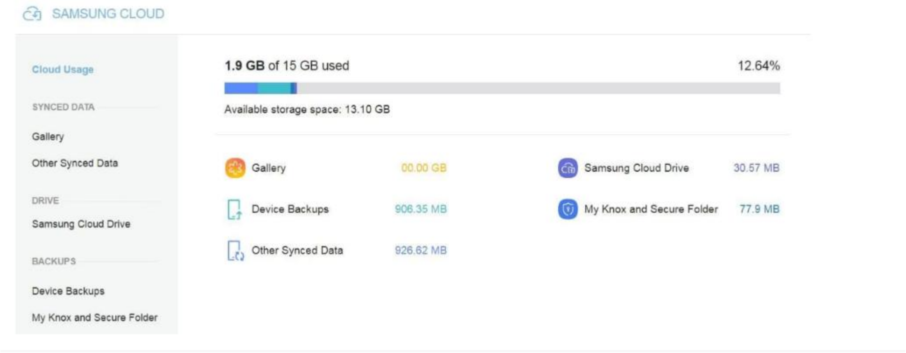
Other Android phones Backups:

Samsung Cloud: https://www.samsung.com/levant/support/mobile-devices/how-to-manage-samsung-cloud-on-the-browser/

1. Follow this link: https://support.samsungcloud.com
2. Log in using your Samsung account and password details for your Android device.
3. After logging in, the summary page will be shown. This will show you your cloud storage, synced data, Samsung Cloud Drive, and Backups.



You've been signed out of your Samsung account. Sign in again to use Samsung Cloud.



1.9 GB of 15 GB used 12.64%

Available storage space: 13.10 GB

Gallery	00.00 GB	Samsung Cloud Drive	30.57 MB
Device Backups	906.35 MB	My Knox and Secure Folder	77.9 MB
Other Synced Data	926.62 MB		

OnePlus: https://service.oneplus.com/uk/search/search-detail?id=op35

1. Connect your device and run the OnePlus Switch application.
2. Go to the **Backup and Restore**. There are two options, **New Backup, and Restore Backup.**
3. You can tap **New Backup** and choose what you would like to back up then click **Backup Now.**
4. You can also see your backed-up data.
   a. Go to **File Manager.**
   b. **Storage**
   c. **OPBackup**
   d. **MobileBackup.**
      i. You can see your backup data under mobile backup.

LG Android: https://www.lg.com/us/support/help-library/lg-android-backup-CT10000025-20150104708841

1. Go to **Settings.**
2. **General Tab.**
3. Scroll to find **Backup.**
4. **Backup & Restore then Backup.**
   a. You can then decide on the backup location by selecting internal storage or SD card (if installed). All your data will be stored here.
   b. You can then click on the items you want to backup and then click **Start.**
   c. To Restore backup, from the Backup list,
      i. Click on the items you wish to restore then click on the expand section.
      ii. Select the items you wish to restore then click **Next.**

Issues logging into your Google Account.

You may want to manage your Google Account but forgot your email or password. Use the following steps to try and recover your account. There are limited options if you are unsuccessful in recovering the account as there is no customer service for that issue. If this method does not work then try the following:

- Remove the account from your device if it is possible.
- Set up a new Google account that is safe to use with your device.
- Register your device with the new and safe Google account.

Following steps for recovering your account.
https://support.google.com/accounts/answer/7682439?hl=en

Forgotten Password.

1. Use the following steps to recover your Google Account. Click on the link https://accounts.google.com/signin/v2/recoveryidentifier?flowName=GlifWebSignIn&flowEntry=AccountRecovery
2. Answer the questions to you best ability.
3. If you are having trouble, then try these tips. **Please note you may not see the same questions described here.**
    - **a.** Use a familiar device and location.
        - **i.** The device you frequently sign in on.
        - **ii.** Use the same browser (Chrome or Safari).
        - **iii.** Try to sign in from a location you usually sign in.
    - **b.** Use exact passwords and answers to security questions.
        - **i.** Avoid typos and pay attention to lowercase/uppercase letters, and symbols.
    - **c.** If you are asked for the last password, you remember then use the most recent one you recall.
        - **i.** If you don't remember the last one then use a previous one that you do remember. The most recent is better.
        - **ii.** If you can't remember any passwords at all then take your best guess.
    - **d.** Answers to security questions.
        - **i.** If you do not remember the answer, take your best guess.
        - **ii.** If you know the answer but it did not work then try a different variation such as "NY" instead try "New York".
    - **e.** If you are asked to enter an email connected to your account.
        - **i.** A recovery email address will help you get back in by a security code sent to that email address.
        - **ii.** Use an alternate email address you can sign in on.
        - **iii.** The cntact email is where you get information about most Google Services you use.
    - **f.** Check your spam folder for any verification codes. Please note Google will never ask for your password or verification code through email, phone call, or message. Only enter your verification code through accounts.google.com.

Forgotten Email.

1. To find your username, follow the link https://support.google.com/accounts/answer/7682439?hl=en you will need to know:
    a. A phone number or recovery email address for the account.
    b. The full name that is on your account.
2. Follow the instructions to confirm your account.
3. You will find a list of usernames that matches your account.

Provide extra security measures for a hacked or compromised Google Account.

Step. 1: Sign into your Google Account.

Go to the recovery page: https://accounts.google.com/signin/v2/recoveryidentifier?flowName=GlifWebSignIn&flowEntry=AccountRecovery

Use this page if someone has:

- Changed your account information (password or recovery phone number).
- Someone deleted your account.
- You are not able to sign in for any other reasons.

Step 2. Review activity and help secure your hacked Google account.

Review activity.

1. Go to your Google account: https://www.google.com/account/about/?hl=en
2. On the left navigation panel, click on **Security.**
3. Find the "Recent security events" panel then select **Review security events.**
4. Check for any suspicious activities:
    a. **If you find anything that did not come from you**: Select, **No it wasn't me.** Then follow the steps on screen to secure your account.
    b. **If you did the activity**: Select **Yes.**

Review which devices use your account.

1. Go to your Google account: https://www.google.com/account/about/?hl=en
2. On the left navigation panel, press **Security.**
3. On the "Your Devices" panel, click on **Manage Devices.**
4. Check for devices that you do not recognize.

a. **If you find a device you do not recognize**, select "**Don't recognize a device?**". Follow the steps on the screen to help secure your account.
b. **If you recognize all devices but believe someone is still using your account see below for finding out if your account is hacked.**

Step 3. Take more security steps.

Turn on 2-Step Verification.

1. Open your Google Account and sign in: https://www.google.com/account/about/?hl=en
2. On the navigation panel, click on **Security.**
3. Under **Signing into Google**, click on **2-Step Verification > Get Started.**
4. Follow the on-screen steps.

Please note if you are using a work, school, another group account then these steps may not work. Contact your administrator for help.

Google recommends using Google prompts (https://support.google.com/accounts/answer/7026266), prompts are easier to sign in than enter a verification code. They can also help against SIM swaps and other phone number-based hacks.

Google prompts are push notifications you will receive on.

- Android phones that are signed into your Google Account.
- iPhones with the Smart Lock app (https://apps.apple.com/app/google-smart-lock/id1152066360), Gmail app, Google Photos app, YouTube app, Google app signed in to your account.

Based on the device and the location prompted on the screen, you can:

- Allow the sign-in if you had requested by pressing **Yes.**
- Block the sign-in if you did not request the login by pressing **No.**
- For added security, Google may ask for a PIN or another confirmation method.

Never give your verification codes to anyone!

Google Authentication.

If you do not have internet, you can download Google Authenticator for when you are out. https://support.google.com/accounts/answer/1066447

1. With your Android device, go to your Google Account. https://www.google.com/account/about/?hl=en
2. At the top, select **Security** tab.
3. Under **Signing into Google**, click on **2-Step Verification.** You may need to sign in.
4. Under "Authenticator app", tap **Set up.** Some devices may show **Get Started.**
5. Follow the steps on the screen.

Contact your back or local authorities.

Ensure someone else did not give your bank or government instructions to open an account or transfer money. This is important if you:

- Have any banking information saved in your account such as credit cards saved to Google Pay or Chrome.
- Have personal information like tax or passport information saved in your account. You may have personal information saved to Google Photos, Google Drive, or Gmail.
- If you think there might be someone using your identity or impersonating you, then contact your bank/local authorities.

Google Chrome Settings.

Add or change payment and address information you saved in Chrome.

1. On your computer, open Chrome.
2. At the top right, click **Profile, then Payment Methods, or addresses and more.**
3. Add, edit or, deleted info:
    a. **Add:** Next to **Payment methods** or **Addresses**, click **Add**. This will save information to Google Chrome on your device.
    b. **Edit:** On the right of the card or address, click **More** (three dots) then **Edit.**
        c. **Delete:** On the right of the card or address, click **More** (three dots) then **Remove.**

Please note if you add, edit, or delate an address and you have turned on sync. The changes will show up on your other devices.

Edit or delete in Google Pay.

1. Go to pay.google.com
2. On the left side, click **Payment methods.**
3. Find the card you want to edit or delete.

    a. **Edit:** Below the card, click **Edit.**
    b. **Delete:** Below the card, click **Remove.**

If you want to Chrome stop offering to save payment and contact information to Chrome see below.

1. On your computer, open Chrome.
2. At the top, under **People**, Click **Payment methods or Addresses and more.**
    a. To stop saving payment information, turn off **Save and fill payment methods.**
    b. To stop saving addresses and contact information, turn off **Save and fill addresses.**

Delete your saved Autofill form information.

1. Sign in on Chrome through your computer.
2. At the top right, click on **More** (three dots).
3. Click **More tools.**
4. Select **Clear browsing data.**
5. Choose a time range such as **Last hour** or **All time**.
6. Under "Advanced", choose **Autofill form data.**

Manage your saved passwords under Chrome.

Show, edit, delete, or export saved passwords.

1. Open Chrome on your computer or any other device.
    a. For computers:
        i. At the top right click on **Profile then Passwords.**
        ii. If you can't find passwords, at the top right of the screen click **More** (three dots), then **Settings** > **Autofill** > **Password Manager.**
    b. For devices, open Chrome.
        i. At the top right, tap **More** (three dots).
        ii. Click on **Settings** then **Password Manager**
2. **Show, delete, edit, or export a password:**
    a. **Show:** Tap the password you want to show then click **Show Password.**
    b. **Delete:** Tap the password you want to delete and at the top click **Delete.**
    c. **Edit:** Tap the password that you want to edit then edit the password following with **Done.**
    d. **Export:** Tap **More** (three dots) then **Export passwords.**

Start or stop chrome from saving passwords.

1. On your computer open Chrome.
2. At the top right, click on **Profile** then **Passwords.**
3. If you can't find the password icon, at the top right click **More** (three dots) then **Settings > Autofill > Password Manager.**
4. Turn **Offer to save passwords** on or off.

Sign into sites and apps automatically.

1. Open Chrome on your computer.
2. At the top right click on **Profile then Passwords.**
3. If you can't find the password icon, at the top right click **More** (three dots) then **Settings > Autofill > Password Manager.**
4. Turn **Auto sign-in** on or off.

Manage password change alerts.

This will notify you if a password or username you use gets comprised by a data leak on a third-party website or app. If you get this notification, it is recommended to immediately change your passwords.

To start or stop notifications:

1. Open chrome on your computer.
2. At the top right click on **More** (three dots) then **Settings.**
3. Click on **Privacy and security then Security.**
4. Click on **Standard protection.**
5. You will then have the option to turn on or off, **Warn you if passwords are exposed in a data breach.**

Only available if Save Browsing option is activated.

Remove harmful software.

Remove malware from your computer (Windows)

1. Open Chrome.
2. At the top right click **More** (three dots) then **Settings.**
3. Click **Reset and clean up then Clean up Computer.**
4. Click **Find.**
5. If you are asked to remove unwanted software, click **Remove**. It may ask you to reboot your computer after.

Manually remove malicious programs on (Mac).

1. Open Finder.
2. On the left, click **Applications.**
3. Look for programs that you do not recognize.
4. Right click on the name of the programs you do not want.
5. Click **Move to Trash.**
6. When you are finish then you can right-click on **Trash and Empty Trash.**
7. Be aware of the contents you are emptying from the Trash.

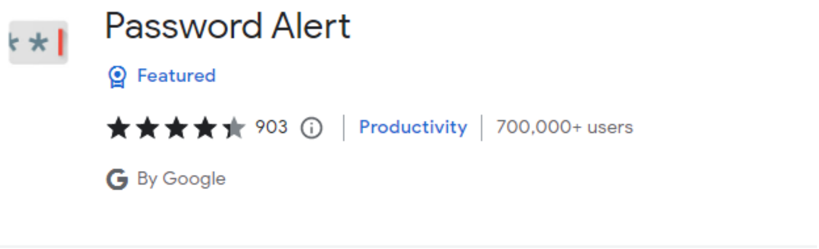
Install a more secure browser.

1. some internet browsers are less secure and have security weaknesses. Use more secure browsers such as Google Chrome, Firefox, Brave.

<u>Help prevent password theft with Password Alert.</u>

Password Alert will notify you when your Google password is used to sign in to non-Google sites.

To Turn on Password Alert



1. In Google Chrome, sign into your Google Account.
2. Go into the Chrome Store and download Password Alert
3. Follow the instructions on the screen.
4. Sign into your Google Account again to get started.

Please note this only works with the Google Chrome browser.

Turn off Password Alert

1. Sign into your Google Account through Google Chrome.
2. In the top right select **More** (three dots).
3. Select **More Tools.**
4. Select **Extensions.**
5. Find **Password Alert** on the list of extensions.

6. Select **Remove.**

Checking for Spyware/Stalkerware

These applications can be installed on a phone with the purpose of secretly collecting information and sharing it without the knowledge or permission of the phone's owner. It is difficult to for someone to install spyware on an updated Android phone unless they had physical access to the device.

Check your Android Software Version.

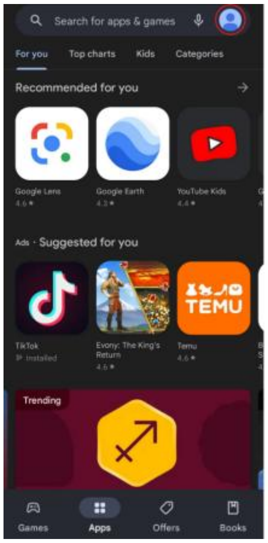
Most modern versions have protection against stalkerware and spyware.

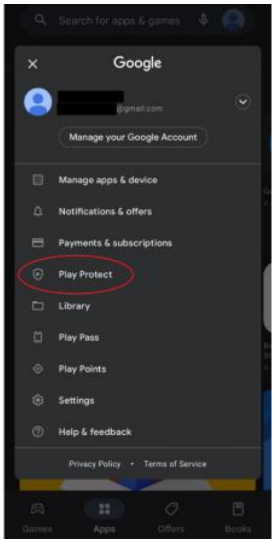
1. Open your phone's Settings app.
2. Tap About phone then Android version.
3. It will let you know if there is **security update** available. It is recommended to install any security updates that are new or outdated.

Google PlayProtect

Google Playprotect would likely have to be turned off for stalkerware and spyware to be installed. This may not be true for dual-use apps. To check:

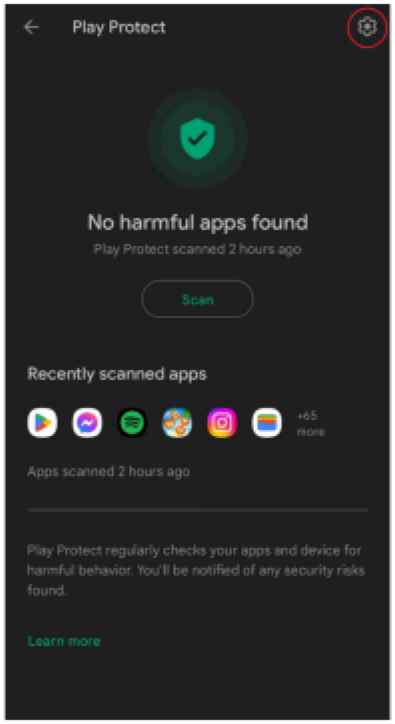
1. Open the Google Play app. This might be on the home screen, or you can find it by searching all applications.
2. Click on the Google Play icon
3. Click on the **Profile** icon in the top right hand corner.
4. Click on **PlayProtect** when the menu opens up. (see below).





PlayProtect will notify you if there are any harmful apps. You can then click on the app for more information and have the ability to uninstall the app. Be aware if an abusive person is monitoring your phone they may get a notification that it is uninstalled. If you have any concerns about your safety, reach out to a local domestic violence agency for a safety plan.

To ensure PlayProtect is working, click on the **Gear icon** in the top right corner. The first toggle ensures that it is scanning your applications on your phone. The second toggle is not necessary and does not affect the effectiveness of PlayProtect. That function also sends information to Google.



Play Protect

No harmful apps found

Play Protect scanned 2 hours ago

Scan

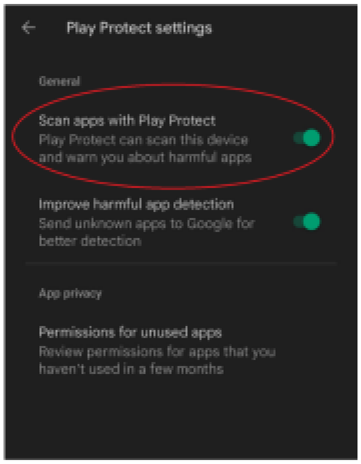
Recently scanned apps

+65 more

Apps scanned 2 hours ago

Play Protect regularly checks your apps and device for harmful behavior. You'll be notified of any security risks found.

Learn more



Play Protect settings

General

Scan apps with Play Protect
Play Protect can scan this device and warn you about harmful apps

Improve harmful app detection
Send unknown apps to Google for better detection

App privacy

Permissions for unused apps
Review permissions for apps that you haven't used in a few months

If your Android software is not up-to-date or you suspect someone had access to your device and installed something malicious on your phone. You can check for spyware manually. Spyware will need to ask for permission from the Android operating system to view sensitive information such as location, text messages, or keyboard access.

Checking Apps.

A common permission that spyware would request is the location of a device. Even if it is not spyware, it could be another app that the abusive person has access to. The app may inadvertently share your location.

To review apps with access to the location:

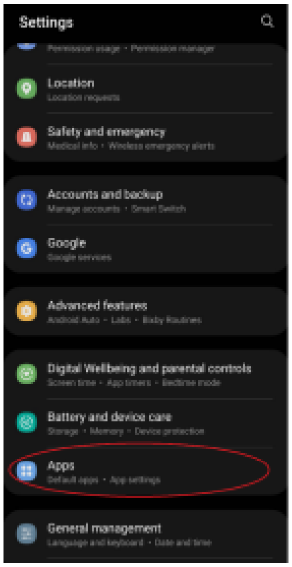
1. Settings app.
2. Go to **Location** then **App Location Permissions.**
3. You can then review all the apps with location on or off. Be careful when turning these features off as it can notify the abuser.

App Permissions.

You can also check the other applications' permissions which include **SMS, Location, Microphone,** and **Keyboard.** Disabling these permissions may be visible to the abuser.

1. Go to **Settings app.**
2. Scroll until you see **Apps.**

3. Tap on it then click on each **App.** then look for **Permissions.**



Settings

Permission usage · Permission manager

Location
Location requests

Safety and emergency
Medical info · Wireless emergency alerts

Accounts and backup
Manage accounts · Smart Switch

Google
Google services

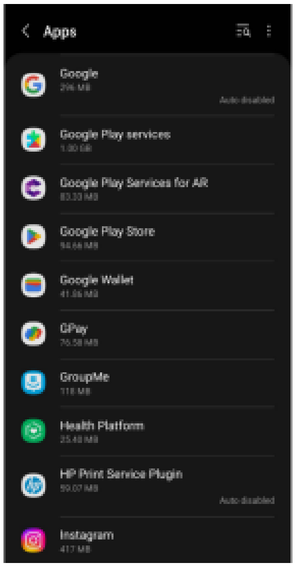
Advanced features
Android Auto · Labs · Bixby Routines

Digital Wellbeing and parental controls
Screen time · App timers · Bedtime mode

Battery and device care
Storage · Memory · Device protection

Apps
Default apps · App settings

General management
Language and keyboard · Date and time



Apps

Google
296 MB
Auto disabled

Google Play services
1.00 GB

Google Play Services for AR
83.33 MB

Google Play Store
94.66 MB

Google Wallet
41.86 MB

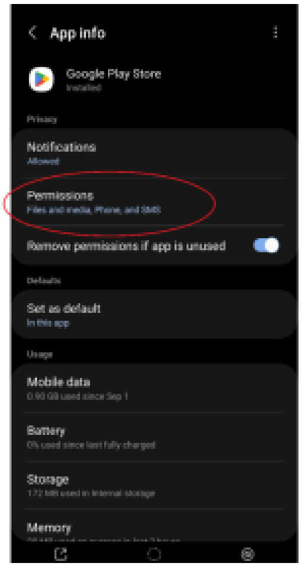
GPay
76.58 MB

GroupMe
118 MB

Health Platform
25.48 MB

HP Print Service Plugin
59.07 MB
Auto disabled

Instagram
417 MB



App info

Google Play Store
Installed

Privacy

Notifications
Allowed

Permissions
Files and media, Phone, and SMS

Remove permissions if app is unused

Defaults

Set as default
In this app

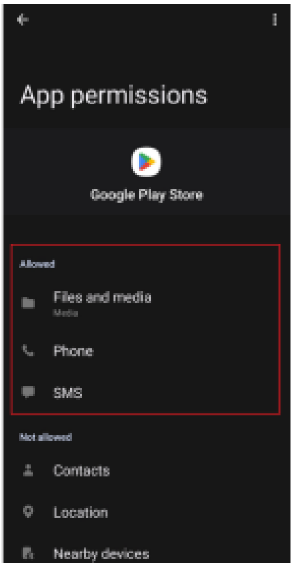
Usage

Mobile data
0.90 GB used since Sep 1

Battery
0% used since last fully charged

Storage
172 MB used in internal storage

Memory



App permissions

Google Play Store

Allowed

Files and media
Media

Phone

SMS

Not allowed

Contacts

Location

Nearby devices

Rooting Android Devices.

It is not common for an Android device to be rooted and abusers take easier methods to harm their targets. Rooting means taking full control over the device and limiting the software that is original to it. This will allow someone to install malicious software or change the functionality of an app. This requires more work and higher degree of technical knowledge. It can be difficult to know if your phone is rooted. If you are worried, then you could factory reset your phone to fix the issue.

Warning. A factory reset will delete all of your information on the phone. This will include contacts, text messages, and photos. This would be an extreme step to solve the issue. **"Keep in mind that if access to your phone is coming from an improperly configured app or Google account, factory resetting the phone will not solve the issue, but you will lose a lot of data".** It is encouraged to speak with an IT specialist if you want to factory reset your phone.

On most Android phones you can factory reset by:

1. Going to **Settings.**
2. **General and Back up.**
3. **Reset**
4. **Factory Data Reset** then **Reset Device.**

Internet/social media: When you are at home you can use "incognito" or "private" mode to do research. You could delete your history as well but sometimes you may forget. Going private mode will not save the history.

On an Android phone, open Chrome, click the three dots on the top right then tap the **New Incognito** tab**.** To close the incognito tab, click the square at the top right then Close incognito tabs.

iOS Safety Guide

https://www.ceta.tech.cornell.edu/_files/ugd/9e6719_088a4195809c40a89aec05adcd095a75.pdf

Shared Phone Plans

Please note, if you share a phone plan with someone else, they will have access to information about what you are doing on your phone. It will be easier to access that information especially if they are the account holder. They can view information about call logs, phone numbers of people who call/text you, and other potential information. The increase security guide below will not prevent information that is being accessed through a shared plan.

iOS Safety Check Feature

Apple has developed a feature called, Safety Check, and is available to certain iPhones and iPads that has a step-by-step guide to secure your device. If you have a device that has iOS version 16 or later and has 2-Factor Authentication enabled, then the Safety Check option is available.

1. Go to **Settings**
2. **Privacy and Security**
3. **Safety Check**

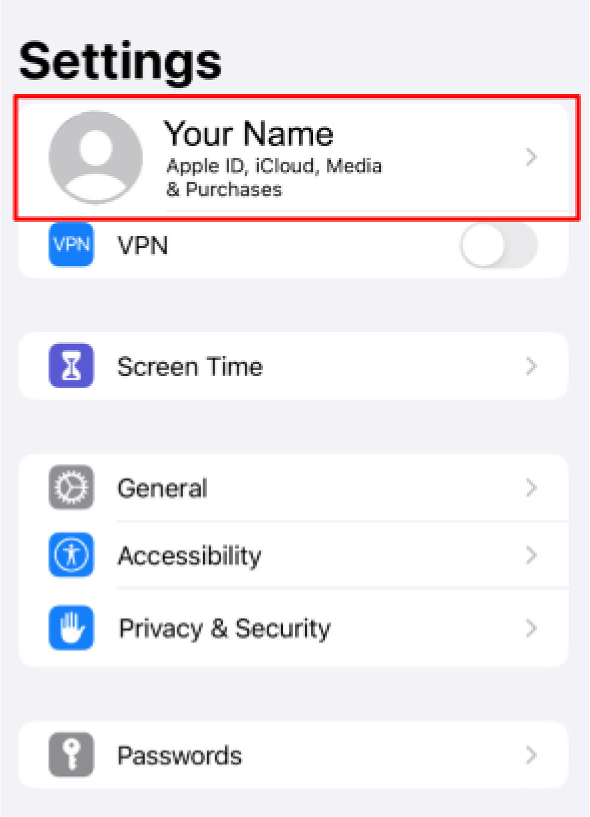
Be aware by using Safety Check, may alert an abuser that certain actions lock them out of your iCloud account or device. Examples could include:

- Changing your Apple ID password.
- Stopping location sharing from your device or apps.
- Change which devices are connected to your iCloud account.
- Changing your device password (someone having physical access to your phone).

Check iCloud Account Settings

Confirm the contact information on your account is yours. If it is not yours, it would allow your abuser to view information on your phone or gain access to the account, even after changing the password. This first step to securing your iCloud account.

1. On the home screen, open the **Settings.**
2. Check the top for the Apple ID and see if you recognize the name and image of the iCloud user.
3. You can click on the Apple ID section to see further details.



If you do not recognize the Apple ID, it means someone else is signed into your device from their iCloud account. Change the Apple ID email address, go to the web browser. https://support.apple.com/en-ca/HT202667

Editing Reachable Information

1. From the **Settings.**
2. Open the **Apple ID Menu** then tap on **Name, Phone Numbers, and Email.**

Check that the email and phone numbers in this section are yours. Apple can send account-related information to the email address attached. The email address that is listed as your Apple ID can be used to recover your account or password. It is recommended to check the security of your account and ensure there is a strong password associated with the account.

If there is an email address or phone number you do not recognize, change it or remove it from your account. Reminder, making any changes or removing the account can notify the user that they will be locked out.

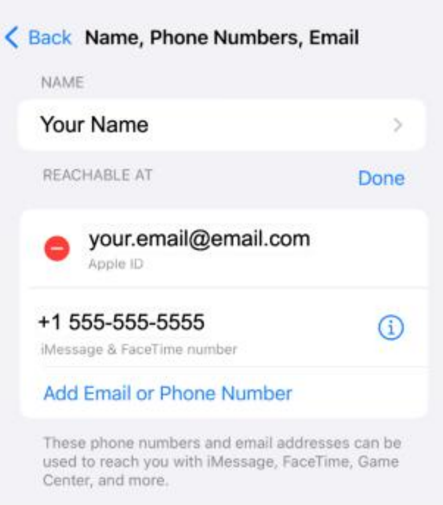
- To change an email address or phone number, click **Edit** which is to the right of **Reachable At**.
- To remove an email address or phone number, select the “minus” icon next to the email or phone number you want to remove.

