Tech Disconnect

Compiled by the Clinic to End Tech Abuse

Last Updated: June 16, 2020

We have created a checklist of ways you may still be connected with your ex-partner. These connections may continue to let them get information about your life.

If you have shared an account with your ex-partner, you can delete the account and/or create a new separate account. This would include removing any payment information and identifying information, such as your email address, from the profile of the shared account.

Your ex-partner may realize immediately or quickly if you make these changes. If you are concerned that this will increase any risks to your safety, we recommend that you consult with a case worker at a domestic violence organization or other appropriate support organization beforehand.

You can start by making a list of your shared accounts and a list of every electronic device you own.

Checklist

- ❏ Make a list of your current **devices**, such as phones, laptops, or tablets as well as connected devices, like cameras, thermostats, smart speakers, and smart TVs. Then, think about whether you could be logged into any of your shared accounts on these devices.

- ❏ Make a list of all the **accounts** you have and how you log into each (example: Instagram - registered email: sample@gmail.com). Think about whether your ex-partner might know or be able to guess your password.

- ❏ Think about **signing out** of your accounts on any devices your ex-partner might still be able to get access to. You can also think about changing the password or passcode (PIN) that you use to unlock the device.

- ❏ **Remove any saved passwords** in your web browsers. These are the steps to follow to check the saved passwords you might have in your web browsers:
    - ❏ In **Google Chrome**, go to the following link: chrome://settings/passwords
    - ❏ In **Firefox**, go to the following link: about:preferences#privacy

      Next, scroll down until you reach the **Logins and Passwords** and click on the **Saved Logins** button.
    - ❏ If you have a **Safari** window opened, click on Safari on the top left corner > Preferences > AutoFill > click the Edit button for User names and passwords > Enter your computer's password.
- ❏ Change your **passwords**. Now that you have your list of accounts, you may want to change your passwords to these accounts. A few tips:
    - ❏ A strong password is about 8-12 characters long, uses a mix of capital and lowercase letters, and uses some numbers and symbols (such as $, &, @)
    - ❏ A good password is one that your ex-partner won't be able to guess. We recommend not using your name, any children's or relatives names, or any guessable numbers like birthdays.
    - ❏ If you have to answer security questions to get into your account, we suggest you pick answers that can't be easily guessed.
    - ❏ The following website can help you test the strength of passwords: https://password.kaspersky.com
    - ❏ There are secure password managers that can help you keep track of your passwords, which may be helpful. LastPass is one example of a password manager that you can download from Apple's App Store or Google Play Store.
- ❏ Check your **phone's privacy and security settings**
    - ❏ If you have an iPhone, go to **Settings** and then **Privacy**

      You will see a list of categories, including Microphone and Camera. If you tap on one category, you will see the apps that have permission for that category (for example, apps that have permission to access your

microphone). In this screen, you can stop an app from having permission for a specific activity by tapping on the toggle button -- the one that looks like a switch -- and making sure it turns grey.

- ❏ If your phone is not an iPhone, it is probably an Android. Go to **Settings** > **Lock screen and security**

  Here, you can pick a way to lock your screen (password and PIN are the recommended options). You can also check if **Unknown sources** is disabled (if it is enabled, the installation of apps outside the Google Play Store is allowed, which is a security risk for you).

  To check for the permissions apps have, go to **Settings** > **Applications** and tap on an app. Then, tap on **Permissions**.

- ❏ Check your **phone's location settings**

  - ❏ If you have an iPhone, got to **Settings** > **Privacy** > **Location Services**

    Here, you will see a list of apps that have access to your location information. If you tap on one of them, you can change its location permission. If you decide to let some apps access your location, such as a maps app, we recommend making sure you have changed your passwords for those apps or are logged in with a new, safe account.

    Additionally, we recommend you to check the **Share My Location** option too. By going to **Settings** > **Privacy** > **Location Services** > **Share My Location**, you can check people who can see your location. You can stop sharing your location and -- if you like -- turn off **Find My iPhone** on this screen too.

  - ❏ If you have an Android phone, go to **Settings** > **Location** > **App permission**. If this option is not available, go to **Apps** > **Settings** > **Applications** and tap on an app. Then, tap on **Permissions**. Check if **Location** is enabled.

    For more information, we recommend you to check Google's guide on choosing which apps use your Android phone's location: https://support.google.com/accounts/answer/6179507?hl=en

- ❏ Check your **social media privacy and security settings**

- ❏ Check your **Photos Settings** to make sure you are not sharing your photos with your ex-partner.

    - ❏ If you have an iPhone, go to **Settings** > **Your name (Apple ID)** > **iCloud** > **Photos**. Make sure the **Shared Albums** option is turned off. If you had a shared album, you can remove a subscriber or delete the shared album. To do this, open the Shared Album, then go to the **People** tab. Then, select the subscriber you would like to remove and tap on **Remove Subscriber**. You might want to delete the Shared Album by tapping on **Delete Shared Album**.

      For more information, we recommend you to check Apple's guide on Shared Albums in Photos: https://support.apple.com/en-us/HT202786

    - ❏ If you have an Android phone and have the Google Photos app, we recommend you to check if you are sharing your library with your ex-partner. If you want to stop sharing your library, open your Google Photos app and tap **Sharing**. Next to your ex-partner's name tap **More**. Finally, tap on **Stop sharing your library**.

      If you want to remove a partner, open your Google Photos app, tap on **Sharing** > **Your ex-partners name** > **More** > **Settings** > **Remove partner** > **Remove**.