Note you can not remove the email that is associated with your Apple ID

To change the email that is associated with the Apple ID by going to the following website.

https://support.apple.com/en-us/HT202667

1. Go to this website and log in https://appleid.apple.com/
2. In the Sign-in and Security section on the left side, choose **Apple ID.**
3. You can now enter the new email address that will be connected with your Apple ID.
4. You can also update your password in the same section by clicking on **Password.**



Name, Phone Numbers, Email

NAME

Your Name

REACHABLE AT

your.email@email.com
Apple ID

+1 555-555-5555
iMessage & FaceTime number

These phone numbers and email addresses can be used to reach you with iMessage, FaceTime, Game Center, and more.

When removing a phone number, you may have to sign out of Messages and FaceTime. If this step is required, follow the steps below:

1. Go to **Settings**, scroll to **Messages**, then select **Send & Receive.**
2. You can click on your phone number, then tap **Remove.**

3. Another way is to select your **Apple ID** at the bottom of the screen then select **Sign Out.**
4. Go to **Settings**, scroll to **FaceTime**, then select your **Apple ID** and click **Sign Out**

If you want to remove a phone number that is on a phone that you can not access, you must change your Apple ID password to delete it. Changing your Apple ID password will remove all phone numbers from your devices and will be known to anyone who had previous access.

When you remove a phone number from your iCloud account, information records (previous phone calls or messages) for the number that is removed will no longer appear on your devices. If you want to collect evidence, please keep this in mind.

To add a new phone number or email address, select "Add Email or Phone Number". You may need to have access to the phone number or email address for any verification codes.

Check which devices connected to iCloud.

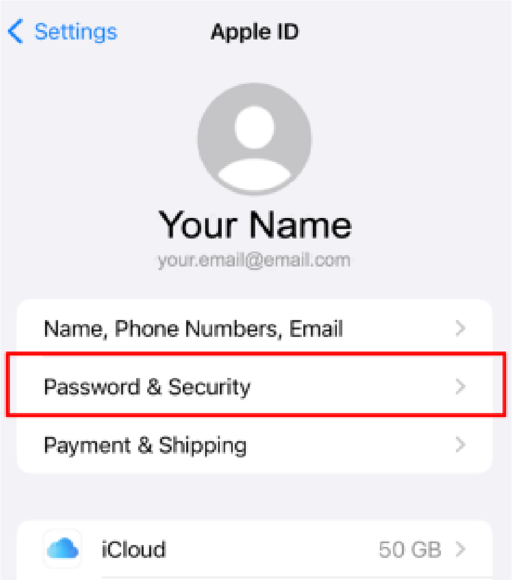
Devices are smartphones, tablets, laptops, or other electronic devices that can connect to the internet. Devices that were previously used to log in to your iCloud account, then Apple-trusted devices could gain access to your iCloud account and manage it.

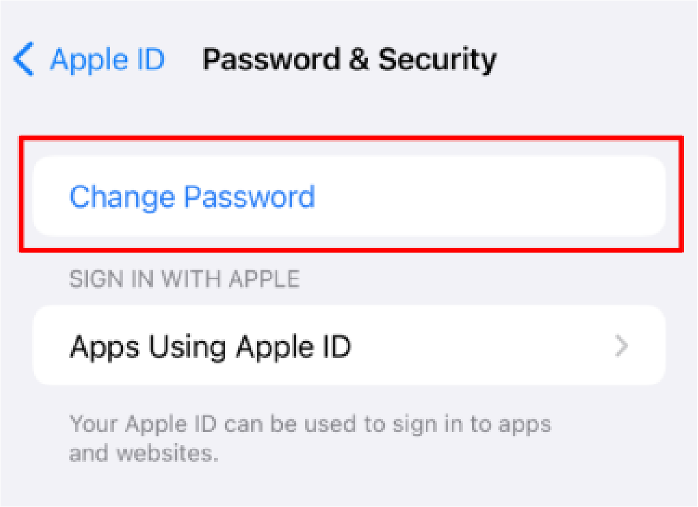
1. Go to your **Apple ID Menu** by going to **Settings** then selecting on **the Icon with your name and photo** (at the top of Settings).
2. Scroll down until you see the lists of trusted devices. These devices are where Apple ID is used to sign into iCloud.
3. If you do not recognize the device, you can click on the specific device then click on **"Remove from Account"** to disconnecting it from the iCloud account. *Please note this may notify the abuser*
4. Lastly, you can change your Apple ID password to keep someone else from logging into your account again.

Secure Access to your iCloud Account.

Changing your Apple ID password

1. Go to Settings > Apple ID Menu > Password and Security > Change Password.





Your Apple ID can be used to sign in to apps and websites.

Tips for creating a strong password.

- At least 8-12 characters long.
- Includes capital and lowercase letters.
- Includes random numbers.
- Includes some symbols such as,!, ?, @, and $
- Do not use words or numbers that could be easy for someone to guess, such as a child's name, pet's name, or birthday.

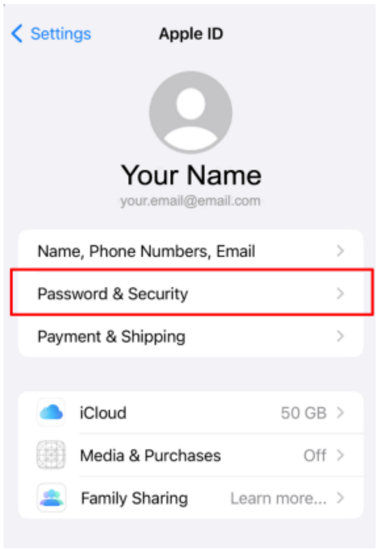
Enabling Two-Factor Authentication (2FA)

2FA provides another secure layer of protection to your account. Signing into your account will require you to enter your password then a two-factor authentication code which Apple will send through your phone number or one of your trusted devices. *Turning on 2FA will be visible to people who have access to your devices*

As Apple highly requires 2FA, sometimes you may not be able to turn it off after it is on depending on the device. You can always change the phone number or devices which the 2FA is sent to.

To check your 2FA settings

1. Go to Settings > Apple ID Menu > Password & Security

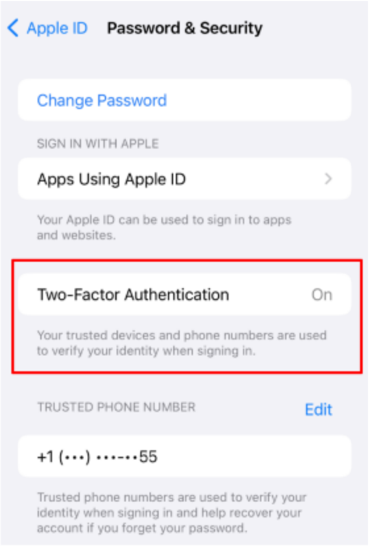


< Settings Apple ID

Your Name
your.email@email.com

Name, Phone Numbers, Email >
Password & Security >
Payment & Shipping >

iCloud 50 GB >
Media & Purchases Off >
Family Sharing Learn more... >



< Apple ID Password & Security

Change Password

SIGN IN WITH APPLE
Apps Using Apple ID >

Your Apple ID can be used to sign in to apps and websites.

Two-Factor Authentication On

Your trusted devices and phone numbers are used to verify your identity when signing in.

TRUSTED PHONE NUMBER Edit

+1 (•••) •••-••55

Trusted phone numbers are used to verify your identity when signing in and help recover your account if you forget your password.

You can view the 2FA section to see if it is on or not. If it is not on, then you will see an option to “Turn on Two-Factor Authentication”. Click to turn it on. Enter a phone number you want to receive verification codes when you sign in. You can either receive the code through a message or an automated phone call.

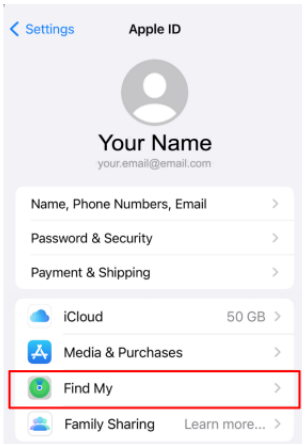
Checking if text messages are being forwarded.

If someone had physical access to your device, they could have set up text forwarding that will happen even after you have secured your Apple ID. This will affect SMS text messages (messages that show up in green unlike iMessage that show up in blue).

To check:

1. Go to **Settings** > **Messages**.
2. Go to **Send & Receive** then the devices under **Text Message Forwarding.**

Location Sharing Settings.



< Settings Apple ID

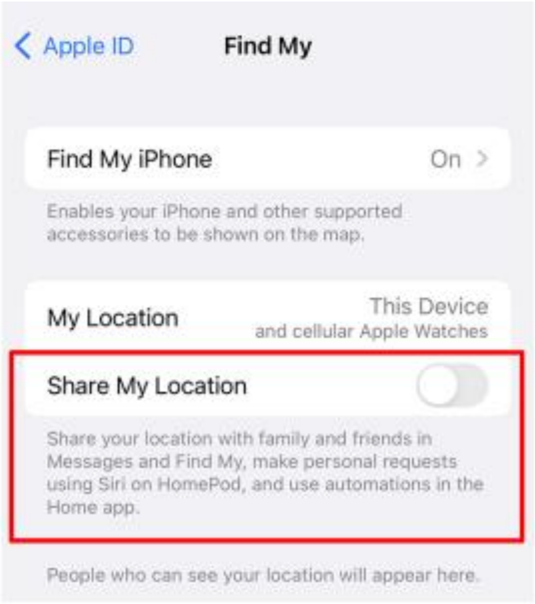
Your Name
your.email@email.com

Name, Phone Numbers, Email >
Password & Security >
Payment & Shipping >

iCloud 50 GB >
Media & Purchases >
Find My >
Family Sharing Learn more... >

Having Find My “on” is usually okay and sometimes is recommended to have on for your safety as long as your iCloud is secure. If you believe your iCloud is not secure, then this feature should be turned off. This feature allows you to track your own devices and allow others to track your location. To check:

1. Go to **Settings.**
2. Apple ID Menu (at the top of Settings)
3. Find My
4. In the **Find My** app, check the **Share my Location**. If it is **ON** then you are sharing your location with the people at the bottom of the screen. If it is **OFF** then your location will not be shared.



< Apple ID   Find My

Find My iPhone   On >

Enables your iPhone and other supported accessories to be shown on the map.

My Location   This Device and cellular Apple Watches

Share My Location   ○

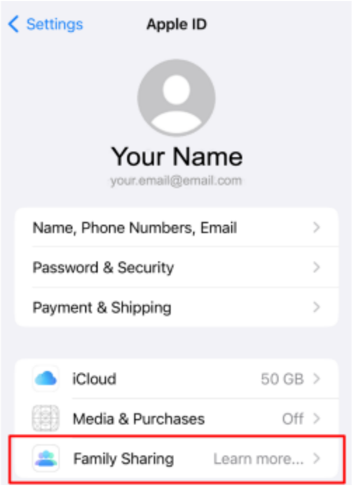
Share your location with family and friends in Messages and Find My, make personal requests using Siri on HomePod, and use automations in the Home app.

People who can see your location will appear here.

Check Family Sharing Settings.

The Family Sharing settings allow you to share Apple purchases, photos, iCloud storage, and your location with up to 5 other people. To check if this feature is turned on, go to:

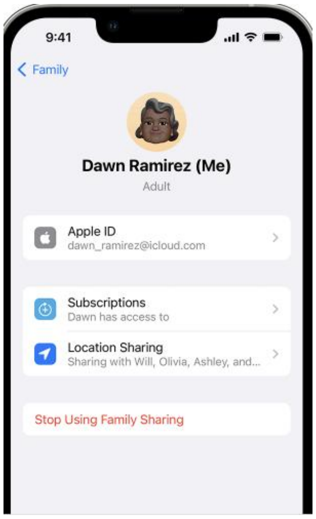
1. Settings > Apple ID Menu > Family Sharing



If the Family Sharing feature is turned off, then it will say **Learn more**. If it is turned on, click on it, then select **Shared Features** to check which information is being shared.

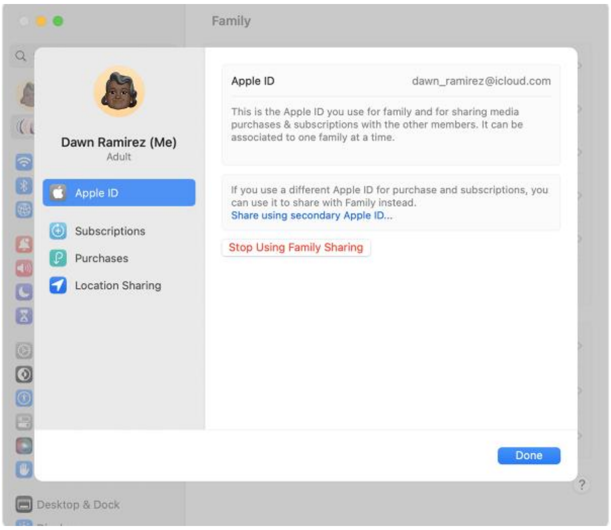
To remove yourself on your iPhone, iPad, or iPod Touch:

1. Go to **Settings**,
2. Tap **Family**, if you do not see **Family** then tap **your name**, then **Family Sharing**.
3. Tap **your name**.
4. Tap **stop** using **Family Sharing**.



On your Mac device:

1. Choose the **Apple menu** > **System Settings**.
2. Click **Family**.
3. Click **your name**.
4. Click **Stop Using Family Sharing**.



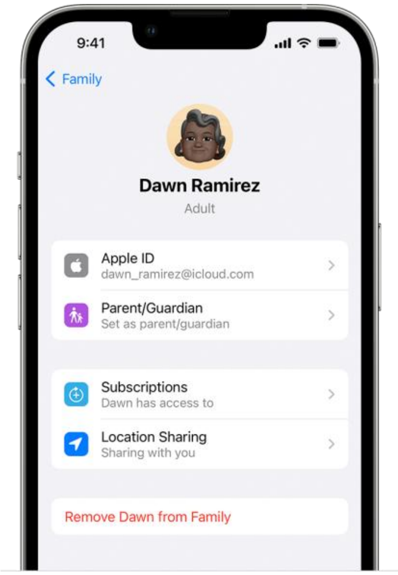
This is the Apple ID you use for family and for sharing media purchases & subscriptions with the other members. It can be associated to one family at a time.

If you use a different Apple ID for purchase and subscriptions, you can use it to share with Family instead. Share using secondary Apple ID...

Remove someone else from your family group.

On your iPhone, iPad, or iPod touch:

1. Go to **Settings**.
2. Tap **Family**. If you don't see the option for **Family,** then tap **your name**. After click on **Family Sharing.**
3. Tap the name of the **individual** that you want to **remove**.
4. Tap **Remove** [their name] from **Family**.

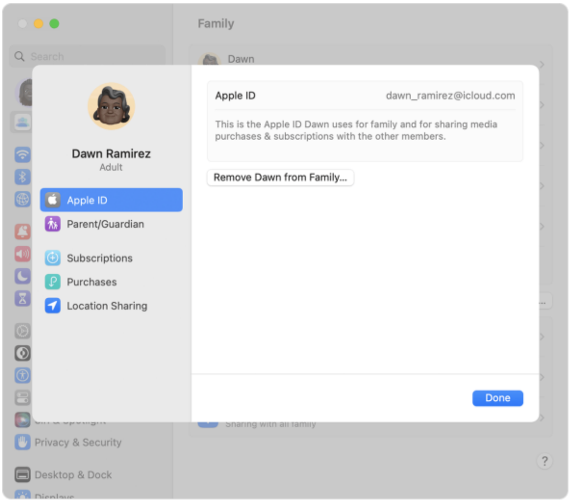


On your Mac device:

In macOS Ventura or later:

1. Click on the **Apple menu** > **System Settings**, then click **Family**.
2. Click the name of the **individual** that you want to **remove**.

3. Click **Remove** [their name] from **Family**.
4. Click Remove [your family member's name] to confirm



Apple ID dawn_ramirez@icloud.com

This is the Apple ID Dawn uses for family and for sharing media purchases & subscriptions with the other members.

Check for nearby AirTags.

iCloud can alert people of unwanted Apple AirTags that are moving with them. The AirTags are used to easily track things like your keys, wallet, backpack, etc. Individuals will use this device to abuse its powers and try to track people.

If an AirTag, Airpods, or any other Find My network accessories are separated from its owner are seen moving with you another time then you will be notified in one of two ways.

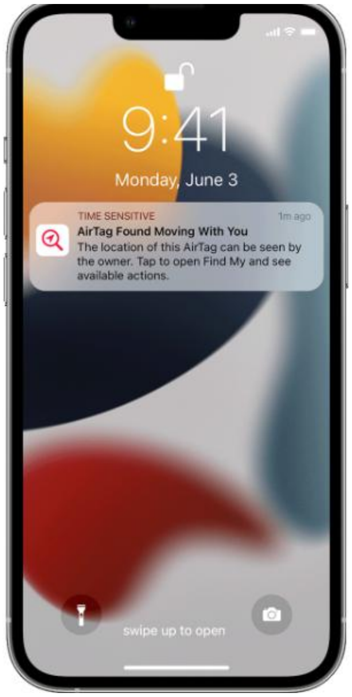
1. If you have an iPhone, iPad, or iPod, etc. **Find My** can send notifications to your Apple device. This feature is available on iOS or iPadOS 14.5 or later. To receive the alerts, ensure that these settings are set up.

- Click on **Settings** > **Privacy > Location Services** and turn **Location Services on**.
- Click on **Settings** > **Privacy** > **Location Services** > **System Services**. Turn **Find My iPhone on.**
- Click on **Settings** > **Privacy** > Location **Services** > **System Services**. Turn **Significant Locations** on to be notified when you arrive in specific locations including home.
- Click on **Settings** > **Bluetooth** and turn **Bluetooth on**.
- Using the **Find My app**, tap the **Me** tab, and turn **Tracking Notifications on**.
- Turn off **airplane mode**. You won't receive any notifications if your phone is on airplane mode.

2. Products including AirTags, AirPods Pro (2nd generation) charging case, or Find My network accessory will make a sound if it is not with its owner for a long time.

If you see an Alert

The AirTag that is separated from its owner is seen moving with you over time and your iPhone is awake. The AirTag make a sound to indicate that it has moved, this alert will be shown.

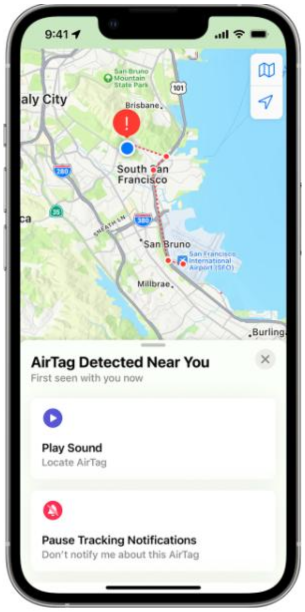


TIME SENSITIVE 1m ago

AirTag Found Moving With You

The location of this AirTag can be seen by the owner. Tap to open Find My and see available actions.

The Find My display will show where the AirTag has been observed with you. The red dots indicates where item was detected near your device. The dashed lines connecting the red dots indicates the connections where the device was near your device.



AirTag Detected Near You

First seen with you now

Play Sound
Locate AirTag

Pause Tracking Notifications
Don't notify me about this AirTag

If you do get an Alert, first check the Find My app if you're able to play a sound on the unknown accessory.

1. Tap the A**lert**.
2. Click on **Continue** and then tap **Play Sound**.
3. Listen for the sound. You can play it multiple times to find the item.

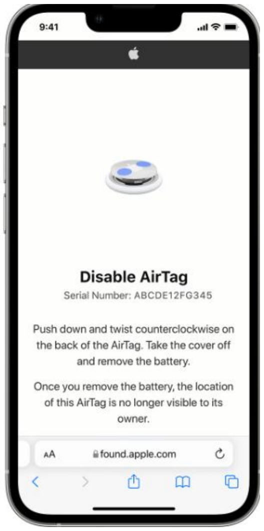
If the option to play a sound isn't available, the item might not be with you anymore. If it was with you overnight, its abuser might have changed it. Find My uses the identifier to identify that it's the same item moving with you. If the item is within range of the person who owns it then you also won't be able to play a sound.

Using an iPhone model with **Ultra Wideband**, you can also tap **Find Nearby** to use **Precision Finding** to help you locate the unknown AirTag.

1. Tap the **alert**.
2. Click on **Continue**, then click on **Find Nearby**.
3. Follow the **instructions** and move around until your iPhone connects to the unknown AirTag.
4. Your iPhone will indicate the distance and direction to the unknown AirTag. Use the information provided to get closer to the unknown AirTag until you find it.
    a. When the **AirTag** is within **Bluetooth** range of your **iPhone**, you can play a **sound** on the AirTag by tapping the **Play Sound** button.
    b. If your iPhone says that more light is required, tap the **Turn Flashlight On**.
5. When you're finish, click on the **Done** button.
   Get information about or disable an AirTag, Find My network accessory, or set of Airpods.

1. If you find the **AirTag**, you can hold the top of your **iPhone** or another **NFC-capable smartphone near** the **AirTag** until you receive a notification.
2. Tap the notification and it will open a website that provides more information about the AirTag. Take a screenshot of the information to keep as evidence.
3. To disable the **AirTag**, **AirPods**, or **Find My** network accessory and stop it from sharing its location. First, click on **Instructions** to **Disable** it, and follow the instructions shown.

4.



Disable AirTag

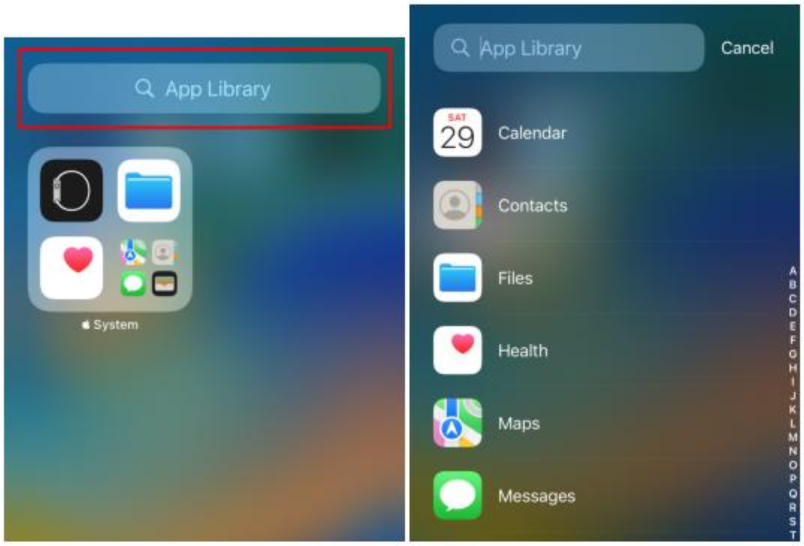
Serial Number: ABCDE12FG345

Push down and twist counterclockwise on the back of the AirTag. Take the cover off and remove the battery.

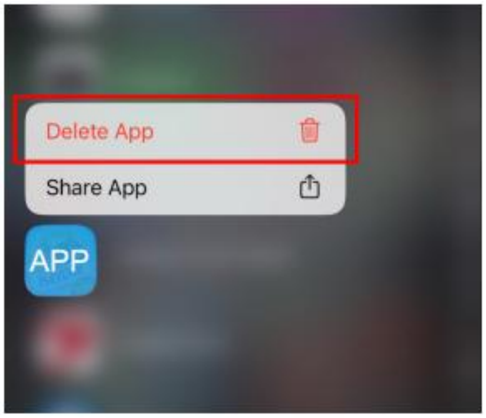
Once you remove the battery, the location of this AirTag is no longer visible to its owner.

Check the App Library for unrecognized apps.

Some apps might not be visible on the home screen of your device. This could have been done on purpose if someone had physical access to your device and they do not want you to see certain apps. To view all of your apps, depending on the version of your device, swipe all the way to the left while you are on your home screen. If that does not work then try swiping all the way to the right of your home screen.



Any apps that you do not recognize or feel like you may be in danger. You can remove the app by tapping and holding on the icon. When the menu shows up, select **Delete App.**



Be Careful Removing an app that an abuser installed may notify them.

Note, sometimes you can not delete Apple apps such as “**Contacts**”. It may remove it from your home screen, but it will still be available in the app library.

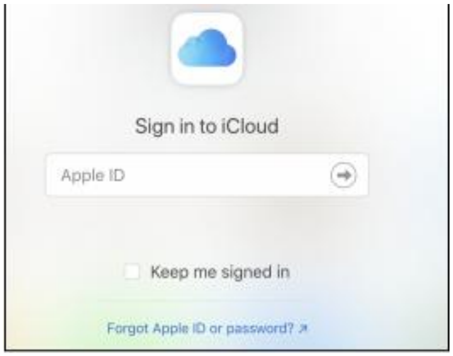
Manage iCloud Settings from a Browser.

Apple has a website that allows you to check various information with your Apple ID account through a web browser such as Google Chrome, Safari, Firefox, etc. These are the same settings as in the previous sections. This section is for those who:

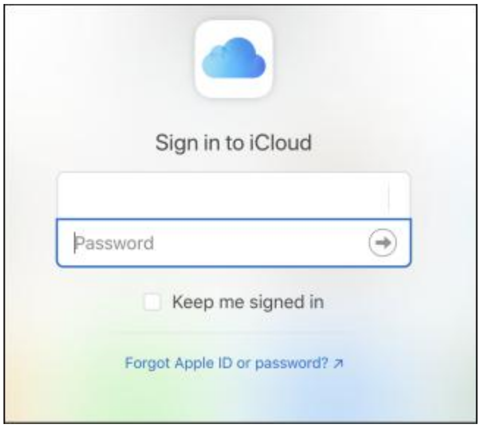
- Have an Apple laptop or Mac, but not an iPhone or iPad.
- Are more comfortable navigating settings on a laptop or iMac rather than their iPhone.
- Want to recover their iCloud account?
- Want to change the email associated with their Apple ID?

The following steps in this section may send prompts to the devices that are connected to your iCloud account, as well as to your email address associated with your Apple ID. *The prompts will send to your devices, information about your location, such as a map of the city or the town from where you have logged in*.

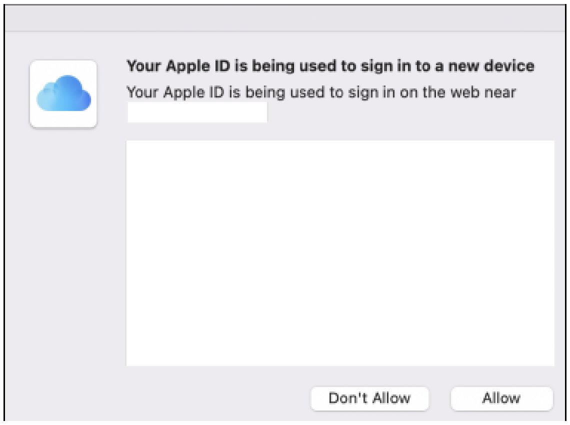
1. Go to https://www.icloud.com/



2. Enter your **Apple ID** (your iCloud address or the email associated with your Apple ID).
3. Enter your **password**.

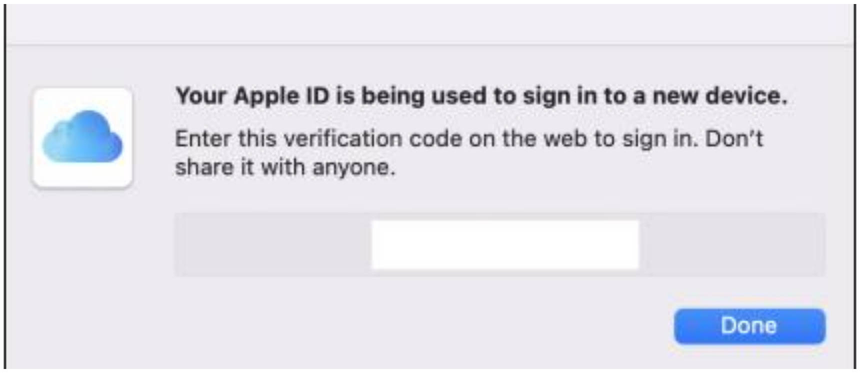


4. A prompt might be sent to your apple devices, check the prompt and follow the instructions.



Your Apple ID is being used to sign in to a new device

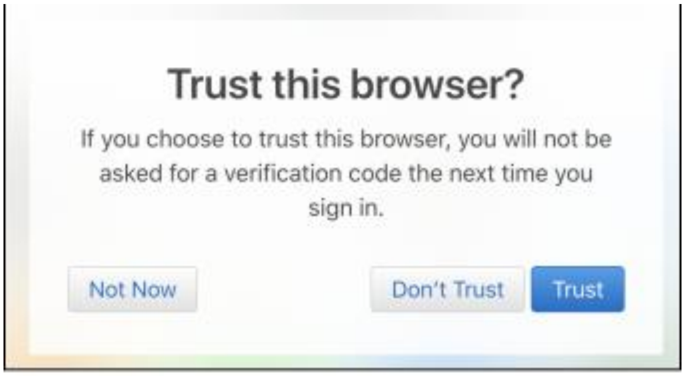
Your Apple ID is being used to sign in on the web near



Your Apple ID is being used to sign in to a new device.

Enter this verification code on the web to sign in. Don't share it with anyone.

5. After the prompt you may see this.

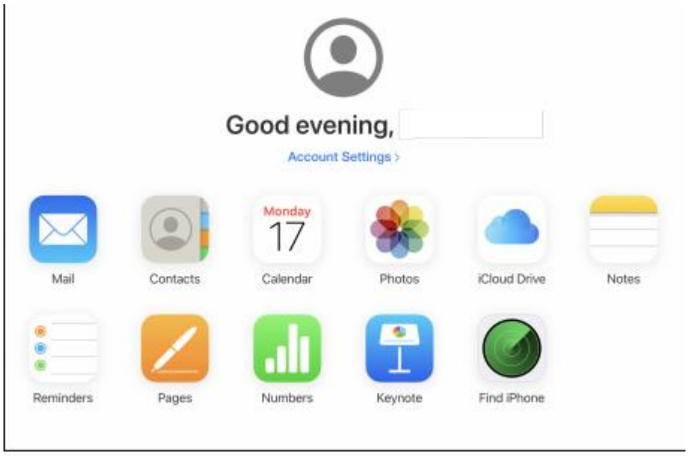


Trust this browser?

If you choose to trust this browser, you will not be asked for a verification code the next time you sign in.

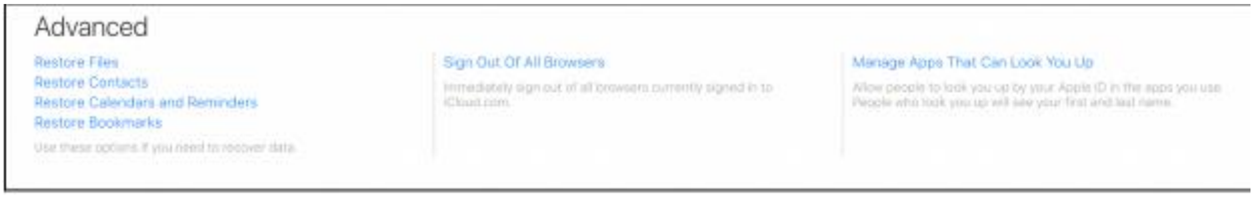
Choose the option that you think is best for you. **Only** select **Trust** if no one else has access to your device.

When you log in then you will see the following:



Click on **Account Settings**, depending on the version. It might be in the middle like the photo above or you have to click on the top right **Icon,** then **Account Settings.**

On this page, you will find resources including the restoration of files, contacts, calendars, reminders, and bookmarks. Also, there is an option that would allow you to sign out of all browsers where your iCloud/Apple ID account is.



Advanced

Restore Files
Restore Contacts
Restore Calendars and Reminders
Restore Bookmarks

Use these options if you need to recover data.

Sign Out Of All Browsers

Immediately sign out of all browsers currently signed in to iCloud.com.

Manage Apps That Can Look You Up

Allow people to look you up by your Apple ID in the apps you use. People who look you up will see your first and last name.

Stalkerware

These applications can be installed on a phone with the purpose of secretly collecting information and sharing it without the knowledge or permission of the phone's owner. It is difficult to for someone to install spyware on an updated Apple phone unless they had physical access to the device.

For iOS devices, stalkerware is usually downloaded directly from the app store and can be disguised as something innocent such as an unrecognized sports app or baby monitor. It is important to check for apps that you do not recognize.

It is extremely rare for spyware that is not in a form of an app. If you are concerned, apple has a feature called, **"Lockdown Mode"** for extreme cases. Enabling this feature will greatly limit the functionality of your device.

How Lockdown Mode protects your device

When the **Lockdown Mode** is turned on, some the features will function differently, including:

- **Messages** - Most message attachment would be blocked, other than certain images, video, and audio. Some features including links and previews will be unavailable.
- **Web browsing** - Certain web features would be blocked. This would cause some websites to load slowly or not operate correctly. In addition, web fonts might be shown properly, and images might be replaced with a "missing image" icon.
- **FaceTime** - Incoming FaceTime calls would be blocked. If you had previously called that person or contact, then they would not be blocked.
- **Apple services** - Invitations from Apple services including invitations to manage the home app are blocked.
- **Shared Albums** - Shared albums will be removed from the Photos app, and any new Shared Album invitations are blocked. You can still look at the shared albums on other devices that don't have Lockdown Mode enabled. When you turn off Lockdown Mode, you might need to turn Shared Albums on through your settings.
- **Device connections** – Your device would need to be unlocked and given explicit approval to connect devices including iPhone/iPad/Mac laptop.
- **Configuration profiles** – Under Lockdown Mode, you will not be able to configure any profiles and the device can't be enrolled in Mobile Device Management.

Phone calls and plain text messages continue to work while Lockdown Mode is enabled. Emergency features including SOS emergency calls, are not affected.

How to enable Lockdown Mode on iPhone or iPad.

1. Open the **Settings** app.
2. Tap **Privacy** & **Security**.
3. Under the **Security** setting, click on **Lockdown Mode**
4. Click on **Turn On Lockdown Mode**.
5. Tap on the **Turn On & Restart**, then enter your device password.

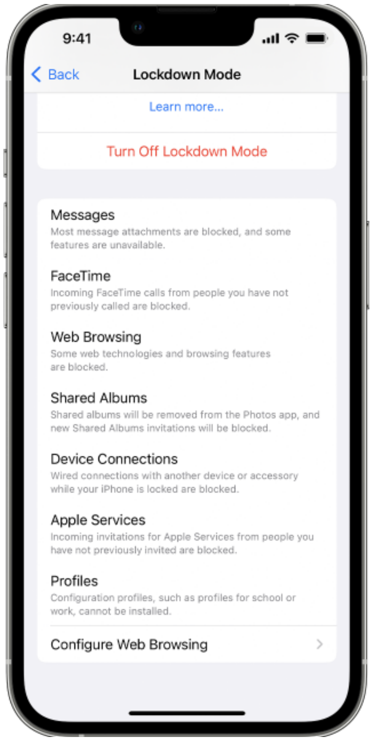
How to enable Lockdown Mode on Mac

1. Go to the **Apple menu**.
2. Click on **System Settings**.
3. From the sidebar, click **Privacy & Security.**
4. Scroll to find **Lockdown Mode**, then click **Turn On**.
5. You might need to enter the user password.
6. Click **Turn On & Restart.**

How to exclude apps or websites from Lockdown Mode

On iPhone or iPad

1. Open the Settings app.
2. Tap Privacy & Security.
3. Under Security, tap Lockdown Mode.
4. Tap Configure Web Browsing.



Messages
Most message attachments are blocked, and some features are unavailable.

FaceTime
Incoming FaceTime calls from people you have not previously called are blocked.

Web Browsing
Some web technologies and browsing features are blocked.

Shared Albums
Shared albums will be removed from the Photos app, and new Shared Albums invitations will be blocked.

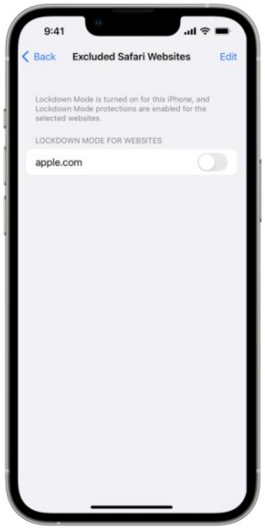
Device Connections
Wired connections with another device or accessory while your iPhone is locked are blocked.

Apple Services
Incoming invitations for Apple Services from people you have not previously invited are blocked.

Profiles
Configuration profiles, such as profiles for school or work, cannot be installed.

To exclude an app, turn that app off in the menu. Only apps that you have opened since enabling Lockdown Mode and will have limited functions that are on this list.

To edit your excluded websites, tap **Excluded Safari Websites**, then **Edit.**



Lockdown Mode is turned on for this iPhone, and Lockdown Mode protections are enabled for the selected websites.

LOCKDOWN MODE FOR WEBSITES

apple.com ○

On Mac

To edit your excluded websites:

1. From the menu bar in Safari, choose the Safari menu > Settings.
2. Click Websites.

3. In the sidebar, scroll down and click Lockdown Mode.
4. From the menu next to a configured website, turn Lockdown Mode on or off.

Jailbreak
Some stalkerware apps require the iOS device to be “jailbroken” in order to be downloaded. Jailbreaking will need physical access to your device since it is changing your iOS operating system. If there are apps “Cydia” or “Sileo” is installed on your device that could be an indicator that it is jailbroken. Best defense against jailbreak option is to keep your device up-to-date. **Internet/social media**: When you are at home you can use “incognito” or “private” mode to do research. You could delete your history as well but sometimes you may forget. Going private mode will not save the history.
***** In Google, you can go to the top right, the three tops (more options) and click **New Incognito Window**. Another way is pressing **Ctrl + Shift + n** or on a Mac press ⌘ + **Shift + n**

- For Apple users, In the Safari app, choose File then New Private Window.

1. On an Apple phone, Open Safari on your iPhone.
2. Tap the Tabs button ⧉.
3. Tap [number] Tabs or Start Page ⌄ to show the Tab Groups list.
4. Tap Private ✋, then tap Done

Chapter 4:

Email, Browsers, Social Media

In this chapter, we will be discussing email, internet browsers, and social media. These tools have become a part of our daily communication and social interactions. They can also pose a significant risk when misused/abused. Email is a common way to communicate and there are risks including phishing scams, malware, and other cyber-attacks. We will also discuss how to stay safe on social media and securing your accounts. It is important not to over share information online.

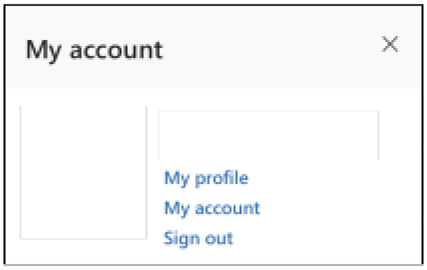
Hotmail

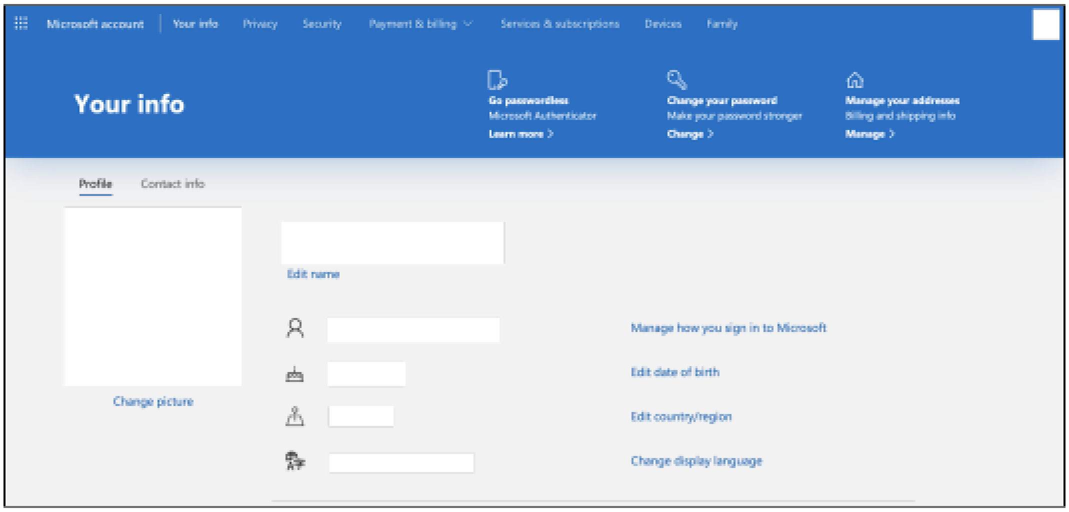
https://www.ceta.tech.cornell.edu/_files/ugd/64c5d9_e6cffbcf0b45424da387db3c4b73754a.pdf

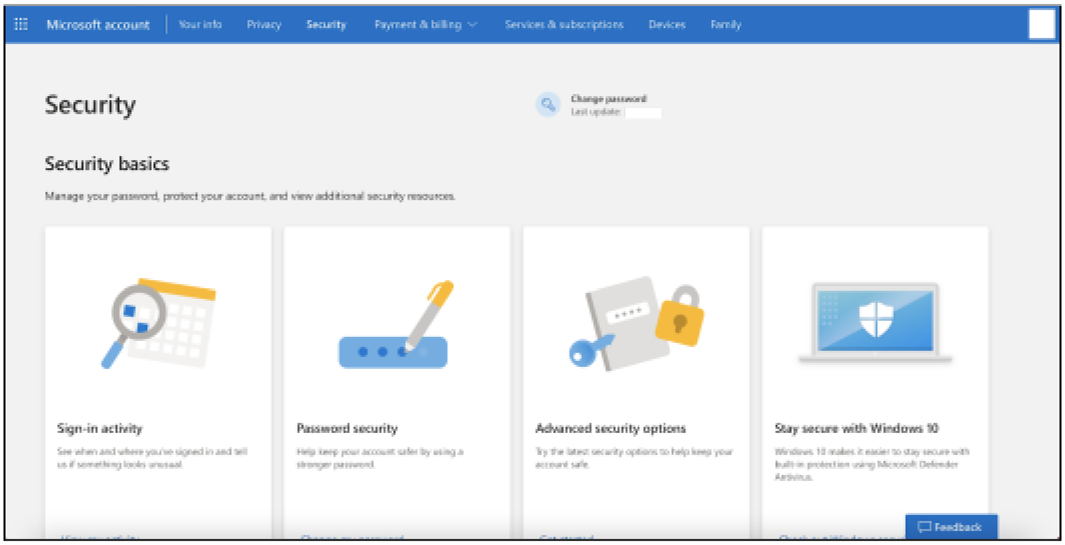
1. Log into your Hotmail account by going to www.hotmail.com
2. Click on the Sign in button at the top right corner.
3. Log into your account.

Steps to Check Device Logins.

1. Click on your **profile** picture located at the top right corner.
2. Click on **My Profile**.
3. At the top of the screen, click on **Security.**
4. Click on **Sign-in Activity** to show who recently signed into your account.
5. Check if you recognize all the locations logged in.
6. Note that approximate locations of logins are less reliable. If someone is using a **Virtual Private Network** (an app like ExpressVPN to hide their internet traffic), their location can be anywhere in the world.
7. If it looks unfamiliar, click on the specific location then select **Secure your Account** under **"Looks unfamiliar?"**.







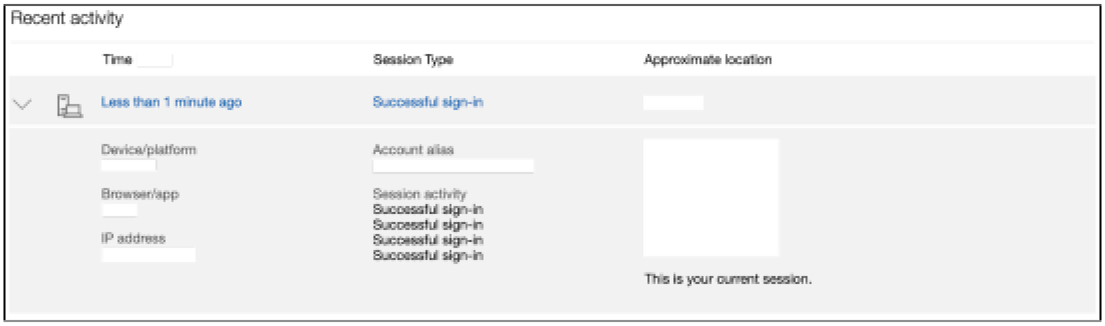
Manage your password, protect your account, and view additional security resources.

See when and where you've signed in and tell us if something looks unusual.

Help keep your account safer by using a stronger password.

Try the latest security options to help keep your account safe.

Windows 10 makes it easier to stay secure with built-in protection using Microsoft Defender Antivirus.



Recent activity

Time	Session Type	Approximate location
Less than 1 minute ago	Successful sign-in	

Device/platform

Browser/app

IP address

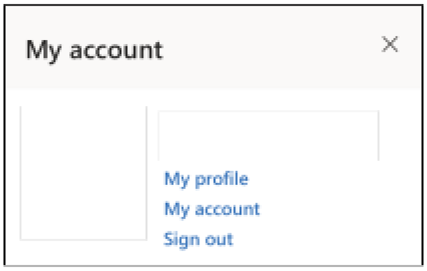
Account alias

Session activity
Successful sign-in
Successful sign-in
Successful sign-in
Successful sign-in

This is your current session.

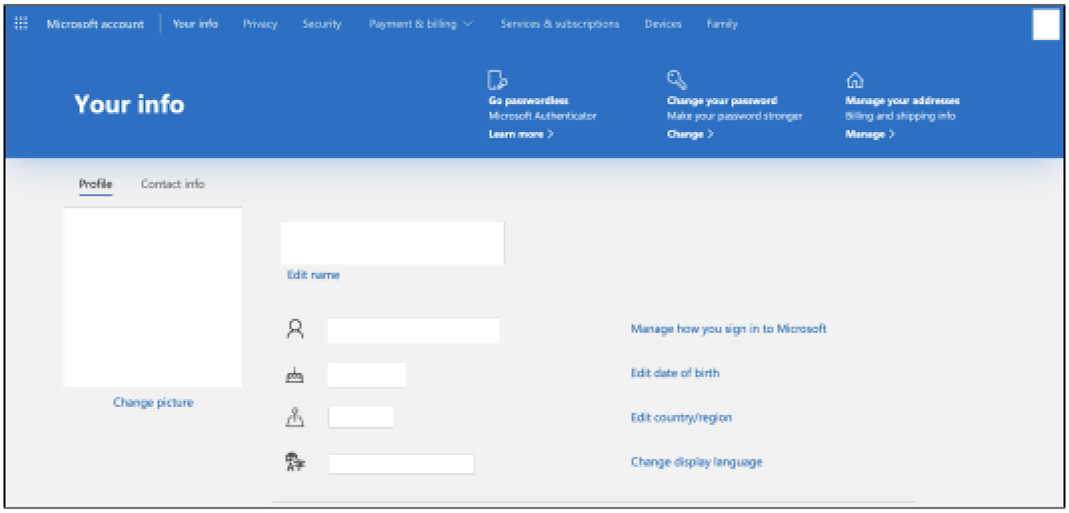
Steps to check Recovery Email and Phone Number

1. Click on your **profile** picture which is in top right corner.
2. Click on **My Profile**.
3. At the top of the screen, click on **Security.**
4. Click on **Advanced Security Options**.
5. Check that all the Information in the **Ways to prove who you are** is correct and recognizable.



My account

My profile
My account
Sign out



Your info

Go passwordless
Microsoft Authenticator
Learn more >

Change your password
Make your password stronger
Change >

Manage your addresses
Billing and shipping info
Manage >

Edit name

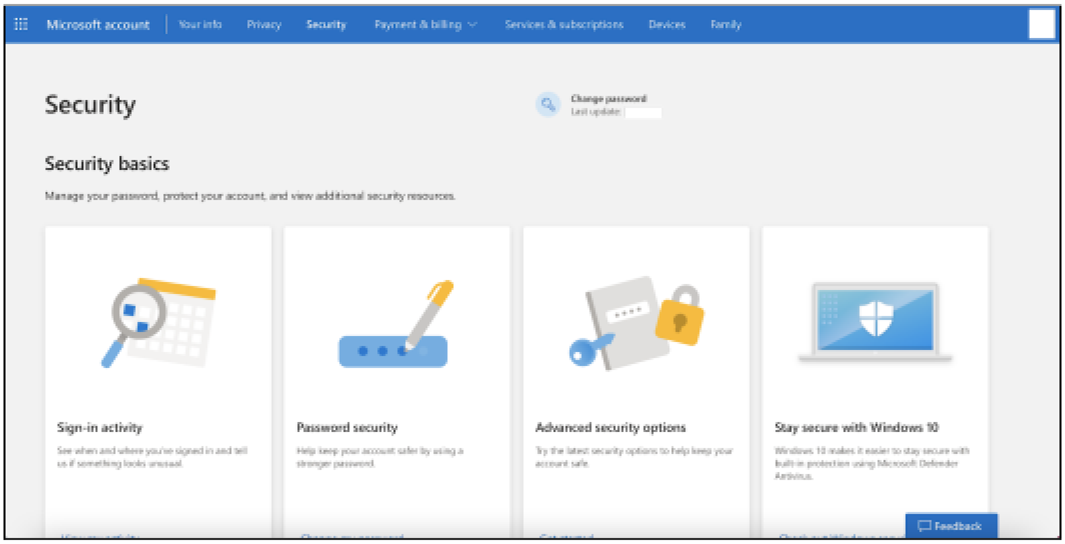
Change picture

Manage how you sign in to Microsoft

Edit date of birth

Edit country/region

Change display language



Security

Change password
Last update:

Security basics

Manage your password, protect your account, and view additional security resources.

Sign-in activity

See when and where you've signed in and tell us if something looks unusual.

Password security

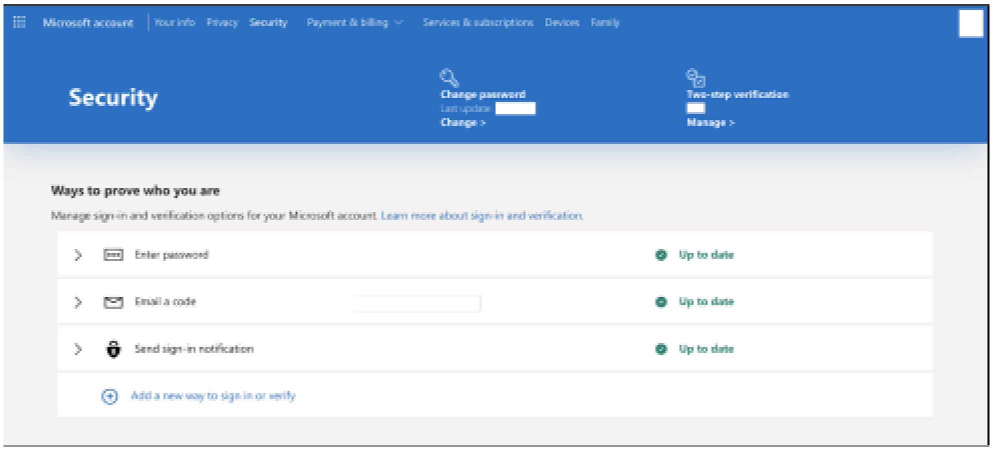
Help keep your account safer by using a stronger password.

Advanced security options

Try the latest security options to help keep your account safe.

Stay secure with Windows 10

Windows 10 makes it easier to stay secure with built-in protection using Microsoft Defender Antivirus.



Security

Change password
Last update:

Two-step verification

Ways to prove who you are

Manage sign-in and verification options for your Microsoft account. Learn more about sign-in and verification.

Enter password — Up to date

Email a code — Up to date

Send sign-in notification — Up to date

Turn on Two-Step Verification.

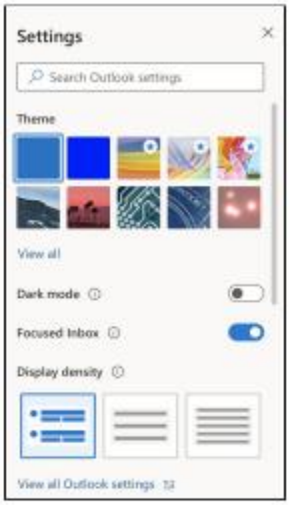
Two-Step Verification provides your account with an additional layer of security.

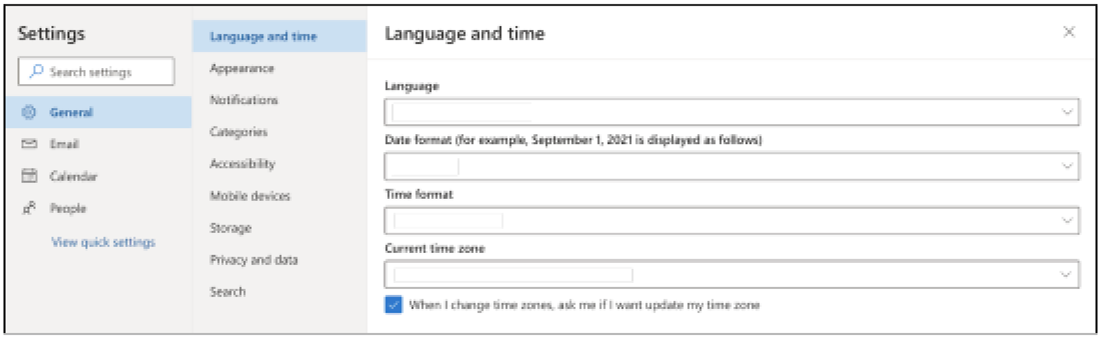
1. Click on your **profile** picture which is in the top right corner.
2. Click on **My Profile**.
3. At the top of the screen, click on **Security.**
4. Click on **Advanced Security Options**.
5. Go to the **Two-Step Verification** section and follow the instructions.

Please note Ensure to use a secured device or app that receives the two-step verification code.

Check the Mobile Devices

1. After logging into your Hotmail account. Click on the **Gear Icon** located at the top right corner.
2. The settings panel will appear then click on **View all Outlook Settings**
3. A Window will appear then click on **General** on the left side panel.
4. Then click on **Mobile Devices.**
5. If you do not recognize a device, select it then click on the **trash button.**





☑ When I change time zones, ask me if I want update my time zone

Check Rules

1. After logging into your Hotmail account. Click on the **Gear Icon** located at the top right corner.
2. The settings panel will appear then click on **View all Outlook Settings**
3. Click on **Email** on the left side panel.
4. Then click on **Rules**.
5. Make sure this list is empty or that you recognize the rules that appear on the list.

Yahoo

https://www.ceta.tech.cornell.edu/_files/ugd/c4e6d5_5229373f1ffa4ea0b8f804269f3038d1.pdf

Always practice safe online habits

- Protect yourself outside of Yahoo by avoiding malicious software. Do not install apps you are not familiar with.
- Sign out of public computers when you are finished using them.
- Do not fall for phishing scams. Do not open email links if you are unsure about them even if they are from friends.
- Check your login activity.
- Update your recovery methods.

Signs of a hacked account.

- You are not getting any emails.
- Your email address is sending spam emails to your contacts.
- You notice logins from unexpected locations on your recent activity page.
- Your account information or mail settings were changed without your knowledge.

Review your Yahoo Mail Settings.

Hackers may change these settings in your Yahoo Mail account to interrupt your inbox or get copies of the emails.

Check to see if any email filters were created.

Filters can save you time by organizing your incoming emails. The filters are prioritized from top-down and if there are 2 filters applied to one email then the top filter will be used. To change the position of the filters, select the filter you want then click the ↑ or ↓ down arrow keys.