      For more information, we recommend you to check Google's guide on sharing Google Photos library with a partner: https://support.google.com/photos/answer/7378858?co=GENIE.Platform%3DiOS&hl=en

- ❏ Check your **Google account settings** to see if anyone else is logged into your account. To do this, go to https://myaccount.google.com and enter your email account and password. Then, click on **Security** in the menu on the left. Finally, scroll down until you reach the **Your devices** section, which will show you the devices where you are logged in. You can click on a device to log it out -- just remember that if your ex-partner is logged in on that device, they may realize

immediately that you have done this.

- ❏ Check your **location settings** on other electronic devices like smartwatches, tablets, laptops etc.

- ❏ Check your **privacy settings on web browsers** (see below for instructions) Clearing the cookies, which are IDs that identify you while you navigate on the Internet, on your browser (for “all time”) should log you out of all active sessions.

- ❏ You may want to set up **two-factor authentication** for all your accounts. This is an extra security step that provides more protection for an online account. By turning it on, every time you want to log into your account, you will first enter your password -- as usual -- and then a second piece of information such as a code, which you will receive via text message or an app such as Duo.

    - ❏ If you turn on two-factor authentication in any account, you should see a guide to next steps.

- ❏ **Backups** allow you to keep a copy of your data in the cloud -- but this can also make your information visible to your ex-partner if they know your sign-in ID and password. Have you set up backups for any information from your device, such as photos or notes? If you have set up a backup, check the email address that is registered and where the data is being backed up to.

  For example, If you have an iPhone, go to **Settings** > **Photos**. If the **iCloud Photos** option is enabled, your phone will automatically send your photos to the iCloud account registered on your phone. Does your ex-partner have access to this account, or might they be able to guess your password?

- ❏ Check all of the apps on your devices to make sure that you recognize them. You should be able to delete any apps you don’t recognize.

- ❏ If you are concerned that your children’s devices may have also been accessed by your ex-partner, we suggest that you follow these same steps for those devices.

How-to guide to the checklist:

- ❑ **Check your phone's location settings**

  If you have an **Android** phone, you will be able to follow one of the following paths (they vary due to Android versions and phone manufacturers):

  - ❑ Open **Settings**, tap **Location**, tap **App permission**, and then review the apps that have access.
  - ❑ Open **Settings**, tap **Biometrics and security**, tap **App permissions**, and tap **Location**

  If you have an **iPhone**, open **Settings**, tap **Privacy**, and then tap **Location Services**. First, we recommend you to tap on **Share My Location**, and then turn off **Find My iPhone** and disable **Share My Location**.

  Second, in **Settings** > **Privacy** > **Location Services**, you will see a list of apps and their location access ("never," "ask next time," or "while using the app"). Review this list and make all necessary changes so that apps do not track your location every time.

  Third, scroll down until you reach the end of the list of apps. Tap on **System Services**, and then tap on **Significant Location***s* (near the bottom). Turn off **Significant Locations** and tap on **Clear History**.

- ❑ **Check your privacy settings on web browsers**

  Google Chrome

  (1) Open Google Chrome. Click on the **three dots** at the top right corner, click on **Settings**, and select **Extensions**. Review the list of installed browser extensions. Remove any extensions you don't recognize or use, as well as those that track your location. You can check the details of a specific extension by clicking on **Details**. To remove an extension, click on **Remove**.

  (2) Open Google Chrome. Click on the **three dots** at the top right corner, click on **Settings**, and select **Privacy and security**. Clear all your browsing data using the **Clear browsing data** option. Also, check websites'

permissions, specially **Location permissions**, using the **Site Settings** option.

(3) Open Google Chrome. Click on the **three dots** at the top right corner, click on **Settings**, and select **About Chrome**. Make sure your browser is up to date.

Additional Accounts

Many people share different types of accounts that can provide information about your day-to-day activities. We have made a list of accounts you may have shared with your ex-partner. You can check and disconnect from any shared accounts.

Categories

(1) Food

- ❏ Seamless
- ❏ Grubhub
- ❏ Restaurants
- ❏ Uber Eats
- ❏ DoorDash
- ❏ Caviar
- ❏ Postmates

(2) Music

- ❏ Spotify
- ❏ Pandora
- ❏ Apple Music

(3) Smart speakers

- ❏ Amazon Echo (Echo Show, Echo Dot, etc..)
- ❏ Google Home

(4) Banking and financial

- ❏ Online banking
- ❏ Venmo
- ❏ Paypal
- ❏ Stocks
- ❏ Retirement accounts
- ❏ Venmo
- ❏ Paypal
- ❏ Investment and other financial accounts
- ❏ Cash App
- ❏ Credit cards

(5) Phone

- ❏ Shared family plan

(6) Car

- ❏ GPS in car
- ❏ Apps for car

- ❏ Waze

(7) Home Technology

- ❏ Ring
- ❏ Nest
- ❏ Camera(s)
- ❏ Alarm system
- ❏ Hue
- ❏ Smart door locks
- ❏ Wemo

(8) Television

- ❏ Netflix
- ❏ Hulu
- ❏ Disney+
- ❏ Amazon Prime Video
- ❏ Apple TV

(9) Shared car rides

- ❏ Uber
- ❏ Lyft
- ❏ Via

(10) Traveling

- ❏ Booking
- ❏ Airbnb
- ❏ Trivago
- ❏ Tripadvisor
- ❏ Airlines

(11) Utilities

- ❏ Cable/Internet
- ❏ Water
- ❏ Gas

(12) Workout apps

- ❏ Strava
- ❏ Garmin
- ❏ MapMyRun

(13) Cloud storage

- ❏ Dropbox
- ❏ Box
- ❏ Amazon Drive
- ❏ Google Drive