To Create:

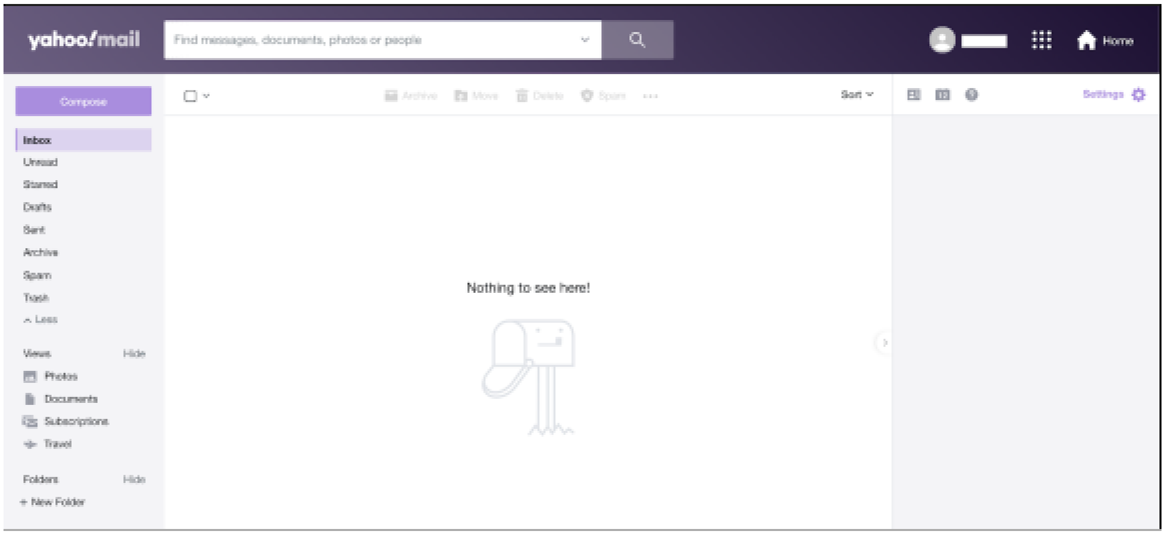
1. Click the **Settings icon** ⚙ | select **More Settings** ⋯.
2. Click **Filters**.
3. Click **Add new filters**.
4. Enter the filter name, set the filter rules, and choose or create a folder for the emails.
5. Click **Save** at the bottom.

To Delete:

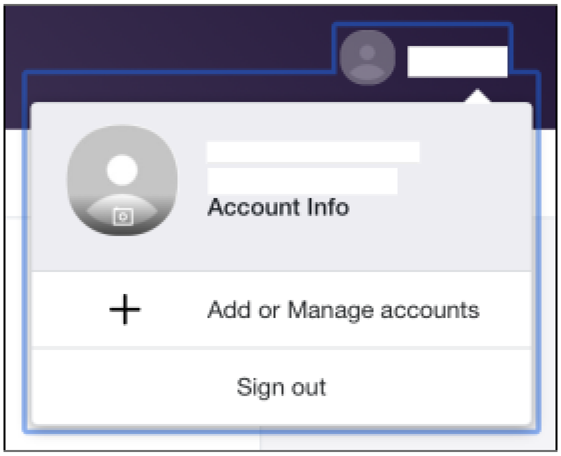
1. Click the **Settings icon** ⚙ | select **More Settings** •••.
2. Click **Filters**.
3. Select the filter you are interested in deleting.
4. Click the **Delete icon** 🗑 .

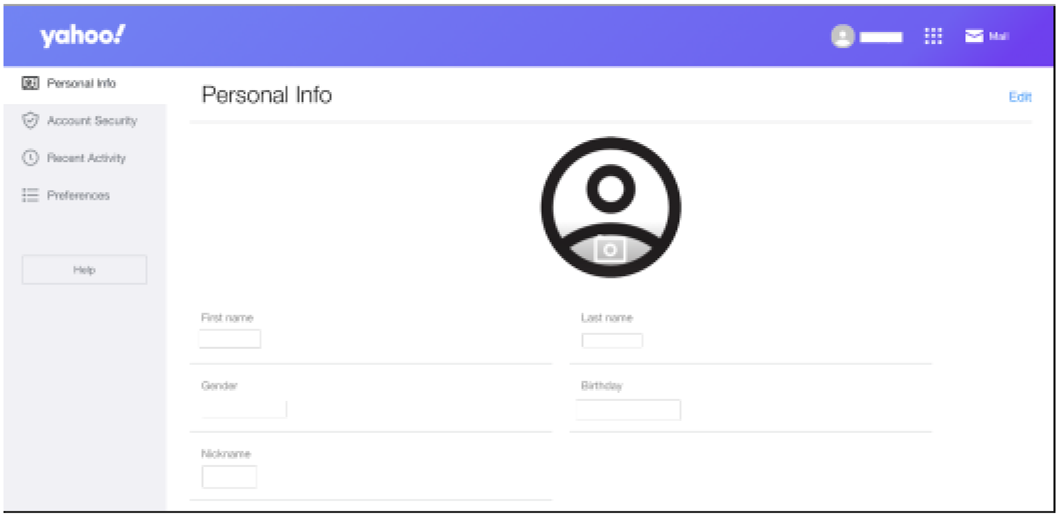
Steps to Check Device Logins on Yahoo

1. Log into Yahoo by going to a web browser, then https://login.yahoo.com/
2. Log into your account then at the top right corner click on **Account Info.**
3. Click on **Recent Activity** on the left side Menu.
4. Click on the specific device to see additional information.



Nothing to see here!





Personal Info

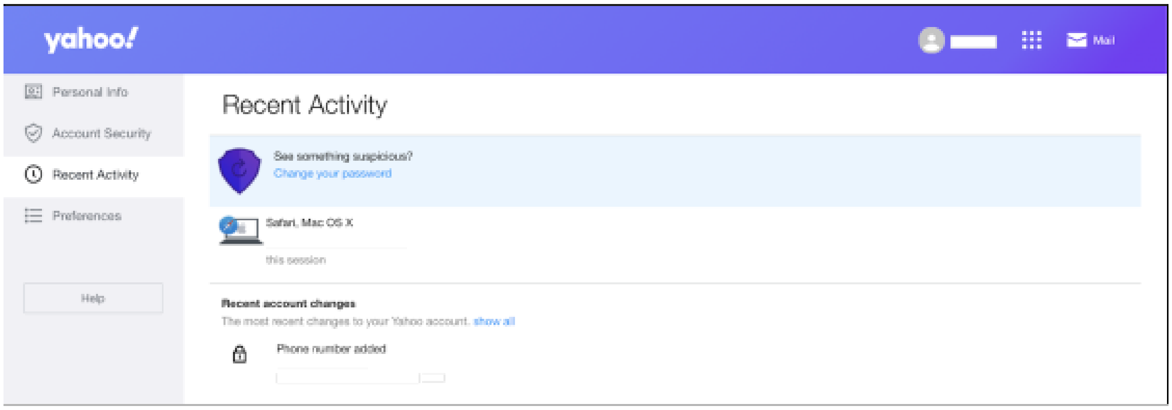
First name

Last name

Gender

Birthday

Nickname



Recent Activity

See something suspicious?
Change your password

Safari, Mac OS X
this session

Recent account changes
The most recent changes to your Yahoo account. show all

Phone number added

Recent activity

Unknown device

Sign in history for the last 30 days

Turn on 2-Step Verification

Two-Step Verification can provide an additional layer of protection for your account. You will need an additional code to access your account. This code could be sent to Yahoo app or your personal cellphone.

1. Sign into your **Account Security page.**
2. Next to **2-Step Verification**, select **Turn on 2SV.**
3. Click **Get Started**.
4. Select **Phone number** to use for the 2-step verification method.
5. Follow the instructions on screen to complete the process.

Add, change, or remove a recovery method.

It is important to keep a valid email or phone number linked to your account just in case you ever lose your password. Ensure that the email or phone number is familiar.

Add a mobile number or email address

From a web browser:

1. Sign into the Yahoo Account Security page.
2. Click **Add email** or **Add phone number**.
3. Enter your new recovery info.
4. Click **Add email** or **Add mobile number**.

5. Follow the instructions on screen then verify your new info.

To edit a mobile number or email address

From a web browser:

1. Sign into the Yahoo Account Security page.
2. Click **Edit** next to the verification option you want to change.
3. Click the **Edit icon** ✏ next to the recovery option you want to change.
4. Enter your new recovery info.
5. Click **Confirm**.
6. Follow the instructions on screen and verify your new info.

To delete a mobile number or email address

From a web browser:

1. Sign into the Yahoo Account Security page.
2. Click **Edit** next to the verification option you want to delete.
3. Click the **Edit icon** ✏ next to the recovery option you want to delete.
4. Click **Remove from my account**.
5. Follow the instructions on screen and to confirm the deletion.

Google Chrome

https://www.ceta.tech.cornell.edu/_files/ugd/c4e6d5_e02acdaedd744b329d04f9516611e15f.pdf

What are browser extensions?

First, web browsers are programs you use to access websites or search the internet. Examples of web browsers include Google Chrome, Safar, Firefox, and Microsoft Edge. A browser extension is a program you or someone can install on your web browser to extend the abilities of the program. Browser extensions can be beneficial with useful tools and sometimes fun tools. They are not all harmful. However, there are some extensions that can be harmful. It could let an abusive person track what you do online.

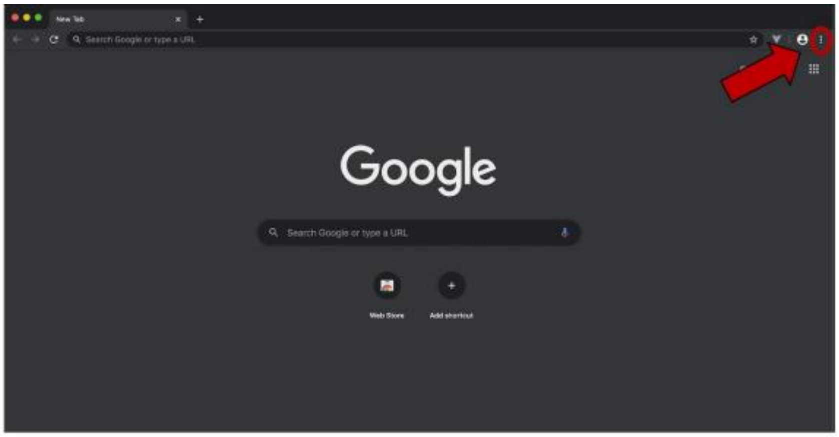
Google Chrome extensions can be downloaded from this website:

https://chrome.google.com/webstore/category/extensions?h1=en

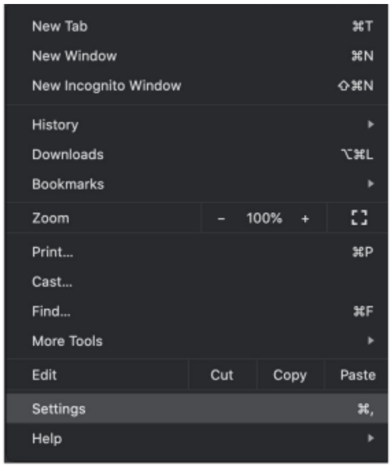
Note, before starting if you are worried that an abusive person has installed a Google Chrome extension. They may know when you disable/delete the extension. Please seek the appropriate organizations to help you through this process.

Checking for Installed Chrome Extensions

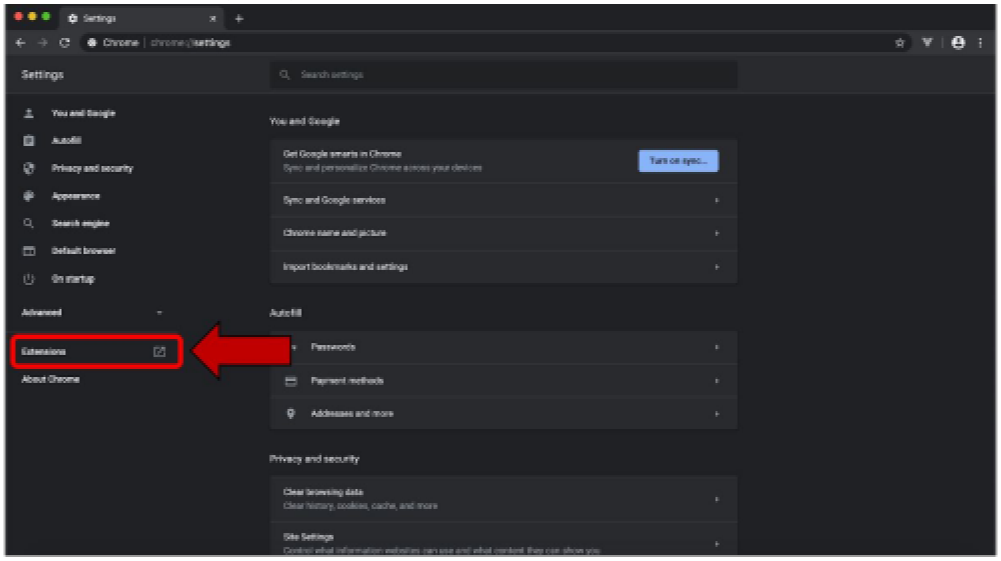
1. Open **Google Chrome**, click on this ic
2. Usually, the following screen will be shown. Located at the top right, click the 3 dots.



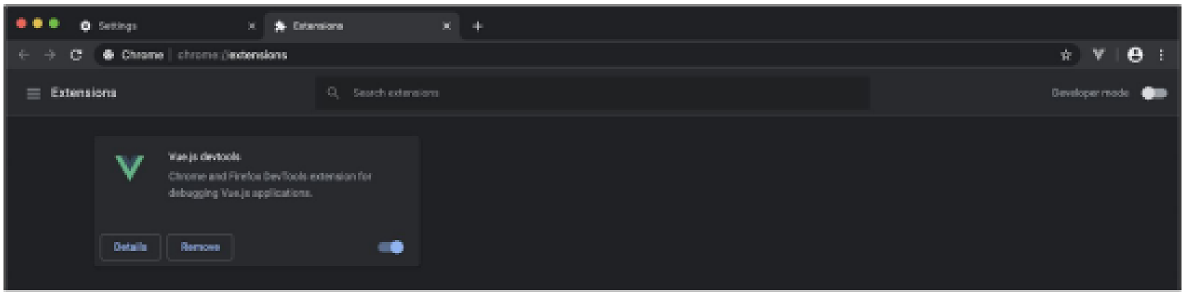
3. The customize and control menu will open, click on **Settings.**



4. On the following page, click on **Extensions** under the menu on the left.

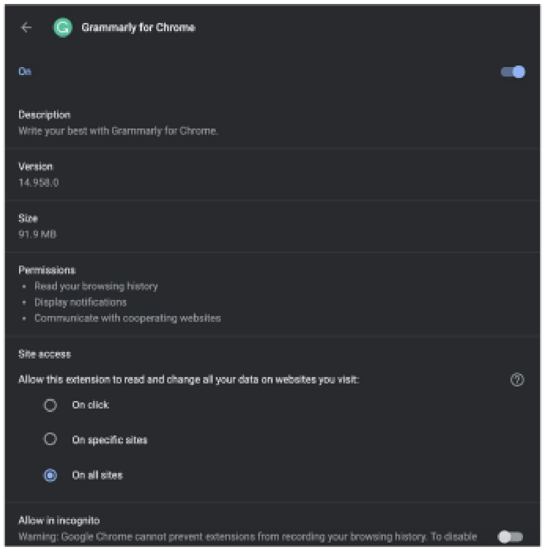


5. The following page will appear. All the Google Chrome extensions will be available here and you have the option to see more **Details, Remove or toggle the application on/off.**



Details

When you click on details, you will find more information about the extension. If you want to look up the extension to find more information about it then use a safe device (not the same one with the extension). There is a possibility of others complaining about the extension if it is a harmful extension in the past.



Grammarly for Chrome

On

Description
Write your best with Grammarly for Chrome.

Version
14.958.0

Size
91.9 MB

Permissions
- Read your browsing history
- Display notifications
- Communicate with cooperating websites

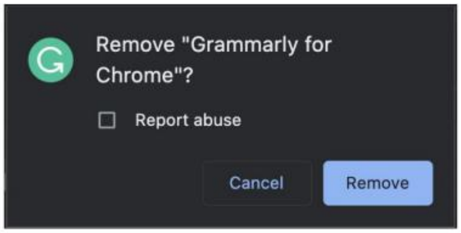
Site access
Allow this extension to read and change all your data on websites you visit:

○ On click
○ On specific sites
● On all sites

Allow in incognito
Warning: Google Chrome cannot prevent extensions from recording your browsing history. To disable

Remove

If you click remove, there will be a popup that will be your confirmation if you want to delete the extension. If you believe an abusive person is using this extension to receive information about you then be careful removing the application. If they stop receiving information, they would be aware you know about the extension. Contact the appropriate agencies to help guide you through this process.

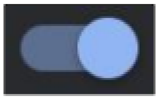
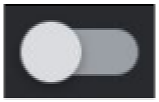


Remove "Grammarly for Chrome"?

□ Report abuse

Disable

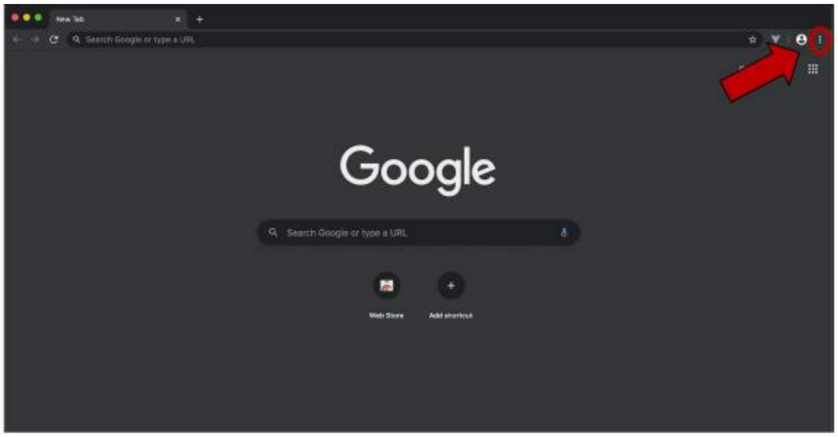
You can click on the toggle button to enable/disable the extension. If you believe an abusive person is using this extension to receive information about you then be careful removing the application. If they stop receiving information, they would be aware you know about the extension. Contact the appropriate agencies to help guide you through this process.

	… means that the extension is enabled
	… means that the extension is disabled

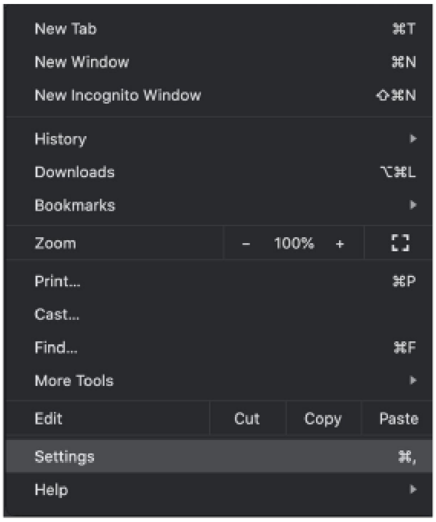
How to Update Google Chrome.

It is always recommended to have the most up-to-date version of Google Chrome. The new updates will provide more security and privacy features. They can also solve issues that may be harmful such as extensions that take advantage of you with an older version of Chrome.

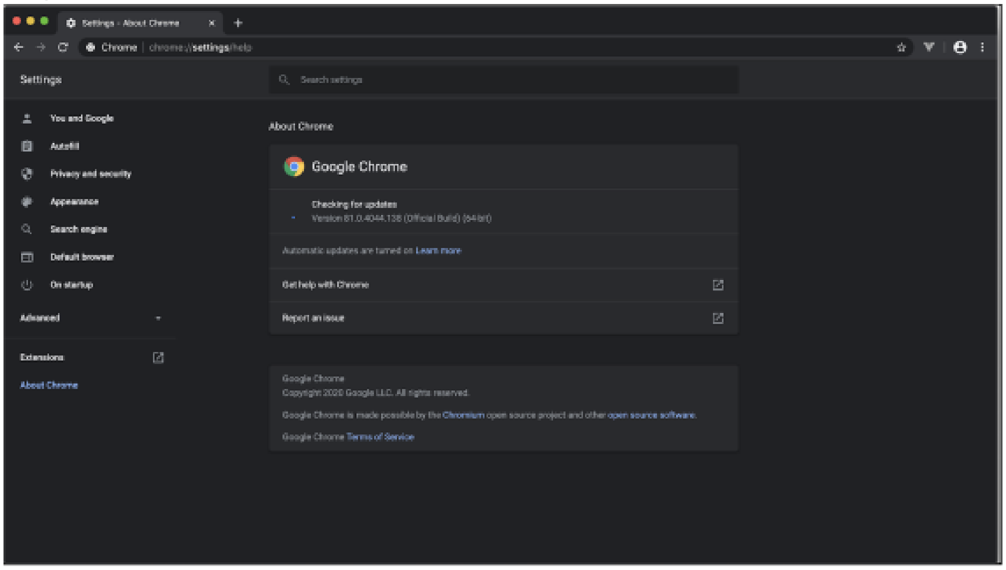
1. Open **Google Chrome**, Click on this icon.
2. Usually, the following screen will be shown. Located at the top right, click on the 3 dots.



3. The customize and control menu will open, click on **Settings.**



4. The menu on the left within **Settings**, click on **About Chrome.** The following page will appear.



About Chrome

Google Chrome

Checking for updates
Version 81.0.4044.138 (Official Build) (64-bit)

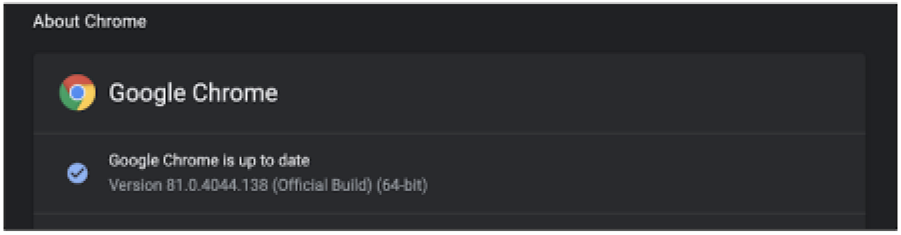
Automatic updates are turned on Learn more

Google Chrome
Copyright 2020 Google LLC. All rights reserved.

Google Chrome is made possible by the Chromium open source project and other open source software.

Google Chrome Terms of Service

5. Chrome will automatically check if there are any available updates. It will automatically update or provide a button for you to click to start updating. After the update is finished then it shows look like the following:



About Chrome

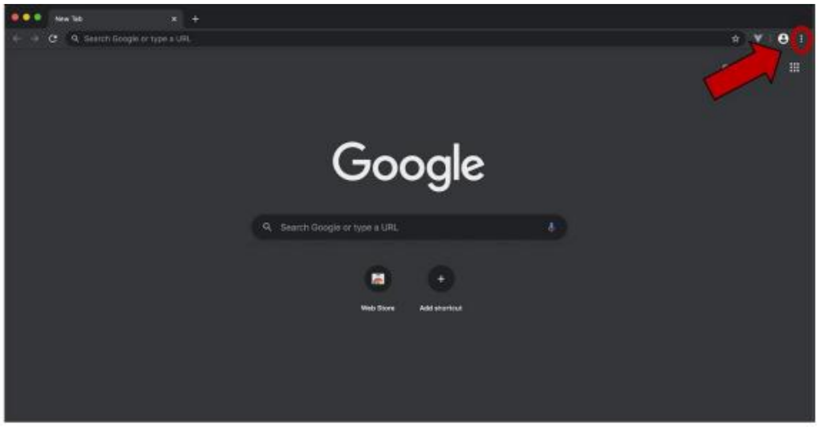
Google Chrome

Google Chrome is up to date
Version 81.0.4044.138 (Official Build) (64-bit)

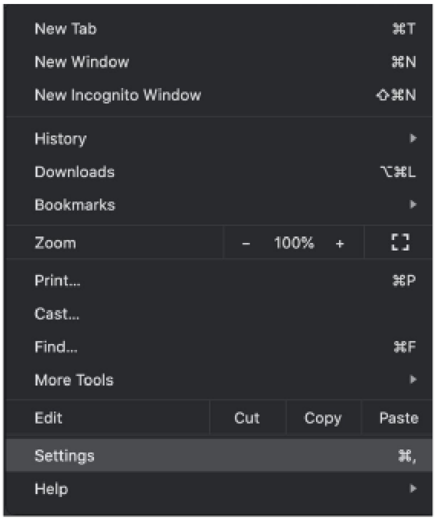
Google Chrome's Privacy and Security Settings.

It is essential to review your privacy and security settings. Abusers could find ways to receive information about the websites you visit.

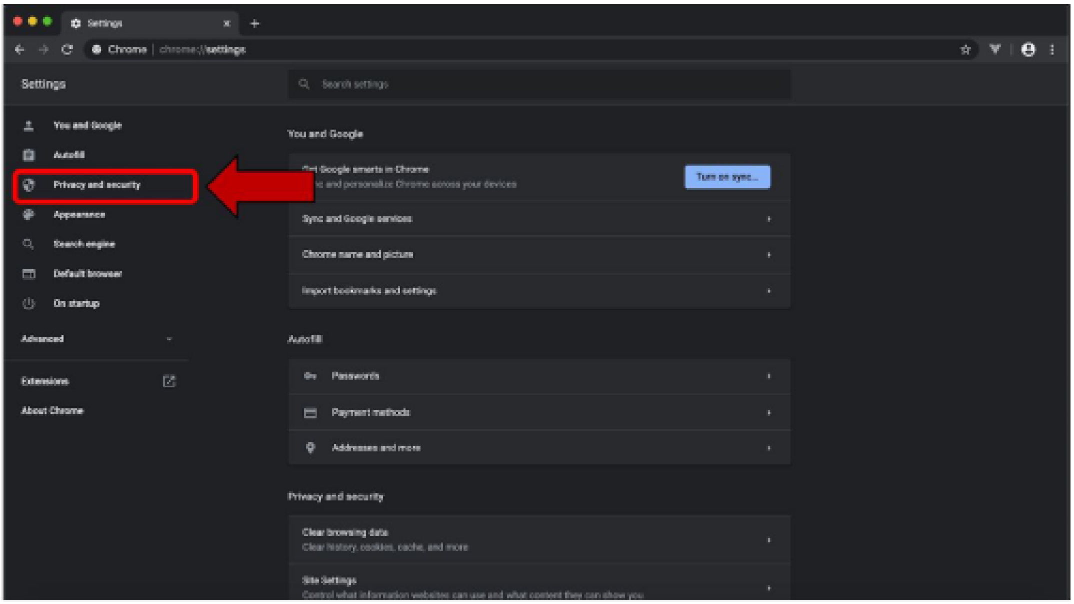
1. Open **Google Chrome**, click on this icon.
2. Usually, the following screen will be shown. Located at the top right, click the 3 dots.



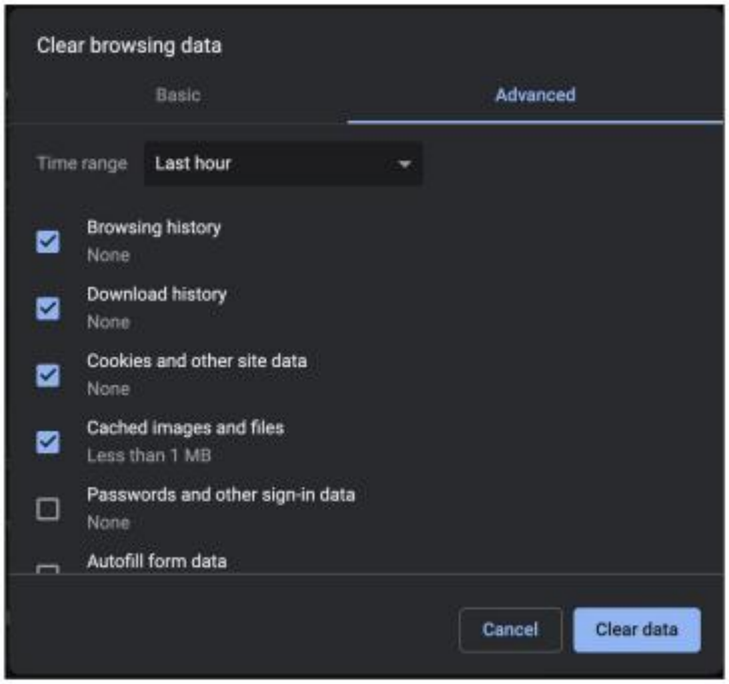
3. The customize and control menu will open, click on **Settings.**



4. Click on **Privacy and Security** on the menu showing on the left of the **Settings'** page**.**



5. On the bottom of the screen, click on **Clear Browsing Data.** The following will appear:



Clear browsing data

Basic | Advanced

Time range: Last hour

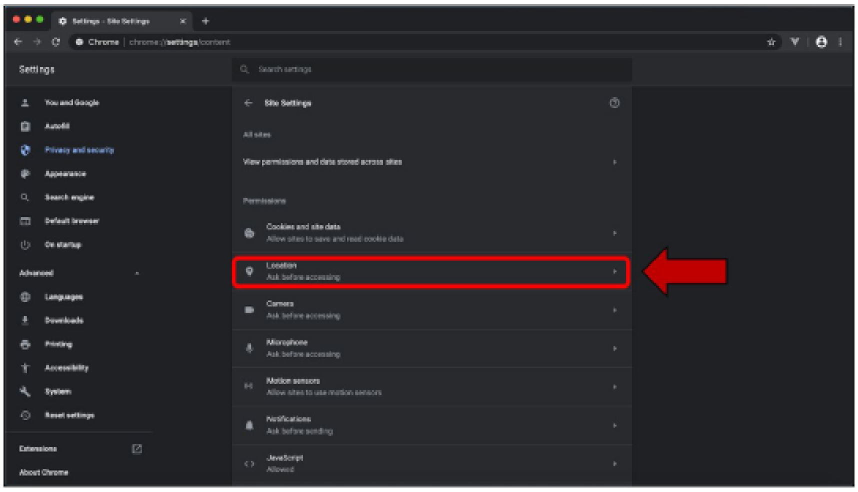
- ☑ Browsing history — None
- ☑ Download history — None
- ☑ Cookies and other site data — None
- ☑ Cached images and files — Less than 1 MB
- ☐ Passwords and other sign-in data — None
- ☐ Autofill form data

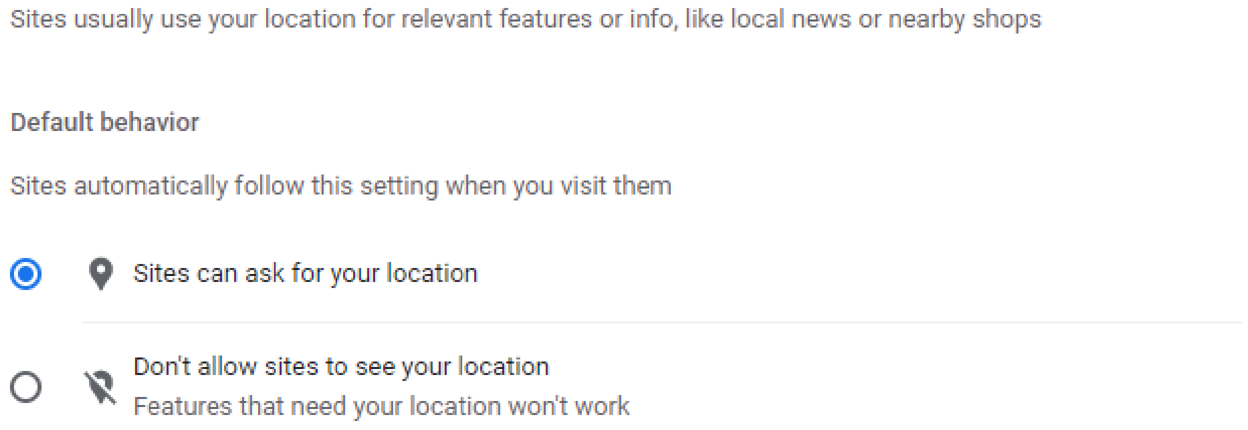
Under **Advanced**, you can check which category you would like to clear data. Browsing history provides a history of the websites you have previously visited. Cookies and other site data are a type of online ID that the websites you had visited use to track and identify you. There is also a section for Passwords and other sign-in data. Once you have selected the categories you would like to delete, click on **Clear Data**.

If abusers are using your saved passwords to gain access to online accounts then they will be aware that you may have cleared that data. Speak with the appropriate organizations to make plans for your safety.

Site Settings

Under the **Privacy and Security Settings**, there is also an option called **Site Settings.** Under Site Settings, you can see which websites can connect to your location, microphone, and camera.





Sites usually use your location for relevant features or info, like local news or nearby shops

Default behavior

Sites automatically follow this setting when you visit them

● Sites can ask for your location

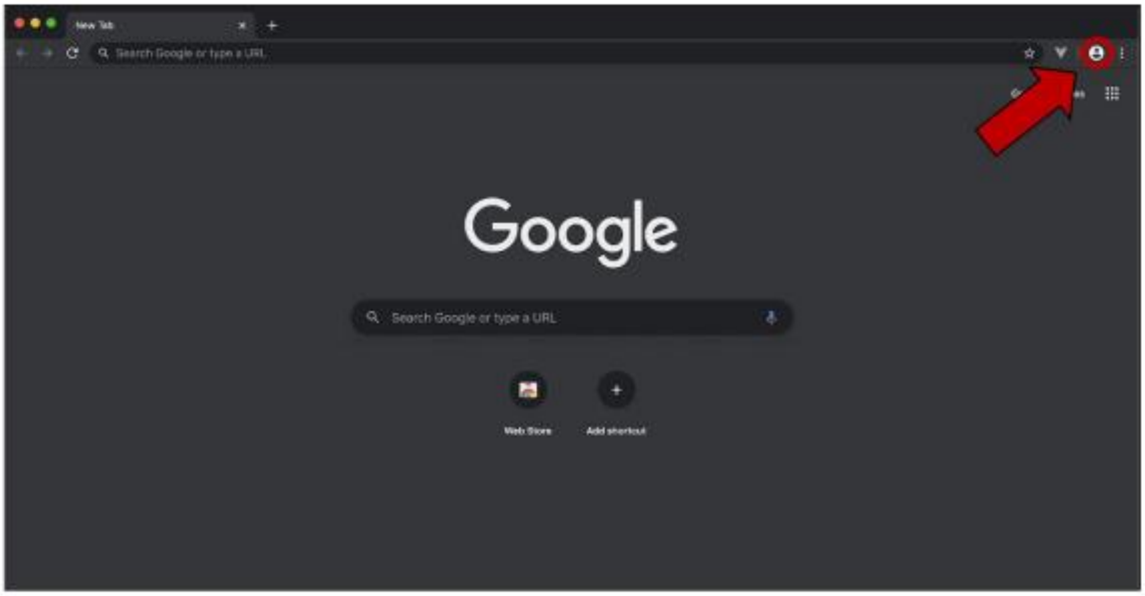
○ Don't allow sites to see your location
Features that need your location won't work

You will have the options to select, "**Sites can ask for your location**" or "**Don't allow sites to see your location**". These options are also available for the microphone and camera.

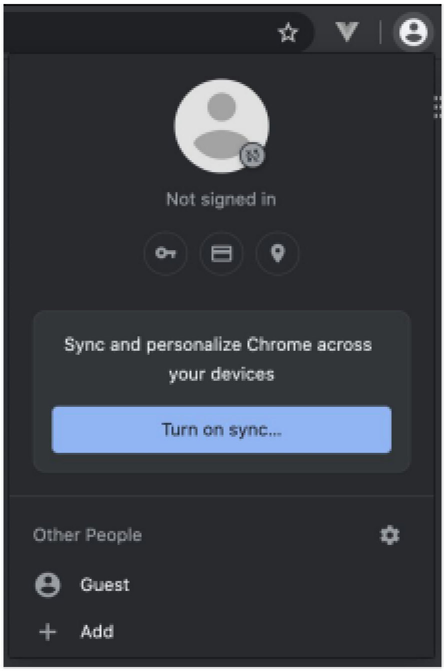
Check if your Sync Feature is on.

The **Sync** Feature with Google Chrome syncs information like bookmarks and extensions across all your devices. This could give an opportunity for an abuser to gain access to your information from various devices.

1. Open **Google Chrome**, click on this icon.
2. Click on the **Profile** button at the top right corner:



3. If you see a **Turn on sync..** button, your sync feature is turned off. If you see a **Turn-off button,** the sync feature is turned on. You could also see that the sync feature says, "**Sync is on"**. You will see the following:


Not signed in

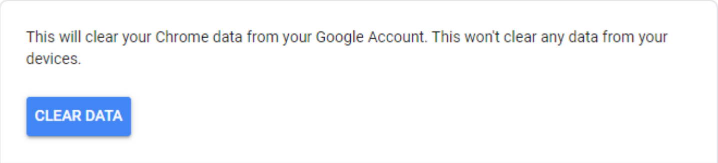
Sync and personalize Chrome across your devices

Customize what you sync.

1. On your computer, open Chrome.
2. At the top right, click More ⋮ > **Settings**.
3. Click **You and Google** > **Sync and Google services**.
4. Under “Sync,” click **Manage what you sync**.
5. Click **Customize sync**.
6. Turn off any data that you don’t want to sync to your account.

Delete Sync Information

1. Click on **Profile**, then the **sync** feature.
2. Click on **Review your synced data.**
3. At the bottom of the page, there is a button, **Clear Data.**



This will clear your Chrome data from your Google Account. This won't clear any data from your devices.

Facebook

https://www.ceta.tech.cornell.edu/_files/ugd/c4e6d5_01e4e6e33987443ea2244afcd7880706.pdf

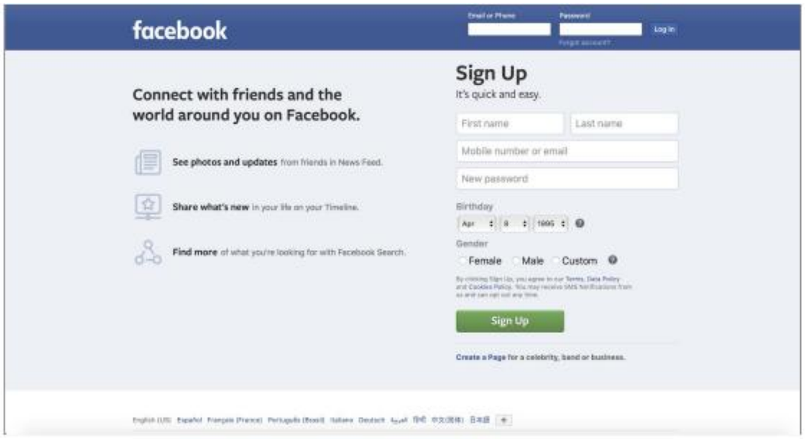
https://www.ceta.tech.cornell.edu/_files/ugd/c4e6d5_baf5a1e048714876b9b91a8c638aaf08.pdf

What is two-factor authentication?

This feature provides an extra security step that protects your online account. When it is turned on, every time you try to log in, you will be required to provide another code that only you should know.

Be aware if your abuser knows your password and has been using it to log in. They will know when two-factor authentication is enabled. Speak with the appropriate organizations to create a plan for your safety and steps moving forward.

1. Logging into your Facebook account, go to: https://www.facebook.com/



Connect with friends and the world around you on Facebook.

See photos and updates from friends in News Feed.

Share what's new in your life on your Timeline.

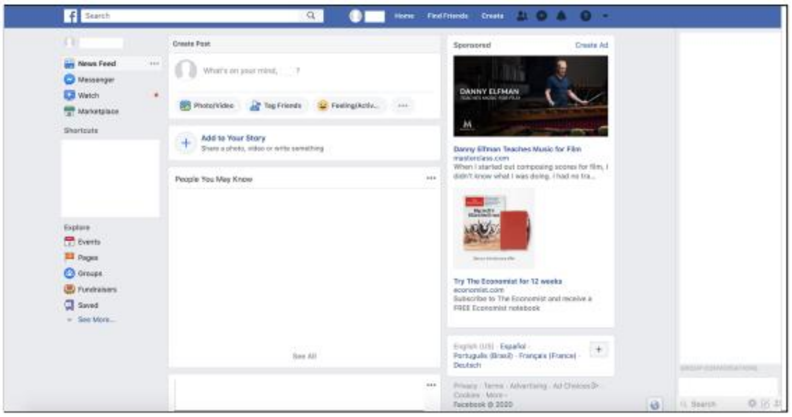
Find more of what you're looking for with Facebook Search.

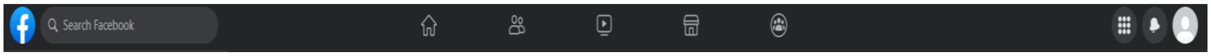
Sign Up

It's quick and easy.

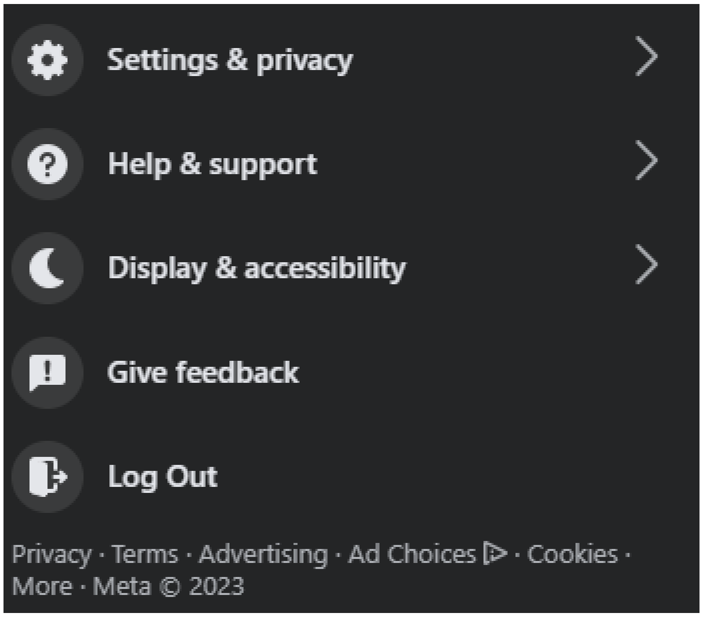
Create a Page for a celebrity, band or business.

2. Once you are logged in, click on the down arrow on the top right or your account profile

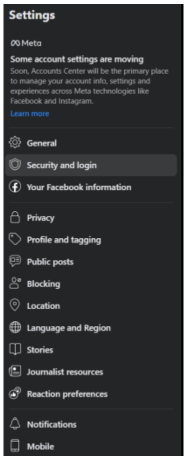




3. Click on Settings & Privacy.



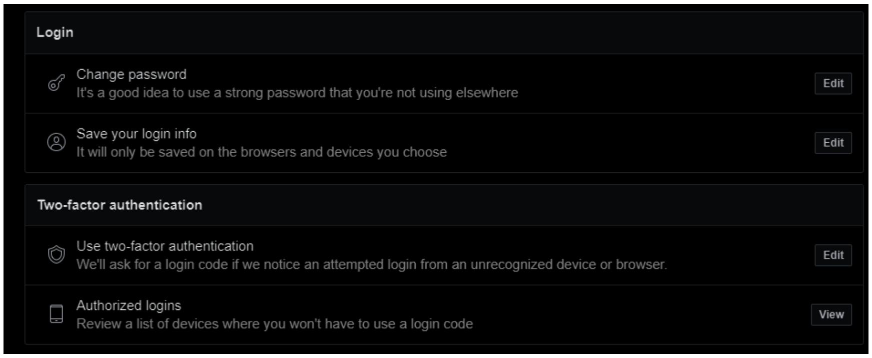
4. On the left side, click on **Security and Login.**



Some account settings are moving

Soon, Accounts Center will be the primary place to manage your account info, settings and experiences across Meta technologies like Facebook and Instagram.

5. In the Security and Login section, scroll until you find **Two-Factor Authentication.** Click "**Edit**" and then you will see the following page:



Login

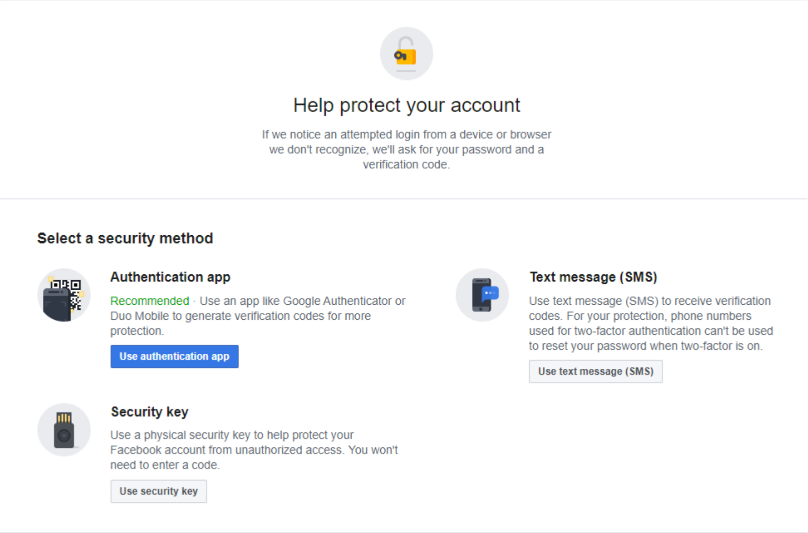
Change password
It's a good idea to use a strong password that you're not using elsewhere

Save your login info
It will only be saved on the browsers and devices you choose

Two-factor authentication

Use two-factor authentication
We'll ask for a login code if we notice an attempted login from an unrecognized device or browser.

Authorized logins
Review a list of devices where you won't have to use a login code



Help protect your account

If we notice an attempted login from a device or browser we don't recognize, we'll ask for your password and a verification code.

Select a security method

Authentication app
Recommended · Use an app like Google Authenticator or Duo Mobile to generate verification codes for more protection.

Text message (SMS)
Use text message (SMS) to receive verification codes. For your protection, phone numbers used for two-factor authentication can't be used to reset your password when two-factor is on.

Security key
Use a physical security key to help protect your Facebook account from unauthorized access. You won't need to enter a code.

There will be different options for you to use.

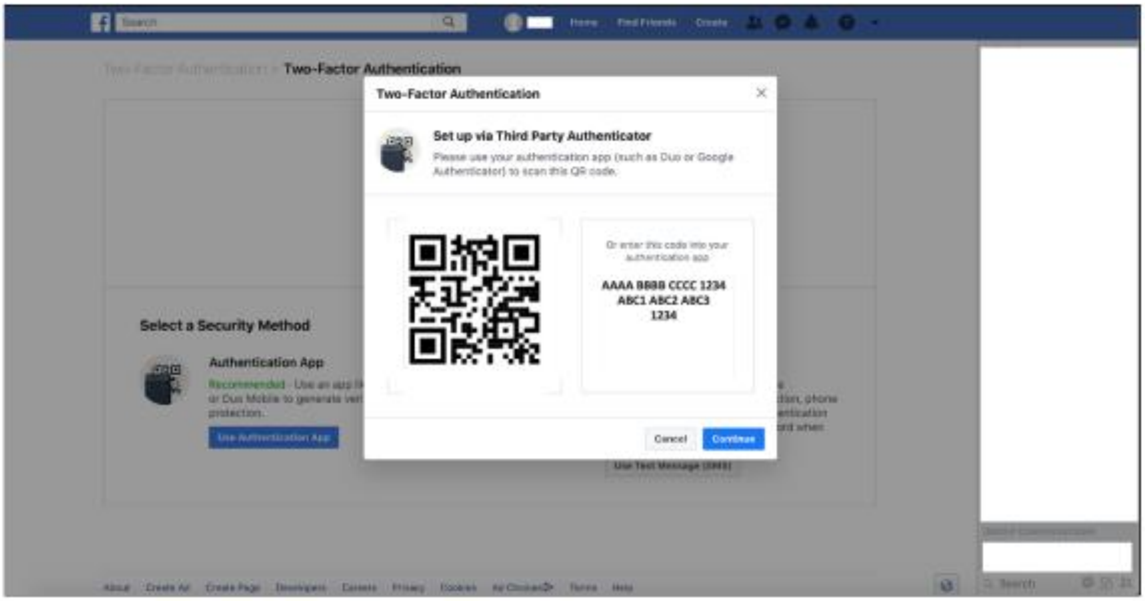
The **authentication app** is a mobile app that generates codes (one-time passwords) whenever you are trying to log in. Apps include **Google Authenticator**. This can be an option if you are concerned about your abuser having access to your text.

The **text message (SMS)** option will send a code to your mobile phone through text message.

Security Key is a physical security key that will protect your Facebook account from any unauthorized users. This method does not provide a code.

To use the authentication app

1. Click on **Use Authentication App**. The following page will appear with a QR Code or code for your authentication app.



Two-Factor Authentication

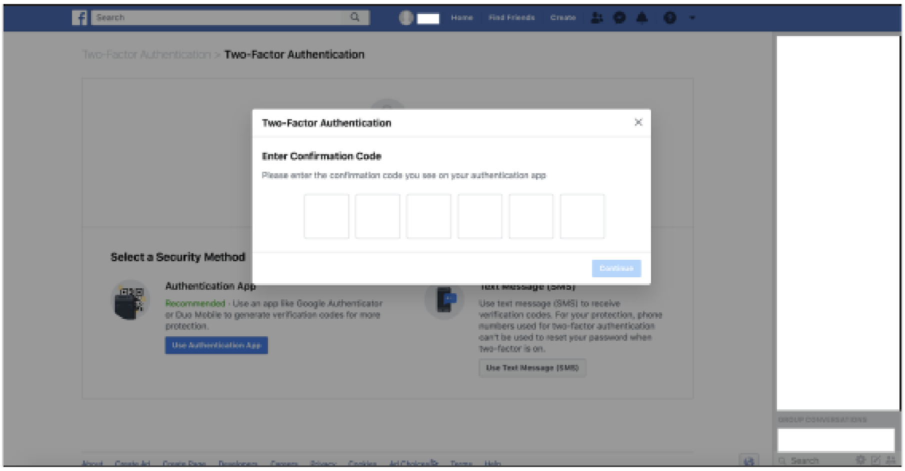
Set up via Third Party Authenticator

Please use your authentication app (such as Duo or Google Authenticator) to scan this QR code.

Or enter this code into your authentication app

AAAA BBBB CCCC 1234 ABC1 ABC2 ABC3 1234

2. You will then need install an authentication app from the app store. Apps include Google Authenticator. You can use an Apple App Store for iPhones and Google Play Store for Android phones (Samsung, LG, or Motorola).
3. Regardless of the app, scan the QR code or enter the code.
    a. For Google Authenticator.
        i. Select the **plus** button at the top right corner.
        ii. A menu will appear, click on the **Scan barcode.**
        iii. Scan the barcode provided by Facebook. You will then see a row titled, “Facebook” with a number in your Google Authenticator app.
4. Once you have scanned the barcode or entered the code, continue on Facebook.
5. You will need to add a confirmation code from the app and then re-enter your Facebook information again.



Two-Factor Authentication

Enter Confirmation Code

Please enter the confirmation code you see on your authentication app

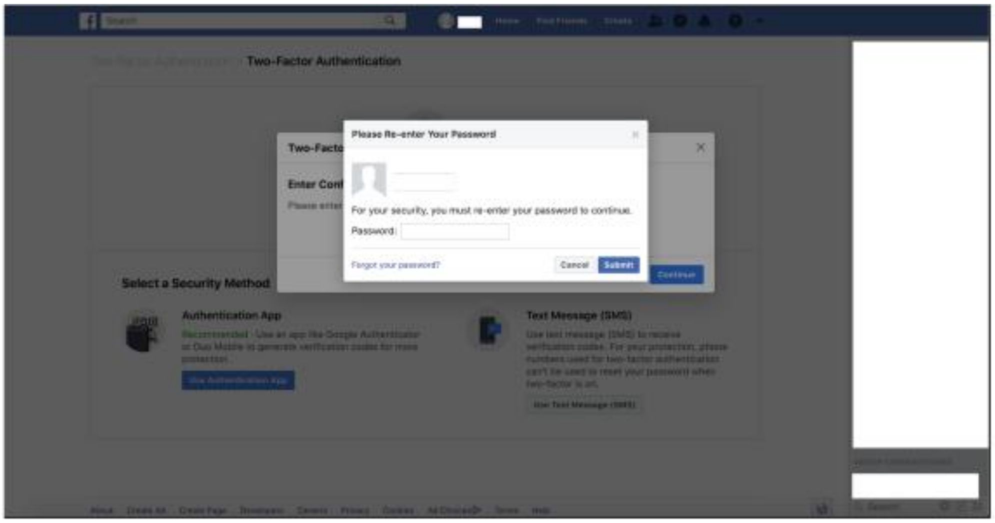
Select a Security Method

Authentication App

Recommended · Use an app like Google Authenticator or Duo Mobile to generate verification codes for more protection.

Text Message (SMS)

Use text message (SMS) to receive verification codes. For your protection, phone numbers used for two-factor authentication can't be used to reset your password when two-factor is on.



Please Re-enter Your Password

For your security, you must re-enter your password to continue.

Password:

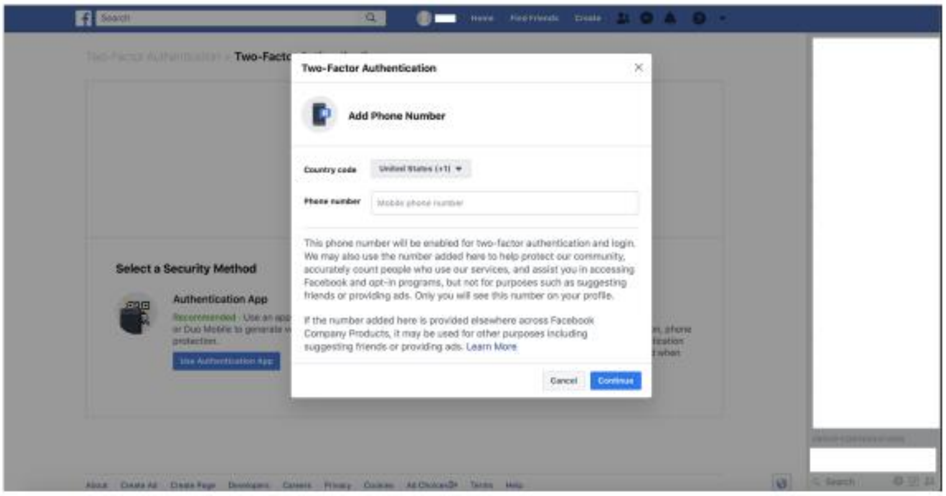
Be aware, you might receive email notifications depending on your settings that you have set up for two-factor authentication. Be careful, if an offender has access to your email account, he may see the message from Facebook.

1. Go to **Settings & Privacy**
2. On the left side menu, click on **Notifications.** You can adjust what information will be sent to your email or phone.

To use the Text Message (SMS)

Only use this method if you have a secure phone and do not have any concerns about an abuser viewing information from your text.

1. On the Security Methods Page, click on **Use Text Message (SMS)**. The following page will appear.



Two-Factor Authentication

Add Phone Number

Country code: United States (+1)

Phone number: Mobile phone number

This phone number will be enabled for two-factor authentication and login. We may also use the number added here to help protect our community, accurately count people who use our services, and assist you in accessing Facebook and opt-in programs, but not for purposes such as suggesting friends or providing ads. Only you will see this number on your profile.

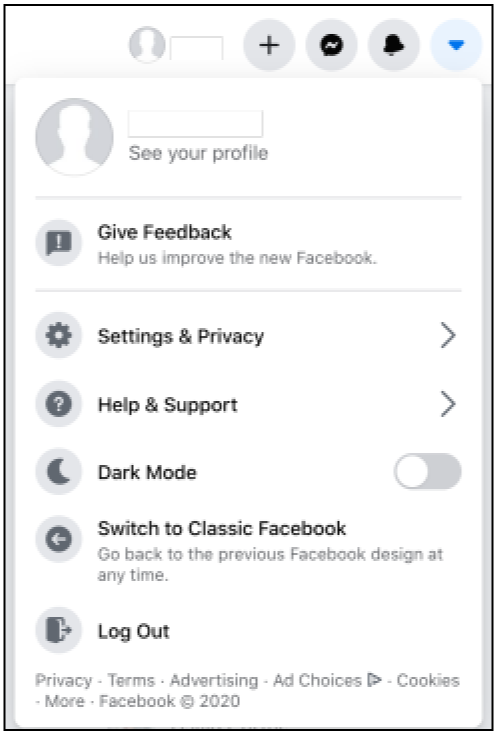
If the number added here is provided elsewhere across Facebook Company Products, it may be used for other purposes including suggesting friends or providing ads. Learn More

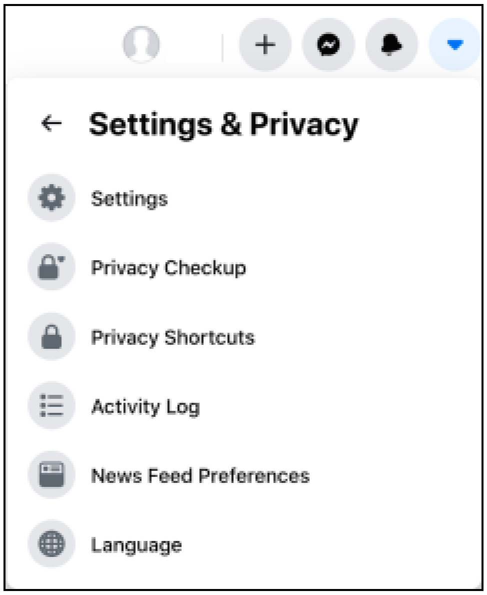
2. Enter your phone number then enter the code that is sent to your phone. You may have to enter your Facebook information once your click done.

Facebook Clean-up

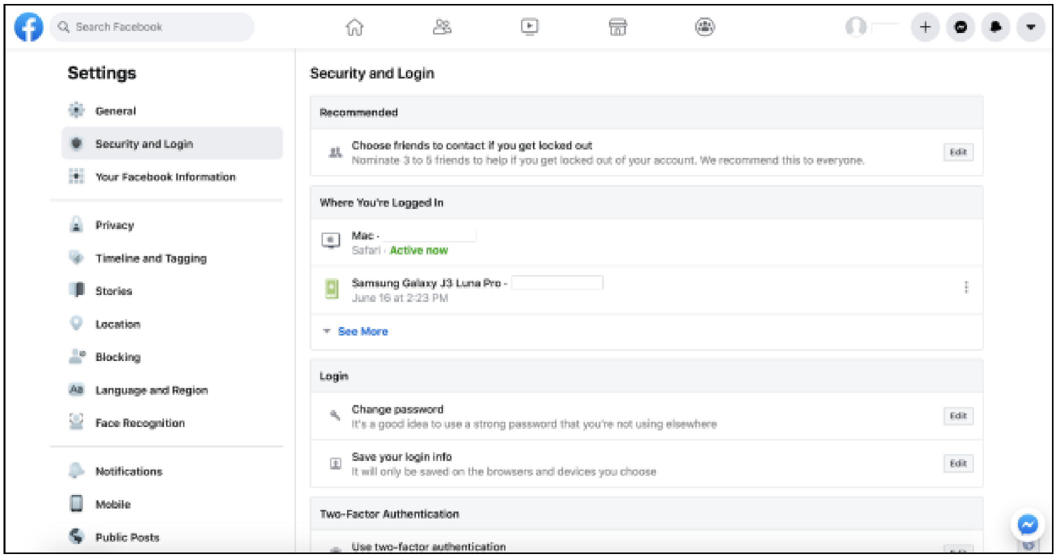
This section is for people who suspect or know someone that has gotten access to their Facebook account.

1. Log into your Facebook book account through https://www.facebook.com/
2. From the main page, click on your **Profile** or the downward triangle.
3. Select the **Settings & Privacy** then select **Settings.**


See your profile
Give Feedback
Help us improve the new Facebook.
Settings & Privacy
Help & Support
Dark Mode
Switch to Classic Facebook
Go back to the previous Facebook design at any time.
Log Out
Privacy · Terms · Advertising · Ad Choices ▷ · Cookies · More · Facebook © 2020



4. On the left side menu, click on **Security and Login**.



Security and Login

Recommended

Choose friends to contact if you get locked out
Nominate 3 to 5 friends to help if you get locked out of your account. We recommend this to everyone.

Where You're Logged In

Mac ·
Safari · Active now

Samsung Galaxy J3 Luna Pro ·
June 16 at 2:23 PM

Login

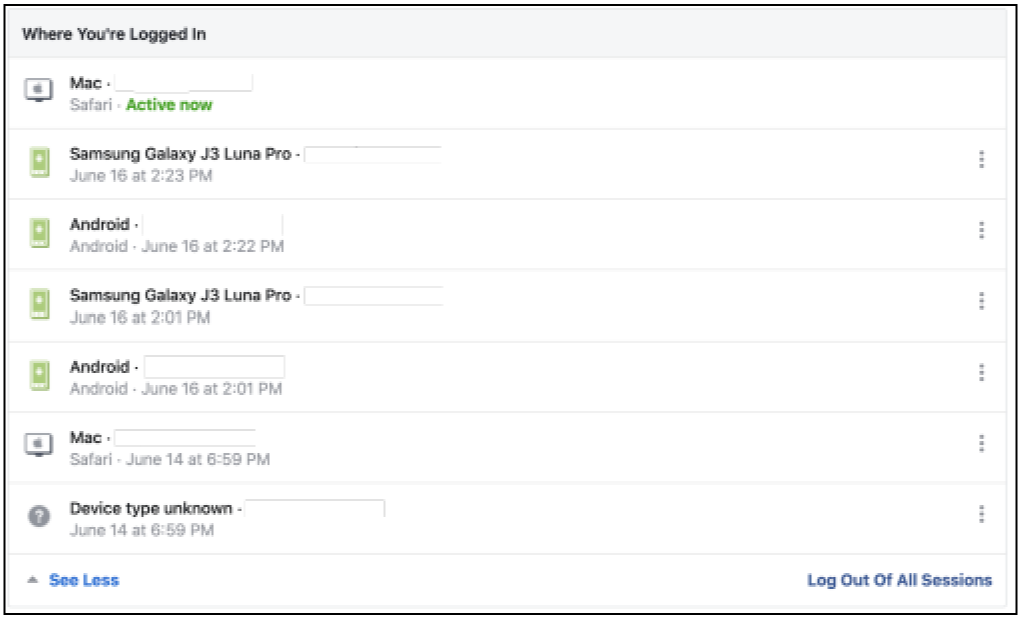
Change password
It's a good idea to use a strong password that you're not using elsewhere

Save your login info
It will only be saved on the browsers and devices you choose

Two-Factor Authentication

Use two-factor authentication

5. Click on **See More** under **Where You're Logged In.** Each session will show when you have logged into your account and contains information about where you have signed in from with the time and browser.



Where You're Logged In

Mac ·
Safari · Active now

Samsung Galaxy J3 Luna Pro ·
June 16 at 2:23 PM

Android ·
Android · June 16 at 2:22 PM

Samsung Galaxy J3 Luna Pro ·
June 16 at 2:01 PM

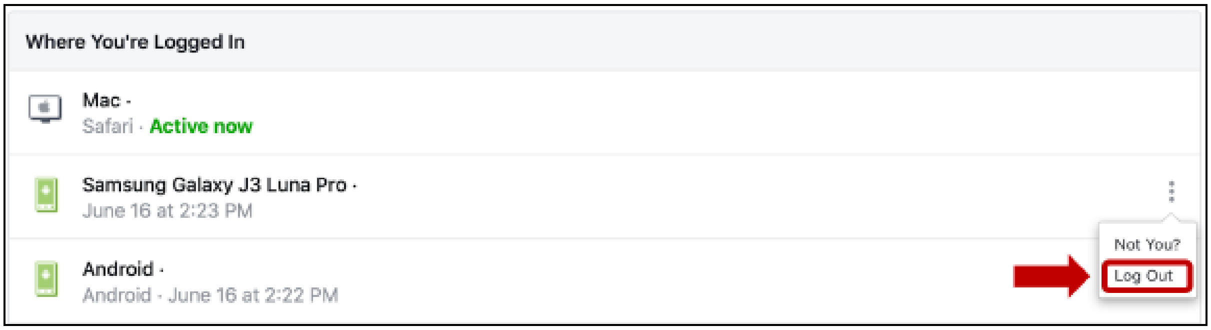
Android ·
Android · June 16 at 2:01 PM

Mac ·
Safari · June 14 at 6:59 PM

Device type unknown ·
June 14 at 6:59 PM

You will then have two options.

First, you can log out of the device if you do not think it is you by clicking on the three dots for that specific device and then clicking **Log Out.**



Where You're Logged In

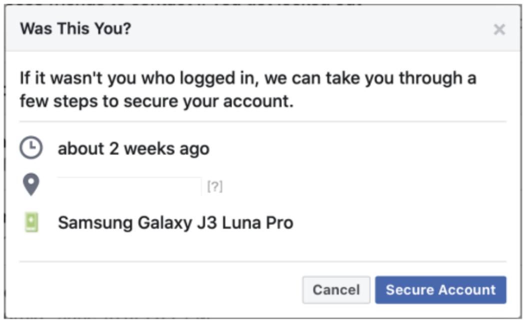
Mac ·
Safari · Active now

Samsung Galaxy J3 Luna Pro ·
June 16 at 2:23 PM

Android ·
Android · June 16 at 2:22 PM

Second, you can click on **Not You?** A window may appear for you to secure your account.

1. First click on **Not You?** Then **Secure Account**. You will then see another page, click on **Get Started**.



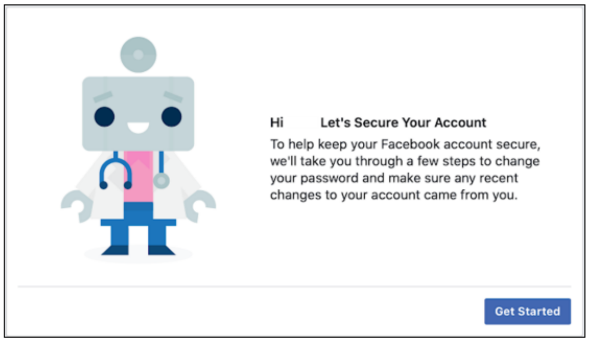
Was This You?

If it wasn't you who logged in, we can take you through a few steps to secure your account.

about 2 weeks ago

[?]

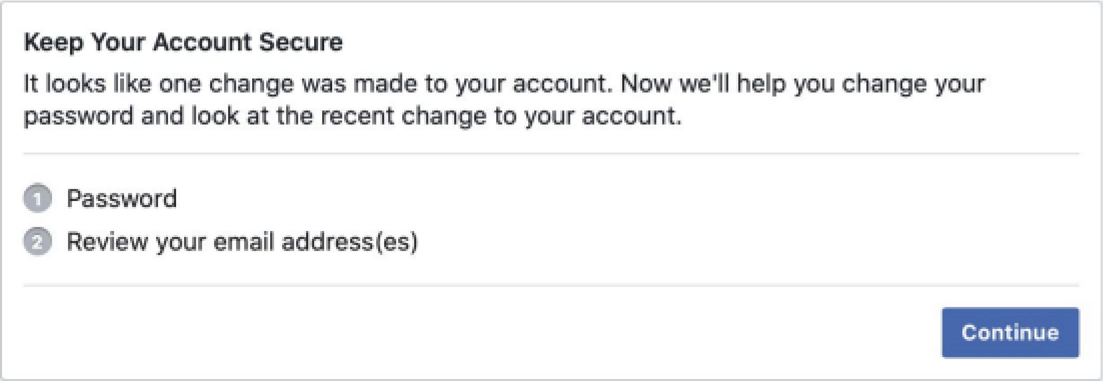
Samsung Galaxy J3 Luna Pro



Hi Let's Secure Your Account

To help keep your Facebook account secure, we'll take you through a few steps to change your password and make sure any recent changes to your account came from you.

2. After Facebook has reviewed your recent activities, it may ask you to check some aspects of the account.



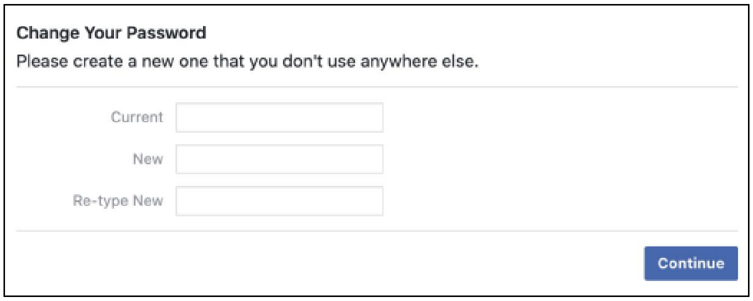
Keep Your Account Secure

It looks like one change was made to your account. Now we'll help you change your password and look at the recent change to your account.

1 Password

2 Review your email address(es)

3. Click **Continue** to update your password and review any email addresses that are linked to your Facebook account.



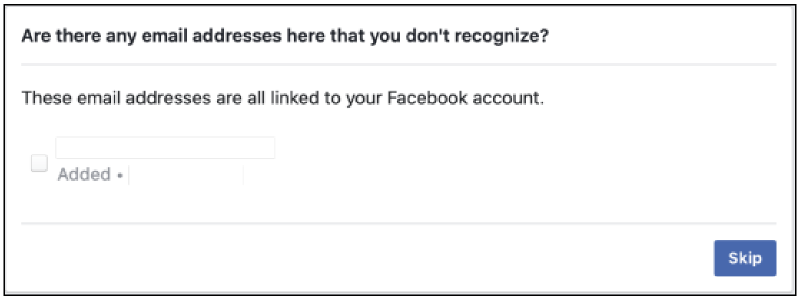
Change Your Password

Please create a new one that you don't use anywhere else.

Current

New

Re-type New

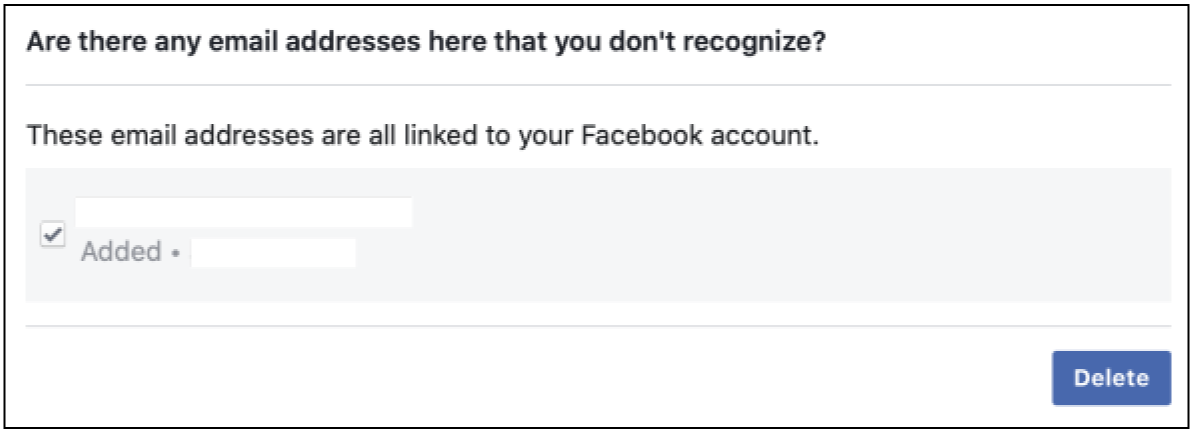


Are there any email addresses here that you don't recognize?

These email addresses are all linked to your Facebook account.

□ Added •

4. You will find the dates when your email address has been added to your Facebook account. For any email addresses you do not recognize, select the **checkbox** then click **Delete.**

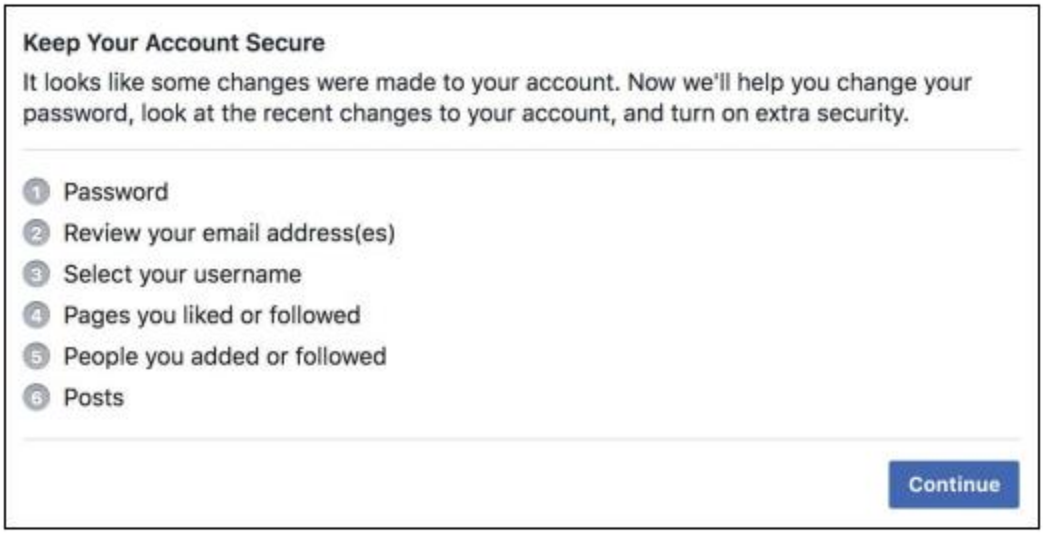


Are there any email addresses here that you don't recognize?

These email addresses are all linked to your Facebook account.

☑ Added •

5. Some accounts may have more options like the following:

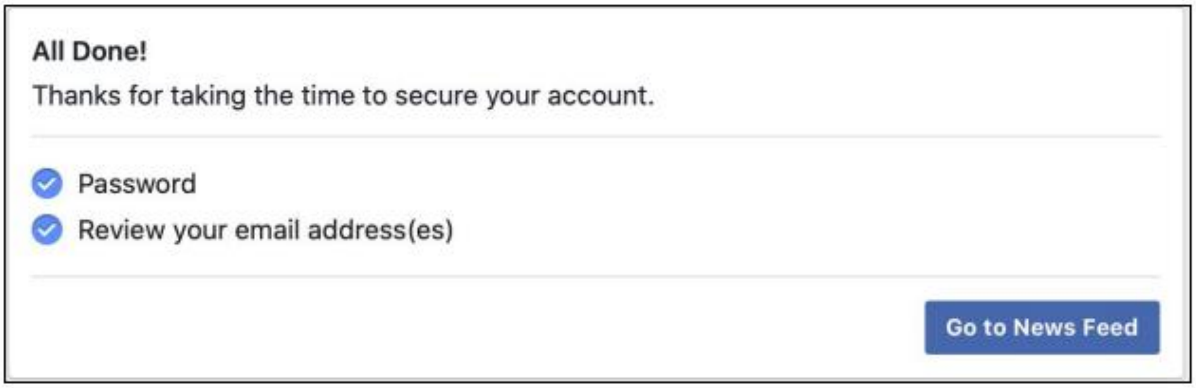


Keep Your Account Secure

It looks like some changes were made to your account. Now we'll help you change your password, look at the recent changes to your account, and turn on extra security.

1. Password
2. Review your email address(es)
3. Select your username
4. Pages you liked or followed
5. People you added or followed
6. Posts

6. Once you are done, you will see the following popup:



All Done!

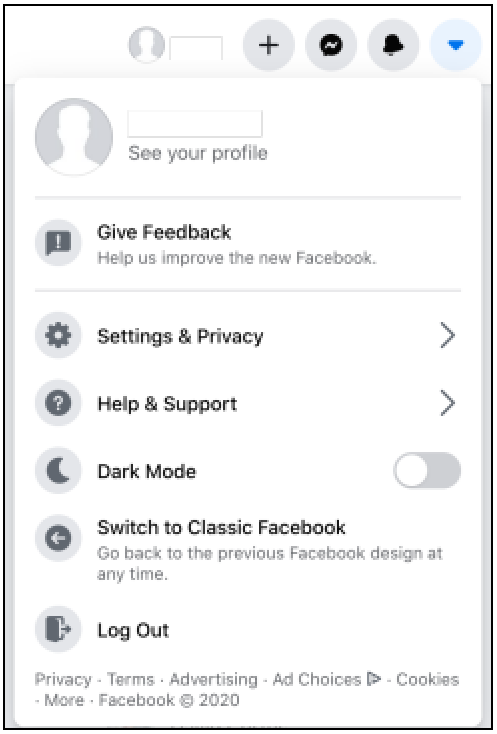
Thanks for taking the time to secure your account.

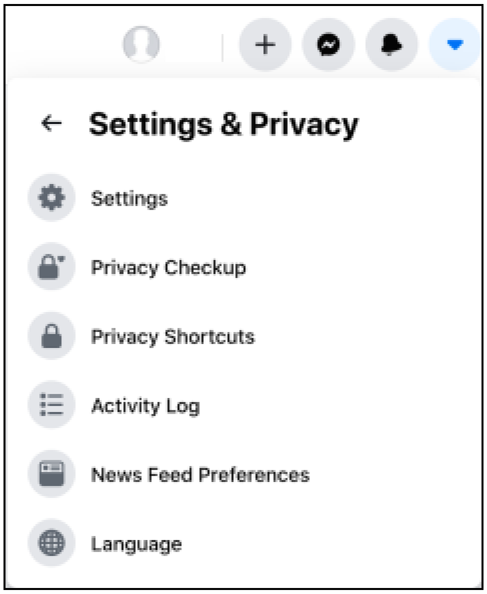
✓ Password

✓ Review your email address(es)

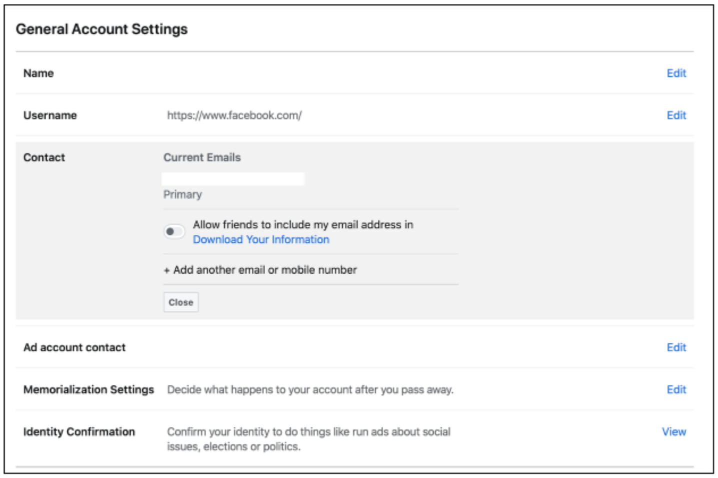
Check for Recovery Email Address and Phone Number

1. Log into your Facebook book account through https://www.facebook.com/
2. From the main page, click on your **Profile** or the downward triangle.
3. Select the **Settings & Privacy** then select **Settings.**


See your profile
Give Feedback
Help us improve the new Facebook.
Settings & Privacy
Help & Support
Dark Mode
Switch to Classic Facebook
Go back to the previous Facebook design at any time.
Log Out
Privacy · Terms · Advertising · Ad Choices ▷ · Cookies · More · Facebook © 2020



4. On the left side menu, click on **General** then click on the **Contact Section.**



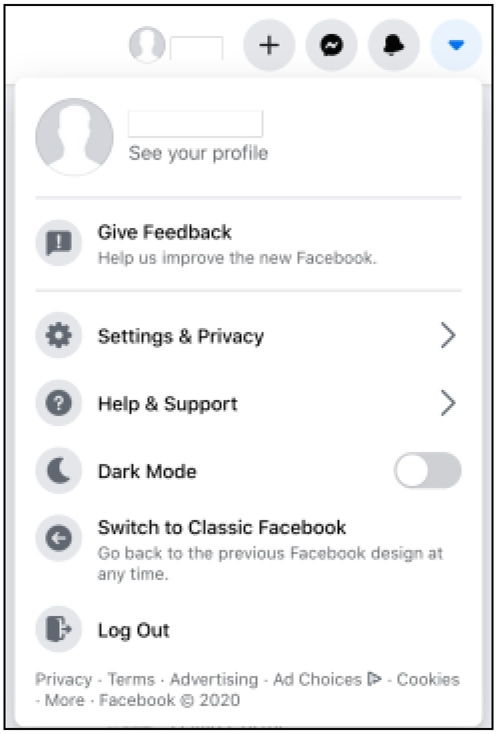
General Account Settings

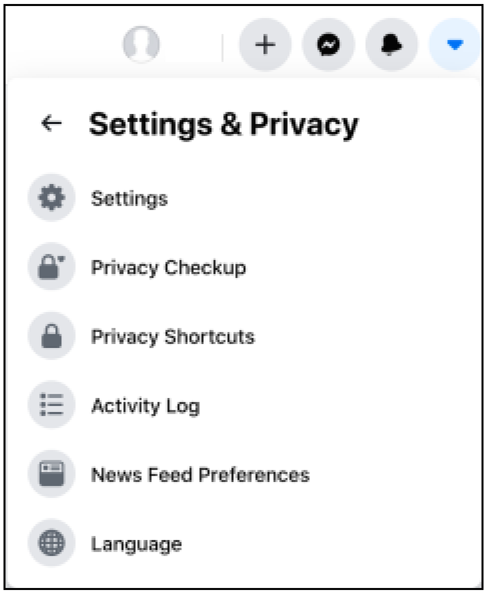
Name		Edit
Username	https://www.facebook.com/	Edit
Contact	Current Emails Primary Allow friends to include my email address in Download Your Information + Add another email or mobile number Close	
Ad account contact		Edit
Memorialization Settings	Decide what happens to your account after you pass away.	Edit
Identity Confirmation	Confirm your identity to do things like run ads about social issues, elections or politics.	View

Confirm all the emails and mobile numbers in this section is yours and is not available to anyone else. To recover your Facebook account with email or phone number, ensure they are safe.

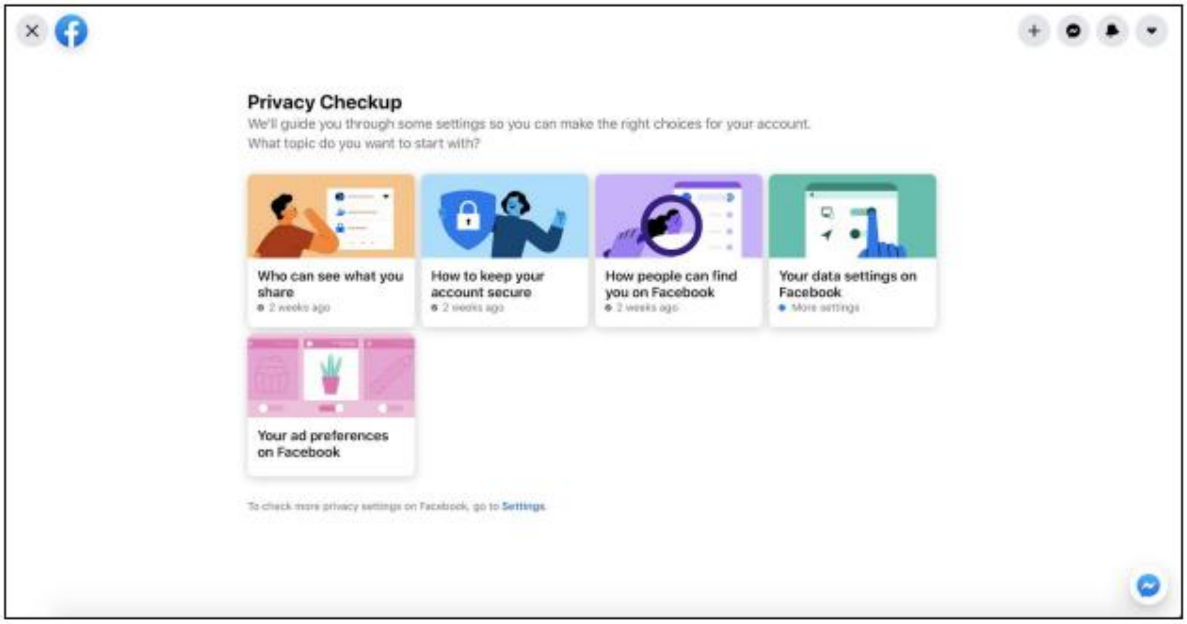
Privacy Checkup

1. Log into your Facebook book account through https://www.facebook.com/
2. From the main page, click on your **Profile** or the downwards triangle.
3. Click on **Settings & Privacy** then click on **Privacy Checkup.**


See your profile
Give Feedback
Help us improve the new Facebook.
Settings & Privacy
Help & Support
Dark Mode
Switch to Classic Facebook
Go back to the previous Facebook design at any time.
Log Out
Privacy · Terms · Advertising · Ad Choices ▷ · Cookies · More · Facebook © 2020



4. The following page will appear will many options. Facebook provides these options to help you review your privacy and security.



Privacy Checkup

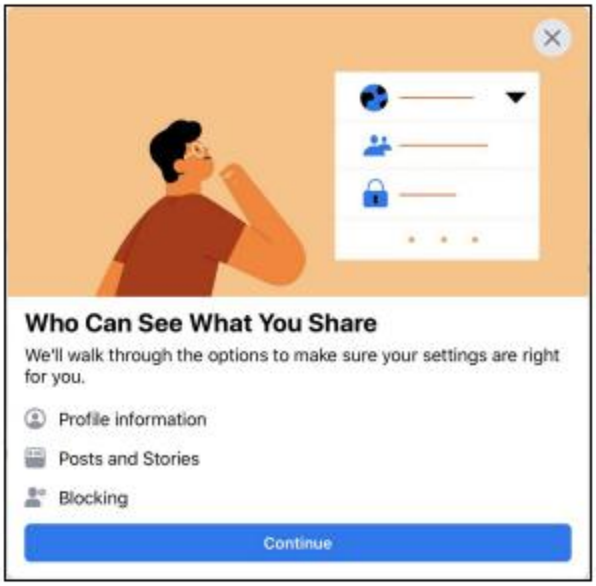
We'll guide you through some settings so you can make the right choices for your account. What topic do you want to start with?

Who can see what you share
2 weeks ago
How to keep your account secure
2 weeks ago
How people can find you on Facebook
2 weeks ago
Your data settings on Facebook
More settings
Your ad preferences on Facebook

To check more privacy settings on Facebook, go to Settings.

5. An example is the **Who can see what you share.**

a. Click on that section, then click **Continue**.



Who Can See What You Share

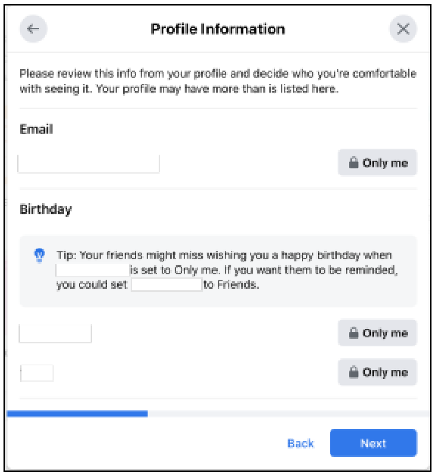
We'll walk through the options to make sure your settings are right for you.

Profile information

Posts and Stories

Blocking

b. You may adjust certain settings with the following pages. They may look like:



Profile Information

Please review this info from your profile and decide who you're comfortable with seeing it. Your profile may have more than is listed here.

Email

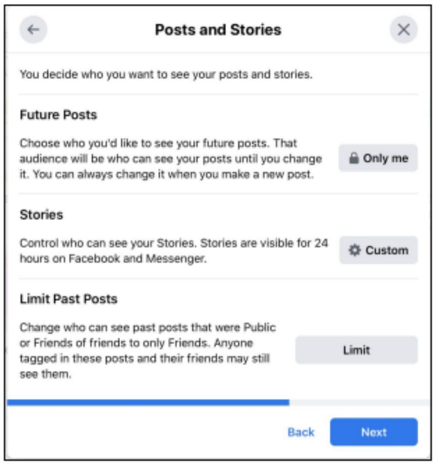
Only me

Birthday

Tip: Your friends might miss wishing you a happy birthday when is set to Only me. If you want them to be reminded, you could set to Friends.

Only me

Only me



Posts and Stories

You decide who you want to see your posts and stories.

Future Posts

Choose who you'd like to see your future posts. That audience will be who can see your posts until you change it. You can always change it when you make a new post.

Only me

Stories

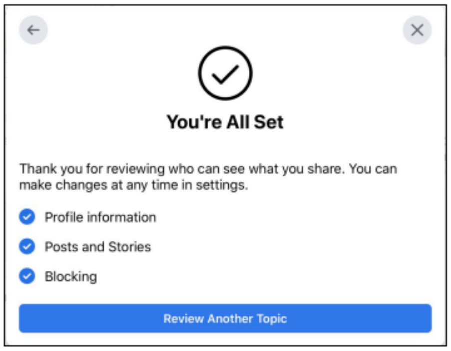
Control who can see your Stories. Stories are visible for 24 hours on Facebook and Messenger.

Custom

Limit Past Posts

Change who can see past posts that were Public or Friends of friends to only Friends. Anyone tagged in these posts and their friends may still see them.

6. Once you are finished, you can **Review Another Topic**



You're All Set

Thank you for reviewing who can see what you share. You can make changes at any time in settings.

- Profile information
- Posts and Stories
- Blocking

Review Another Topic

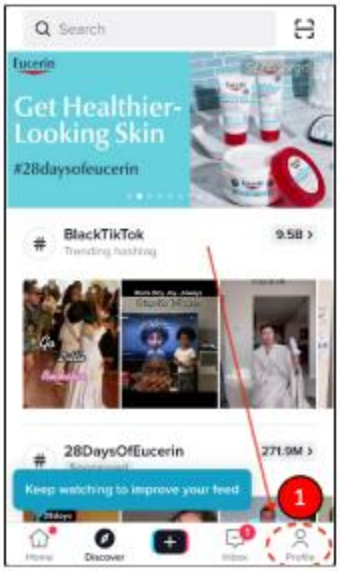
TikTok

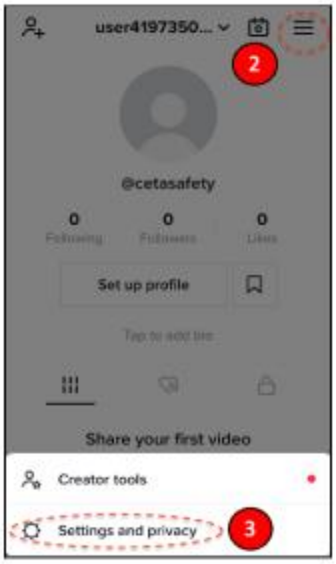
https://www.ceta.tech.cornell.edu/_files/ugd/884c63_d977c4a205d94bf8b919160f67e9ef59.pdf

This section is to strengthen your TikTok account's security and privacy.

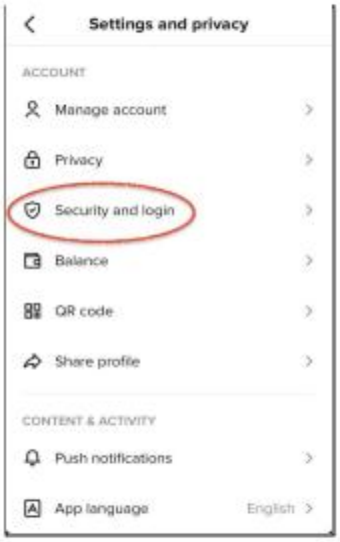
Viewing and Managing Devices Logged into Your Account

1. Open the TikTok app and select the **Settings** menu.
2. From the home page, go to **Profile** from the menu bar at the bottom.
3. In your **Profile** section, click on the **Three Bars** in the top right corner.
4. Lastly, tap **Settings and Privacy.**





5. Click on **Security and Login,** then **Manage Devices**.



Settings and privacy

ACCOUNT

Manage account

Privacy

Security and login

Balance

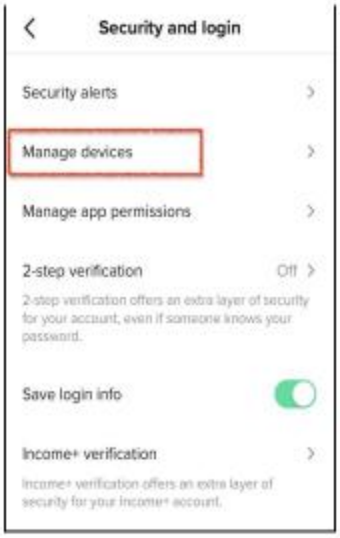
QR code

Share profile

CONTENT & ACTIVITY

Push notifications

App language English



Security and login

Security alerts

Manage devices

Manage app permissions

2-step verification Off

2-step verification offers an extra layer of security for your account, even if someone knows your password.

Save login info

Income+ verification

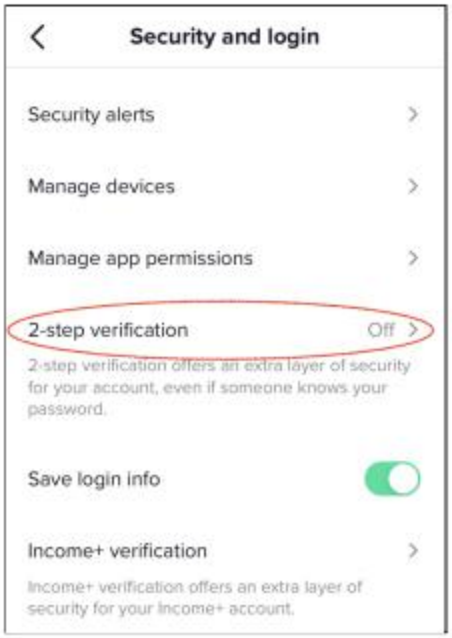
Income+ verification offers an extra layer of security for your Income+ account.

6. Inspect and remove any unauthorized devices you are not familiar with. There is a small trash icon beside each device. Simply click the trash icon to delete the device and it will log your account out of that device.

Turning On Two-Factor Authentication.

Two-Factor Authentication is an extra layer of protection every time you log into your device. You will need another code excluding your password to log in.

1. Go to your **Profile.**
2. Settings and Privacy
3. Security and Login
4. 2-Step verification.



Security and login

Security alerts

Manage devices

Manage app permissions

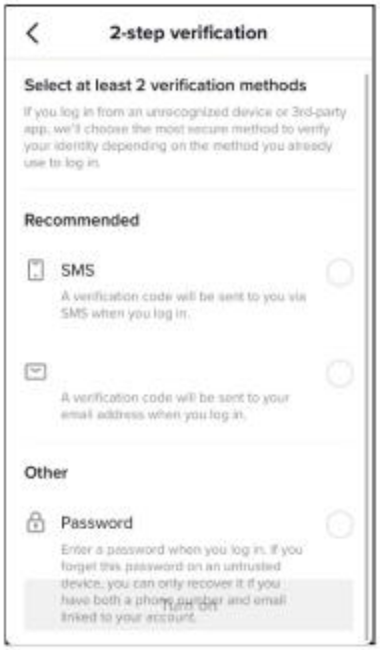
2-step verification Off

2-step verification offers an extra layer of security for your account, even if someone knows your password.

Save login info

Income+ verification

Income+ verification offers an extra layer of security for your Income+ account.



2-step verification

Select at least 2 verification methods

If you log in from an unrecognized device or 3rd-party app, we'll choose the most secure method to verify your identity depending on the method you already use to log in.

Recommended

SMS

A verification code will be sent to you via SMS when you log in.

A verification code will be sent to your email address when you log in.

Other

Password

Enter a password when you log in. If you forget this password on an untrusted device, you can only recover it if you have both a phone number and email linked to your account.

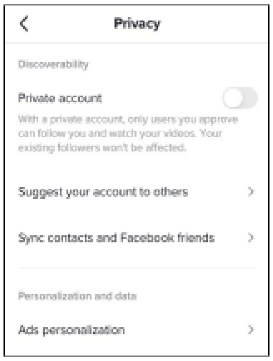
Turn on

You will have SMS or Email options that do require an external app. *Ensure these are safe devices with no suspicion of being tracked. *

- **Text Message (SMS)** will send a text message to your phone with a verification code when you right to log in.
- **Email** option will send an email with a code to the email associated with TikTok.

<u>Managing Visibility and Safety Settings For your Account.</u>

1. Go to your Settings and Privacy Menu.
2. Tap on Privacy
3. The first section at the top is **Discoverability** and the first option is **Private Account**. Accounts that are not aged 13-15 are not automatically set to Private Mode. You can toggle this option to make your account Private and will not allow users that are not following you to see your content.



Privacy

Discoverability

Private account

With a private account, only users you approve can follow you and watch your videos. Your existing followers won't be affected.

Suggest your account to others

Sync contacts and Facebook friends

Personalization and data

Ads personalization

4. There are other options under **Discoverability**, like **Location Services** and **Suggest your account to others.** Open those options and change the settings to your comfort.

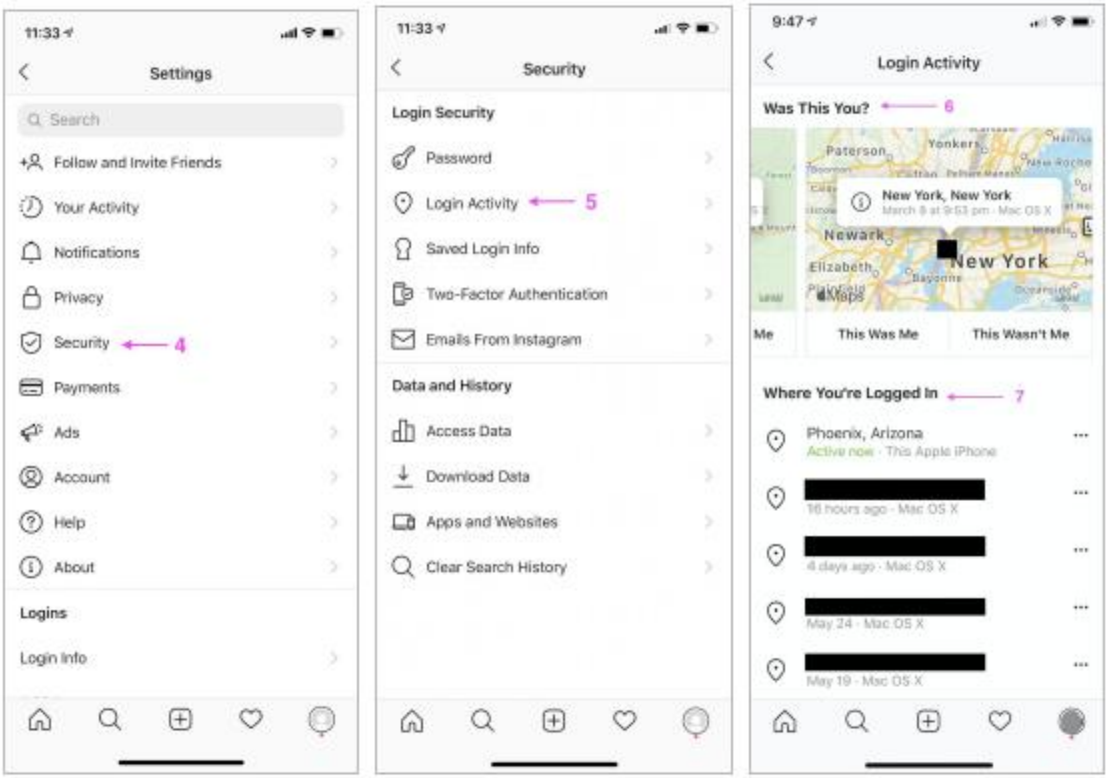
Instagram

https://www.ceta.tech.cornell.edu/_files/ugd/c4e6d5_4c8dd35286fe431d9a353a6aafc06f2e.pdf

This section is if you think someone has access to your account and you want to enhance security features.

Check for Recent Activity

1. Go to your **Profile** by clicking the profile picture at the bottom right.
2. Click the **Three Bars** at the top right of the profile.
3. Go to the Menu and click **Settings**.
4. Click on **Security** then **Login Activity.**



5. You can see the details for each session and log out of the device if it is not you.

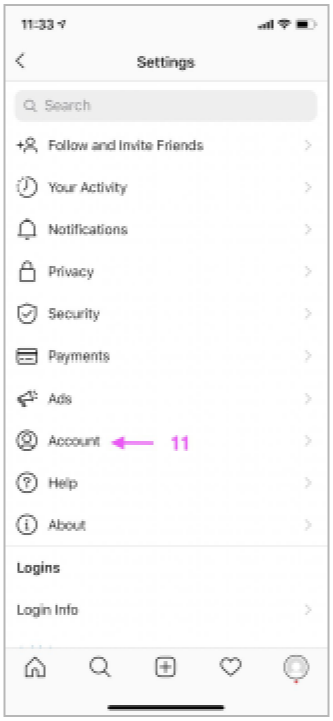
Apps and Website Connections.

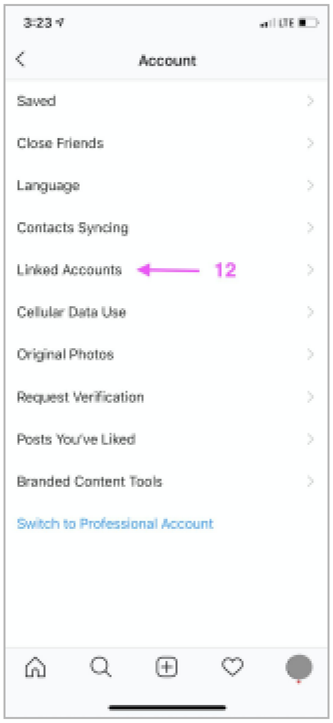
1. Go to your **Profile** by clicking the profile picture at the bottom right.
2. Click the **Three Bars** at the top right of the profile.
3. Go to the Menu and click **Settings**.
4. Under Data and History, click **Apps and Websites**. You can then check if any apps are linked with Instagram. Remove any unfamiliar apps.

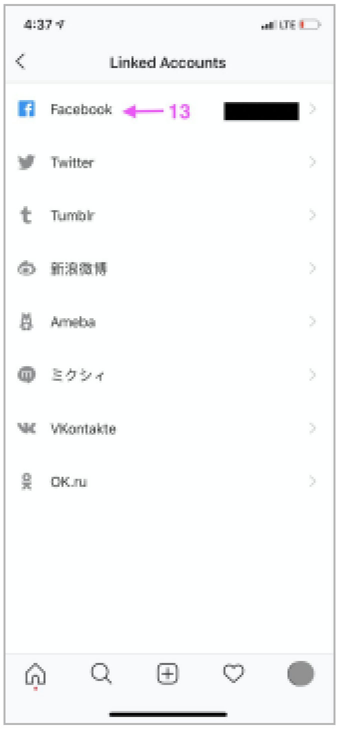
Linked Accounts

Depending on the settings if your Instagram is linked to other social media platforms. It can share your content on the other platform.

1. Go to your **Profile** by clicking the profile picture at the bottom right.
2. Click the **Three Bars** at the top right of the profile.
3. Go to the Menu and click **Settings**.
4. Go to **Accounts** then click on **Sharing to other apps.**





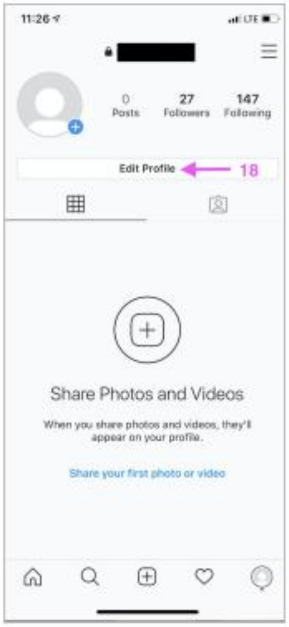


5. If your name is beside one of the platforms, then an account is linked to your Instagram. Click on the social media platform then at the bottom will be an Account center.
6. Click on **Accounts Center** then **Accounts** at the bottom of the screen.
7. It will then give you the option to **Remove** the account.

<u>Check Recovery Email and Phone</u>

Ensure your private information on your Instagram account is a recognizable email or phone number linked to the account.

1. Go to your **profile,** the icon on the bottom right (looks like a figure).
2. At the top of the screen below your information, you will see **“Edit Profile”**.
3. Click on Edit Profile then depending on the device, click on **“Personal Information Settings” or “Profile Information”.**
4. The following page will show all the personal information linked to the account such as email address, phone number, gender, and birthday. You can click on each section to edit the information.

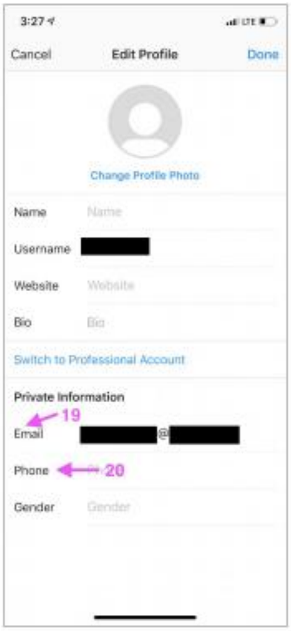


11:26

[redacted]

0 Posts 27 Followers 147 Following

Edit Profile
18
Share Photos and Videos
When you share photos and videos, they'll appear on your profile.
Share your first photo or video



3:27

Cancel Edit Profile Done

Change Profile Photo

Name: Name

Username: [redacted]

Website: Website

Bio: Bio

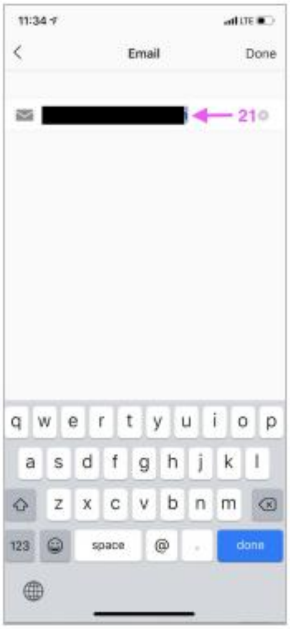
Switch to Professional Account

Private Information

Email: [redacted]@[redacted]

Phone

Gender: Gender



11:34

Email Done

[redacted]

Securing The Account

There are several ways to make your account more private and secure. An option to make your account more secure is changing your password.

1. Go to your **Profile,** the icon on the bottom right (looks like a figure).
2. Click the **Three bars** at the top right of the profile page.
3. Click on **Settings,** scroll, and click on **Security.**
4. Click on **Password.**

It is recommended to use a strong password at least 8-12 characters long and include:

- A mix of both capital and lowercase letters.

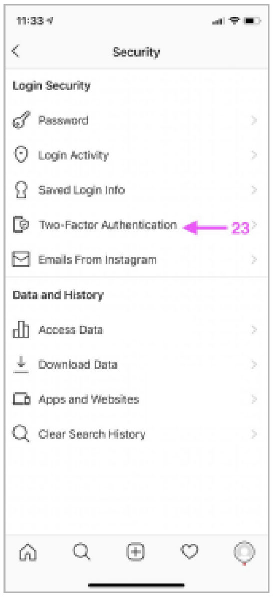
- Some numbers that would be difficult for anyone else to guess -- we recommend avoiding birthdays.
- Some symbols such as !, ?, @, and $

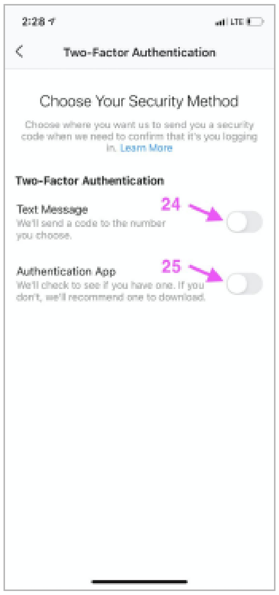
If you do not know your current password, log out by going to **Settings** menu then at the bottom of the screen you can click on **log out** of your account. On the login screen, click on **Forgot Password.**

Two-Factor Authentication

Two-factor authentication is an extra security step that provides more protection for your account. When logging into your account each time, it will request an additional code for you to log into your account. You can choose where this code is sent. It can be through your email or phone number or another application.

1. Go to your **Profile,** the icon on the bottom right (looks like a figure).
2. Click the **Three bars** at the top right of the profile page.
3. Click on **Settings,** scroll and, click on **Security.**
4. Click on **Two-Factor Authentication.**




2:28
LTE
Two-Factor Authentication
Choose Your Security Method

Choose where you want us to send you a security code when we need to confirm that it's you logging in. Learn More

Two-Factor Authentication
Text Message
24

We'll send a code to the number you choose.

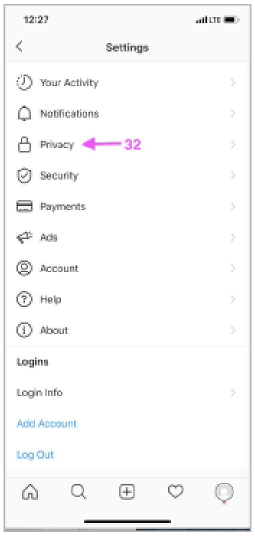
We'll check to see if you have one. If you don't, we'll recommend one to download.

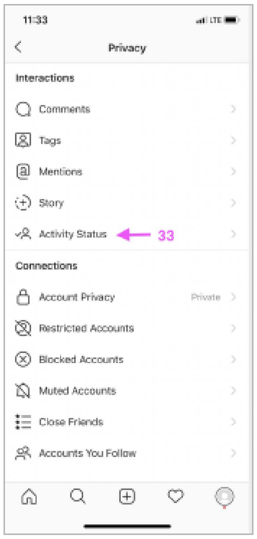
Activity Status & Private Account

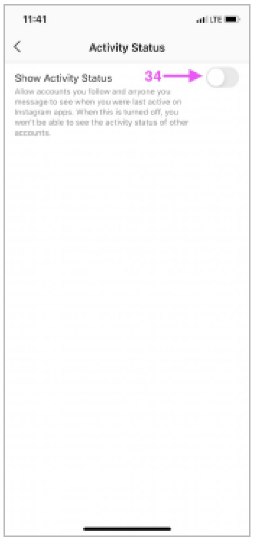
The activity status on Instagram shows when you were last active on the app. When your account is in private mode, your posts will not be shown to the public.

1. Go to your **Profile,** the icon on the bottom right (looks like a figure).
2. Click the **Three bars** at the top right of the profile page.

3. Click on **Settings,** scroll and click on **Privacy.**
4. At the top of the page, you can toggle the **Private Account** setting.
5. On the **Privacy** page, scroll and, click on **Activity Status.**
6. The **Activity Status** page will have an option, **“Show Activity Status”** toggle.

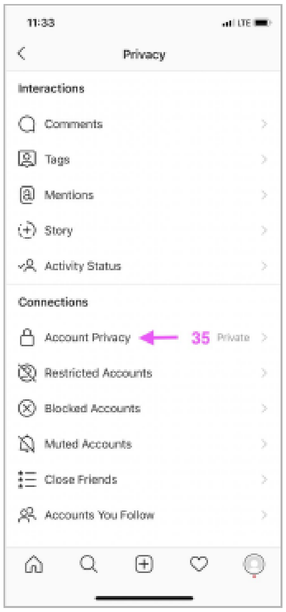


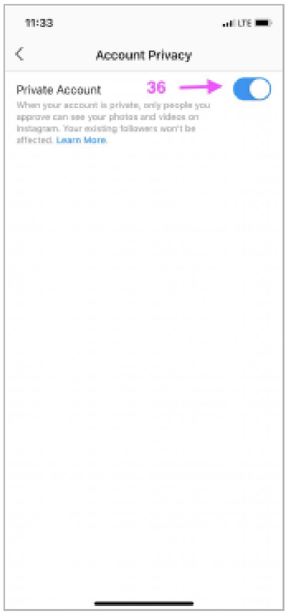




Show Activity Status

Allow accounts you follow and anyone you message to see when you were last active on Instagram apps. When this is turned off, you won't be able to see the activity status of other accounts.





Private Account

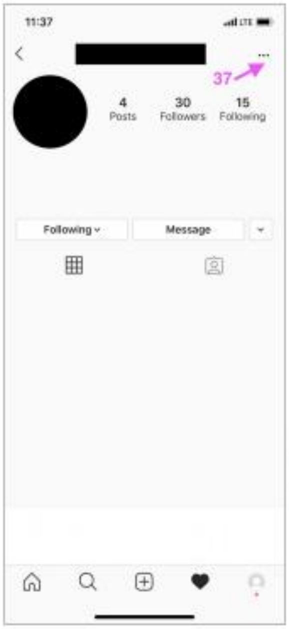
When your account is private, only people you approve can see your photos and videos on Instagram. Your existing followers won't be affected. Learn More.

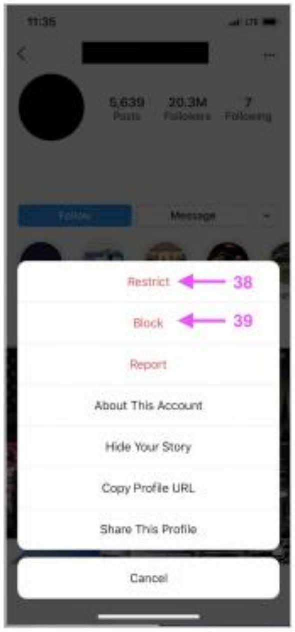
Restricted or Blocking Accounts

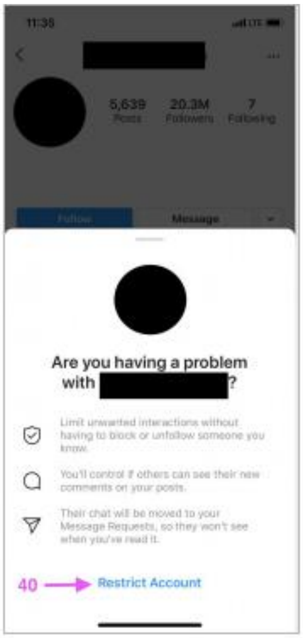
You can stop somebody from viewing your account by restricting or blocking their account.

1. Go to the individual’s **profile** you want to restrict or block.
2. Click on the **three dots** located at the top right corner of their profile.

3. Click on either option (**Restrict or Block)** depending on limit you want the individual to be.
4. When you click on the option then select **Confirm.**





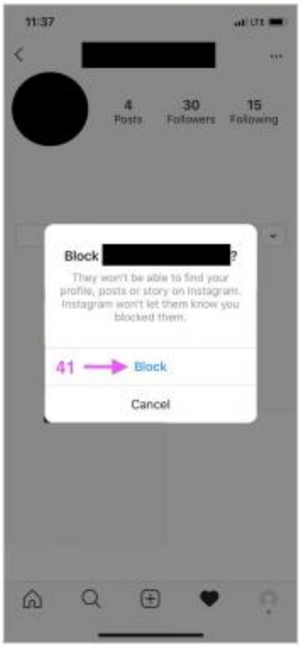


Are you having a problem with [redacted]?

Limit unwanted interactions without having to block or unfollow someone you know.

You'll control if others can see their new comments on your posts.

Their chat will be moved to your Message Requests, so they won't see when you've read it.



Block [redacted]?

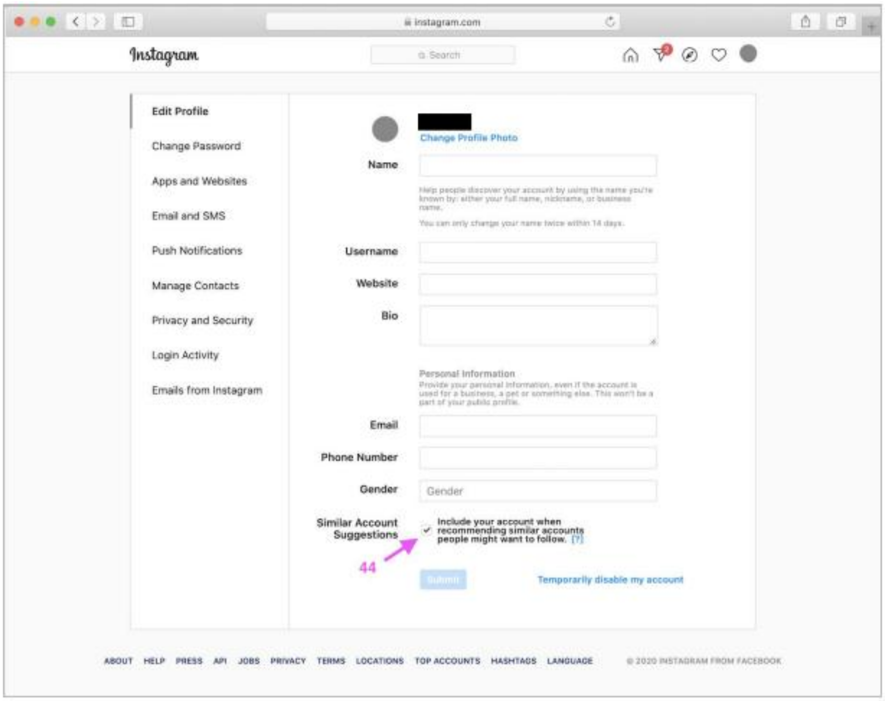
They won't be able to find your profile, posts or story on Instagram. Instagram won't let them know you blocked them.

Prevent Instagram from Recommending Your Account to Other People

This option will include your account when recommending similar accounts to people who you may want to follow.

1. Go to www.instagram.com using a web browser like Safari or Chrome.

2. Go to your **Profile** by clicking the top right profile icon.
3. On the **Profile page,** select **Edit Profile.**
4. At the bottom of the page, there will be an option to **“Show account suggestions on profiles”**. You could uncheck the box if you do not want your account to be recommended to others.



[redacted]

Help people discover your account by using the name you're known by: either your full name, nickname, or business name.

You can only change your name twice within 14 days.

Personal Information

Provide your personal information, even if the account is used for a business, a pet or something else. This won't be a part of your public profile.

Gender

✓ Include your account when recommending similar accounts people might want to follow. [?]

Controlling Tags, Comments, Mentions, and Limits.

There are options allow you to control who you allow tags, comments, and mentions.

1. Go to your **Profile,** the icon on the bottom right (looks like a figure).
2. Click the **Three bars** at the top right of the profile page.
3. Click on **Settings,** scroll and, click on **Privacy.**
4. From the **Privacy Menu**, click on each section (comments, mentions, tags) to edit.
5. There is also a section called **Limits,** when it is turned on it will limit unwanted interactions.

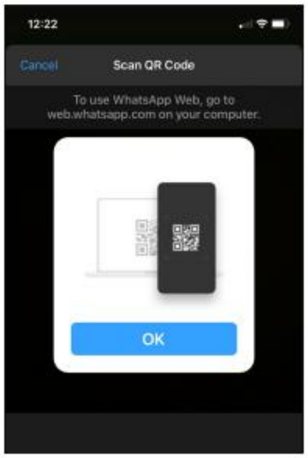
WhatsApp

https://www.ceta.tech.cornell.edu/_files/ugd/c4e6d5_1dc89f5a218041f49b0224d6ace1d218.pdf

This section will focus on enhancing your security and privacy on WhatsApp.

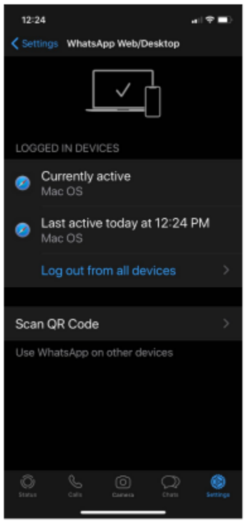
Checking for Logins by Other People and Logouts

1. Go to **Settings** located at the bottom right.
2. Click on **"Linked Devices" or WhatsApp Web/Desktop"**. This will allow users to have access to another device.
3. Go to this website https://web.whatsapp.com and scan the QR shown on the website.
4. You may need to grant access to WhatsApp to use your camera.
5. You will see this popup if no other devices are logged into your account.



To use WhatsApp Web, go to web.whatsapp.com on your computer.

6. If there is another device logged into your account, you will see the following:



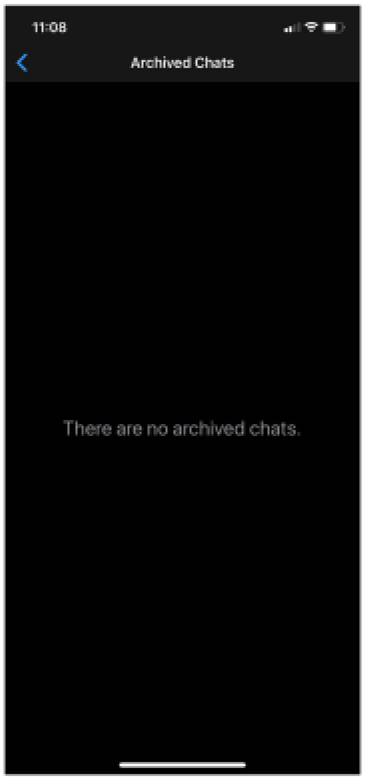
7. You can log out of a device by clicking on the device and then clicking **Logout** or there is an option to **Log out from all devices** shown in the above photo.

Please note by logging out of a device, the abuser may be aware of the actions taken place. Speak with the appropriate organizations to create a safety plan.

<u>Checking Archived Chats</u>

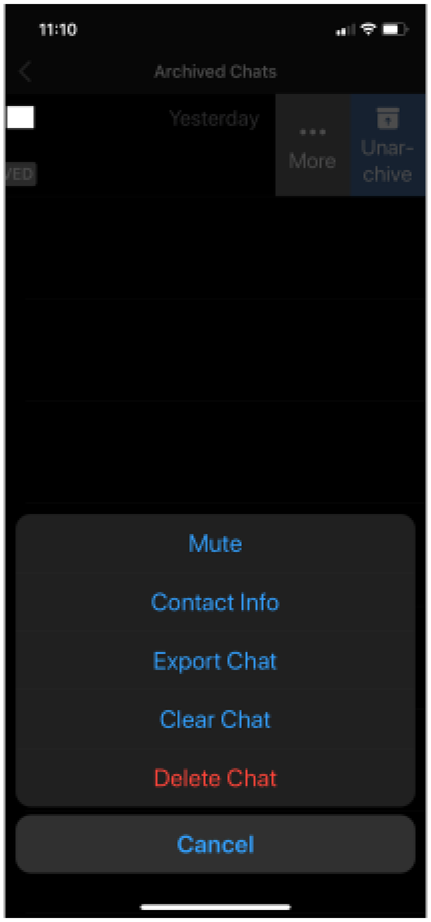
Please note: archiving a chat is not the same as if it was deleted. Chats that are archived are still available within WhatsApp and if your abuser has access to your account, they could see them.

1. Go to WhatsApp.
2. Select **Chats** at the bottom of the screen.
3. Swipe down when you are on the **Chat Page**. The archived Chats option will appear.
4. If you have no archived chats, you will see:



There are no archived chats.

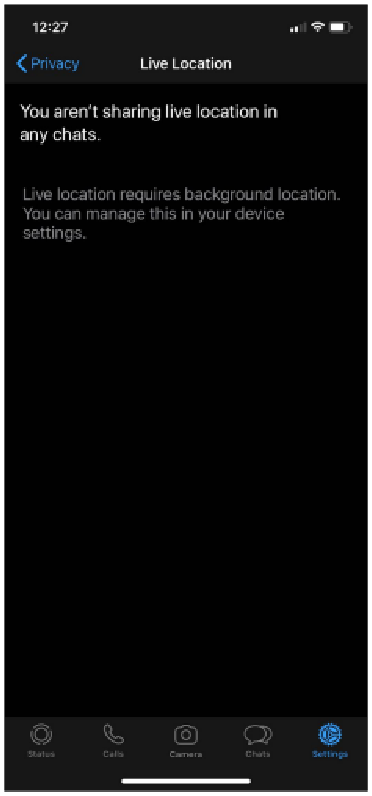
5. If you do have an archived chat, then you can swipe to the left of that chat and unarchive or click **More.**
6. By clicking **More** you can delete, clear, or export chat.



Check if you Share the Location with Anyone.

1. Go to the **Settings** at the bottom right corner.
2. Then **Privacy.**
3. Click on **Live Location**.

If your are not sharing locations with anyone, then you will see:



You aren't sharing live location in any chats.

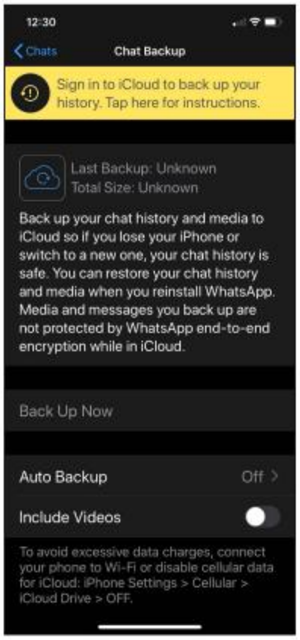
Live location requires background location. You can manage this in your device settings.

How to Check Chat Backup

If you chat is backed up to the iCloud then anyone who gets access to your iCloud account can see your chats.

1. Go to **Settings**.
2. Click on **Chats.**
3. Then click on **Chat Backup**.
4. Click on **Auto Backup**. You will be provided options to turn it off.

If you think an abusive person is receiving information about you through WhatsApp's, then turn this feature off.



Sign in to iCloud to back up your history. Tap here for instructions.

Last Backup: Unknown
Total Size: Unknown

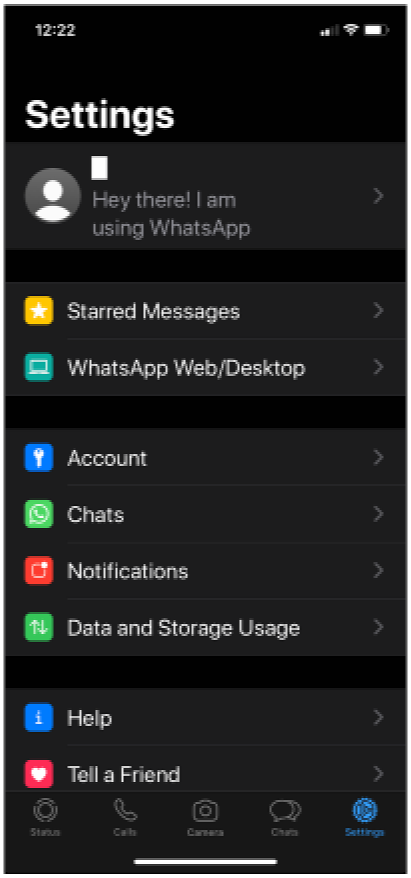
Back up your chat history and media to iCloud so if you lose your iPhone or switch to a new one, your chat history is safe. You can restore your chat history and media when you reinstall WhatsApp. Media and messages you back up are not protected by WhatsApp end-to-end encryption while in iCloud.

To avoid excessive data charges, connect your phone to Wi-Fi or disable cellular data for iCloud: iPhone Settings > Cellular > iCloud Drive > OFF.

Enabling Screen Lock

Using a screen lock will help you keep people out of your WhatsApp since they need your password.

1. Go to **Settings**.
2. Click on **Privacy.**
3. Scroll and click on **Screen Lock.**



12:22

Settings

Hey there! I am using WhatsApp

Starred Messages

WhatsApp Web/Desktop

Account

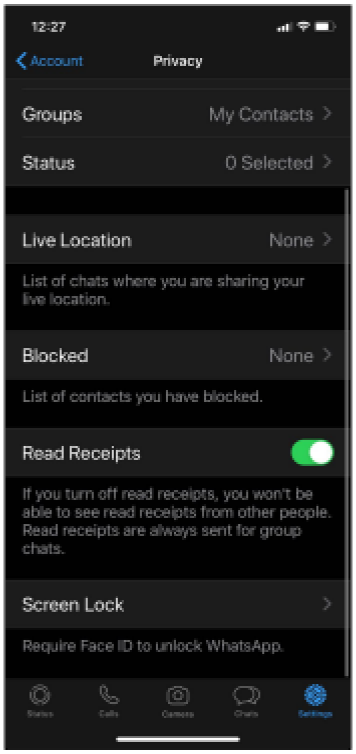
Chats

Notifications

Data and Storage Usage

Help

Tell a Friend



12:27

Account — Privacy

Groups: My Contacts

Status: 0 Selected

Live Location: None

List of chats where you are sharing your live location.

Blocked: None

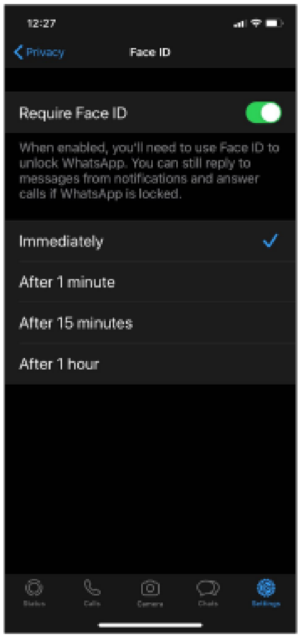
List of contacts you have blocked.

Read Receipts: On

If you turn off read receipts, you won't be able to see read receipts from other people. Read receipts are always sent for group chats.

Screen Lock

Require Face ID to unlock WhatsApp.



12:27

Privacy — Face ID

Require Face ID: On

When enabled, you'll need to use Face ID to unlock WhatsApp. You can still reply to messages from notifications and answer calls if WhatsApp is locked.

Immediately ✓

After 1 minute

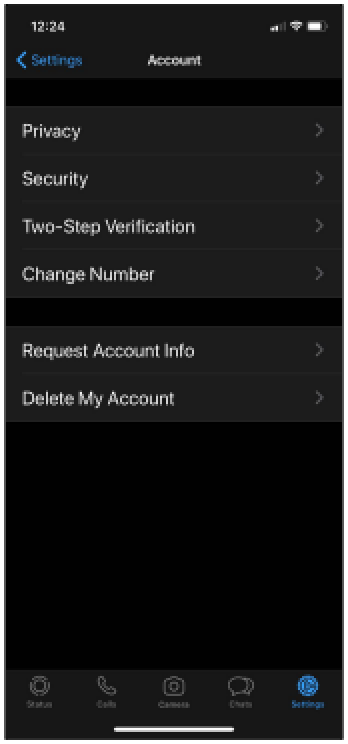
After 15 minutes

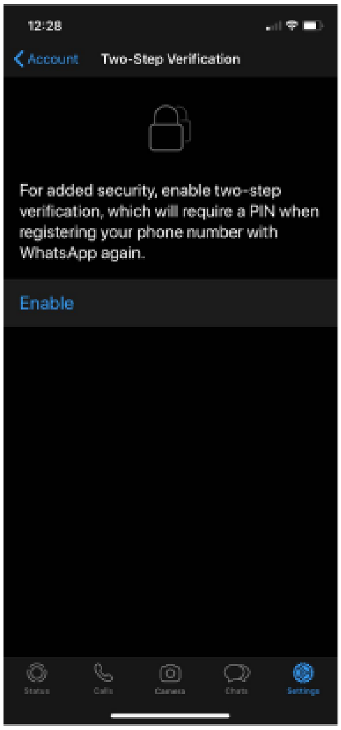
After 1 hour

Turn on Two-Step Verification

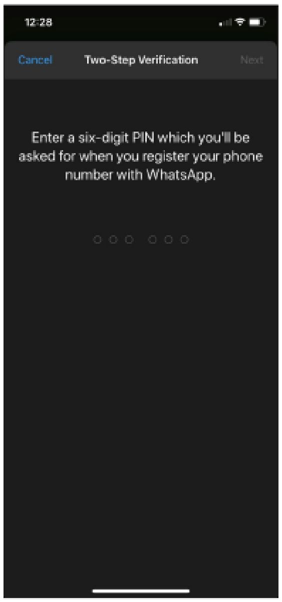
Two-Step Verification will be an additional layer of security for your account. You will need an additional code to gain access to your account.

1. Go to your **Settings** at the bottom right corner.
2. Click on **Account.**
3. Click on **Two-Step Verification.**
4. When activating you will need to enter a 6-digit pin to remember.
5. Confirm your pin then click next. You can enter an email address just in case you forget your pin.





For added security, enable two-step verification, which will require a PIN when registering your phone number with WhatsApp again.



Enter a six-digit PIN which you'll be asked for when you register your phone number with WhatsApp.

○○○ ○○○

Twitter

https://help.twitter.com/en/safety-and-security/twitter-account-compromised

Twitter won't contact you asking for your password. They will also never ask you to download something or sign-in to a non-Twitter website. Never open any attachments or install any software from an email that claims to be from Twitter.

Keep your computer and your web browser updated to help prevent security breaches.

Is your account comprised?

Have you experienced:

- Unexpected tweets created from your account.
- Viewed any unintended messages sent from your account.
- Noticed account behaviors you didn't make or approve (like following, unfollowing, or blocking).
- Received a notification from Twitter explaining that your account may be compromised.
- Received a notification from Twitter explaining that your account information has changed.
- Noticed your password is not working and you are being prompted to reset it.

Ensure your email is secure.

Verify the email attached to your account is your account, it is secure, and you are the only one with access. You can change the email address from the **Account** setting tab.

Update your email address on an iPhone:

1. Click on the **Navigation menu** icon then tap **Settings and Privacy.**
2. Tap **Account.**
3. Tap **Email.**
4. Insert your new email address and tap **Done.**
5. From your email address and click on the **Confirm Now** button from the email sent by Twitter.

Update your email address on an Android:

1. In the top menu, you will see **Navigation Menu** Icon or **Profile** icon. Whichever icon then tap **Settings and Privacy.**
2. Tap **Account.**
3. Tap **Email.**
4. Enter your new email address and click on **Next.**
5. From your email address and click on the **Confirm now** button from the email sent by Twitter.

Update your email address on an Android:

1. Log into Twitter.com and go to **Account Settings** page by clicking the **More** icon then **Settings and Privacy**.
2. Click **Your Account**.
3. Select the **Account Information** and enter your password.
4. Tap **Email.**
5. Insert your new email address and tap **Save.**
6. Go to your email address and click on the **Confirm Now** button from the email sent by Twitter.

Change your password immediately.

Change your password from the **Password** tab in settings. If you are not logged in, you can go to login and click on **Forgot Password**.

Create a strong password.

Do's:

- Create a strong password longer than 10 characters, the longer the better.
- A mix of uppercase/lowercase letters with numbers and symbols.
- Ensure you use a different password for other platforms.
- Keep your password to yourself and if you write it down confirm it is secured.

Don'ts:

- Do not use information including birthdays, phone numbers.
- Do not use common words such as "password".
- Do not use sequences such as "abc123" or key sequences "qwert".
- Do not use the same password on multiple platforms.

Use Two-Factor Authentication

Two-factor authentication is an additional layer of security for your account. When signing into your account you will need an additional code for you to login.

Set up using an iPhone for Text Message:

1. From the main menu, click **Settings and Privacy**.
2. Select **Security and Account Access**.
3. Click **Security.**
4. Tap on **Two-factor authentication**.
5. There will be three methods to choose from: **Text message, Authentication App or Security Key**
6. Click on **Text message.**
7. Read the overview instructions and tap **Get Started**.
8. Enter your password then tap **Verify**.

Set up using an Android for Text Message:

1. From the main menu, you will either see **Navigation Menu** icon or your **Profile** icon. Whichever icon, select **Settings and Privacy**.
2. Select **Security and account access**.
3. Click **Security.**
4. Tap on **Two-factor authentication**.
5. There will be three methods to choose from: **Text message, Authentication App or Security Key**
6. Click on **Text message.**
7. Read the overview instructions and tap **Next.**
8. Enter your password then tap **Verify**.

Set up using a Desktop for Text Message:

1. From the side menu, click **More**, then click **Settings and Privacy**.
2. Click on **Security and account access**.
3. Click **Security.**
4. Tap on **Two-factor authentication**.
5. There will be three methods to choose from: **Text message, Authentication App or Security Key**
6. Click on **Text message.**
7. Read the overview instructions and tap **Next.**
8. Enter your password then tap **Verify**.

References

https://victimsfirst.gc.ca/serv/vrc-dvc.html

https://www.canada.ca/en/public-health/services/mental-health-services/mental-health-get-help.html

https://www.ontario.ca/page/victim-services-ontario#:~:text=Victim%20Services%20Directory%20and%20Support%20Line&text=call%20the%20Victim%20Support%20Line,a.m.%20%E2%80%93%209%20p.m.%20Eastern%20Time

https://cnpea.ca/en/

https://www.casw-acts.ca/en/resources/domestic-violence-resources

https://www.techsafety.org/resources-survivors/technology-safety-plan

https://www.ceta.tech.cornell.edu/_files/ugd/c4e6d5_20fe31daffd74b2fb4b4735d703dad6a.pdf

https://canadianwomen.org/wp-content/uploads/2017/09/CWF-Avon-TipSheet2-EN-web-RevisedJan2017.pdf

https://www.techsafety.org/techmisuse101

https://www.techsafety.org/technology-and-sa

https://www.techsafety.org/image-based-abuse

https://knowledgeflow.org/resource/guide-to-supporting-a-victim-of-sextortion/

https://www.techsafety.org/survivor-toolkit/teens-and-technology

https://www.ceta.tech.cornell.edu/_files/ugd/9e6719_4db0b8e8154844bf84665ad3f04ec6c6.pdf

https://www.ceta.tech.cornell.edu/_files/ugd/9e6719_088a4195809c40a89aec05adcd095a75.pdf

https://www.certosoftware.com/insights/how-a-little-known-iphone-feature-is-opening-the-door-for-cyberstalkers/

https://www.ceta.tech.cornell.edu/_files/ugd/64c5d9_e6cffbcf0b45424da387db3c4b73754a.pdf

https://www.ceta.tech.cornell.edu/_files/ugd/c4e6d5_5229373f1ffa4ea0b8f804269f3038d1.pdf

https://www.ceta.tech.cornell.edu/_files/ugd/c4e6d5_e02acdaedd744b329d04f9516611e15f.pdf

https://www.ceta.tech.cornell.edu/_files/ugd/c4e6d5_01e4e6e33987443ea2244afcd7880706.pdf

https://www.ceta.tech.cornell.edu/_files/ugd/c4e6d5_baf5a1e048714876b9b91a8c638aaf08.pdf

https://www.ceta.tech.cornell.edu/_files/ugd/884c63_d977c4a205d94bf8b919160f67e9ef59.pdf

https://www.ceta.tech.cornell.edu/_files/ugd/c4e6d5_4c8dd35286fe431d9a353a6aafc06f2e.pdf

https://www.ceta.tech.cornell.edu/_files/ugd/c4e6d5_1dc89f5a218041f49b0224d6ace1d218.pdf

https://help.twitter.com/en/safety-and-security/twitter-account-compromised