Is Your Personal Information Easily Found By Criminals?

July 31, 2024

HOW THEY FIND IT AND WHAT YOU CAN DO TO STOP IT.

By Peter James

Crime is changing as we know it.

In today's digital world, your personal information is incredibly valuable, especially as Law Enforcement Officers. Here's why:

I talk to hundreds of officers monthly and hear the same thing: *"Why would anybody want my data? I'm not that valuable."*

That's incorrect. It's simply not true. For example, Facebook says you're worth $700/year.*

That's just one site. What about the hundreds of other sites?

And what about when **some of these sites are actually dangerous…**

You see, criminals are using this same data to harm officers and their families at their homes.

Let's talk about how this happens and what you can do to fix it.

The New Currency

Data brokers, companies that collect and sell data, are at the heart of this. They gather your information from various sources ***(often without your knowledge)***and then sell it to other businesses. This data has become the new currency (sorry, crypto).

The data being sold is personal information – your home address, phone number, email address, name of relatives, and much more.

Here's the problem: Many of the 'buyers' are websites that show that data online, free, for everyone to see.

For most people, this may be a minor inconvenience. ***For law enforcement officers, this puts them and their families in danger.***

As we know, there is a huge lack of respect toward law enforcement officers in the country right now. So, if any criminals can easily find an officer's home address online, this is downright dangerous. What's worse is that officers all over the country are being harassed and doxed. At their homes. All because their data is easily accessible online.

And all of this is preventable.

Let's explore how this happens and what you can do to protect yourself.

How Data Brokers Get Your Information

Data brokers collect your personal information from a variety of sources, including:

1. Other Big Businesses – When you make a purchase (in-store and online), your data is sold. When you get a package delivered to your home, your data is sold. When you get a credit card statement, your data is sold. Because of how valuable your data is, companies are realizing they can make more money from your data than their core business model.

2. Loyalty Programs, Surveys, and Contests – When you sign up for a grocery store rewards program, they sell your data to other businesses. The same thing goes for those casino loyalty programs. And don't forget about free surveys and contests – it's all sold to the highest bidder.

3. Social Media – Anything you share on social media can and will be used against you (and sold). Keep in mind, it's not only what you post… Your Facebook is analyzed to identify your family members. Your Instagram is searched for what posts you like and where you spend your time. Your LinkedIn shows where you work.

Every little data point is being used against you. Everything. Let's see what happens after they have your data.

What Happens Next

And just like that, these big companies have thousands of data points on you. They sell this data to data brokers.

Data brokers then build an online profile for you.

Unlike social media, you have ZERO control over this profile. The power lies in the hands of the data brokers who stole your information to begin with.

Because they *legally* have your information, they can post it online. And they do.

When it's online, anyone can find it, including criminals and crazies.

Now, there are steps you can take to stop this.

How You Can Stop It

As officers, there are some small adjustments you can make to make a huge impact on your online privacy and stop this cycle.

There are two steps to solving this:

First, we must **find and fix** where you're currently exposed.

Then, we need to ensure it doesn't happen again in the future.

Let's dive in on the first step.

1. Search and Find Your Data – Perform an online search to find which of your personal information is currently exposed. We recently found that 98% of officers' home addresses are listed online. If you're in the 98%, we need to find where it's posted online and remove it quickly. OfficerPrivacy.com has created a simple and easy way to search for what's online with the free PrivacyCheck Tool. In less than one minute, you can see about 30% of what's available about you online.

2. Internet Purging – Internet Purging is where you reduce your online presence to be less identifiable. For officers, the best place to start is with data broker sites. Data brokers allow you to opt out of their databases. But remember, this is how they make billions of dollars every year, so they don't make it easy. This process can be time-consuming, but it's worth the investment to protect your privacy.

3. Monitor Your Online Presence – Once you're fully removed, regularly search for your data online to see what's available about you. This can help you catch and address any exposed personal information early. Once officers are removed from the online sites, we find they are relisted on 3-5 sites every 90 days. That's why it's important to stay on top of this. One simple way to monitor is to utilize Google Alerts. You simply enter the information you are looking for. Anytime Google finds something, it sends you an email with what it found. It's simple and effective. Consider OfficerPrivacy, as we do all of this work for you.

Now that you removed your information, it's time to move on to step two: prevent this from happening again.

Preferred Names – Data brokers connect you and your home address. Make every attempt to break that connection by using a 'preferred name', also known as an alias. Plus, you can use an alternate address, like a Post Office box, for even more security.

Be Aware of What You Post – Social media is one source, but not the only source, of information. Limiting what you share on social media is important, but it will not stop your data from being collected and sold by other sources. Lock down your privacy settings to restrict who can see your posts and personal details.

Wanting to protect your privacy doesn't mean you are trying to hide any wrongdoing. This is about protecting you and your family from the unstable and hateful people out there. They want to harm you and your family, so it's only smart to protect yourself.

Take a couple of easy steps to protect yourself and your family – it's worth a small investment to enjoy peace of mind.

About the author:

Pete James is the Founder of OfficerPrivacy.com, an LEO-owned and staffed company. Offering free and paid services, they help remove law enforcement officers' private information from the internet.

* https://proton.me/blog/what-is-your-data-worth

How to Hide / Blur Your Home on Google Maps & Apple Maps

If you're creeped out or bothered by the Street View cameras for Google Maps and Apple Maps taking pictures of your house, you can request for Google Maps or Apple Maps to hide, blur, and censor the address. When the request has been approved, the home address gets pixelated or blurred, effectively blocking any identifying imagery of the house.

How to Hide / Blur Home on Google Maps

Here's how you can censor your home address on Google Maps:

1. Go to Google Maps at maps.google.com
2. Enter your Home Address, then enter into Street View by dragging the little yellow person icon from the corner of the screen into the street
3. Locate your house by 'driving' to it with Street View
4. Click on "Report a problem" text in the bottom right corner

5. At the ‘Maps Report Inappropriate Street View’ screen, choose that you wish to blur your home and provide the home address
6. Fill in your email address and submit the request

When the request has been fulfilled, the home will be blurred and not visible on Street View.

These are the official instructions from Google support, and they do fulfill the requests.

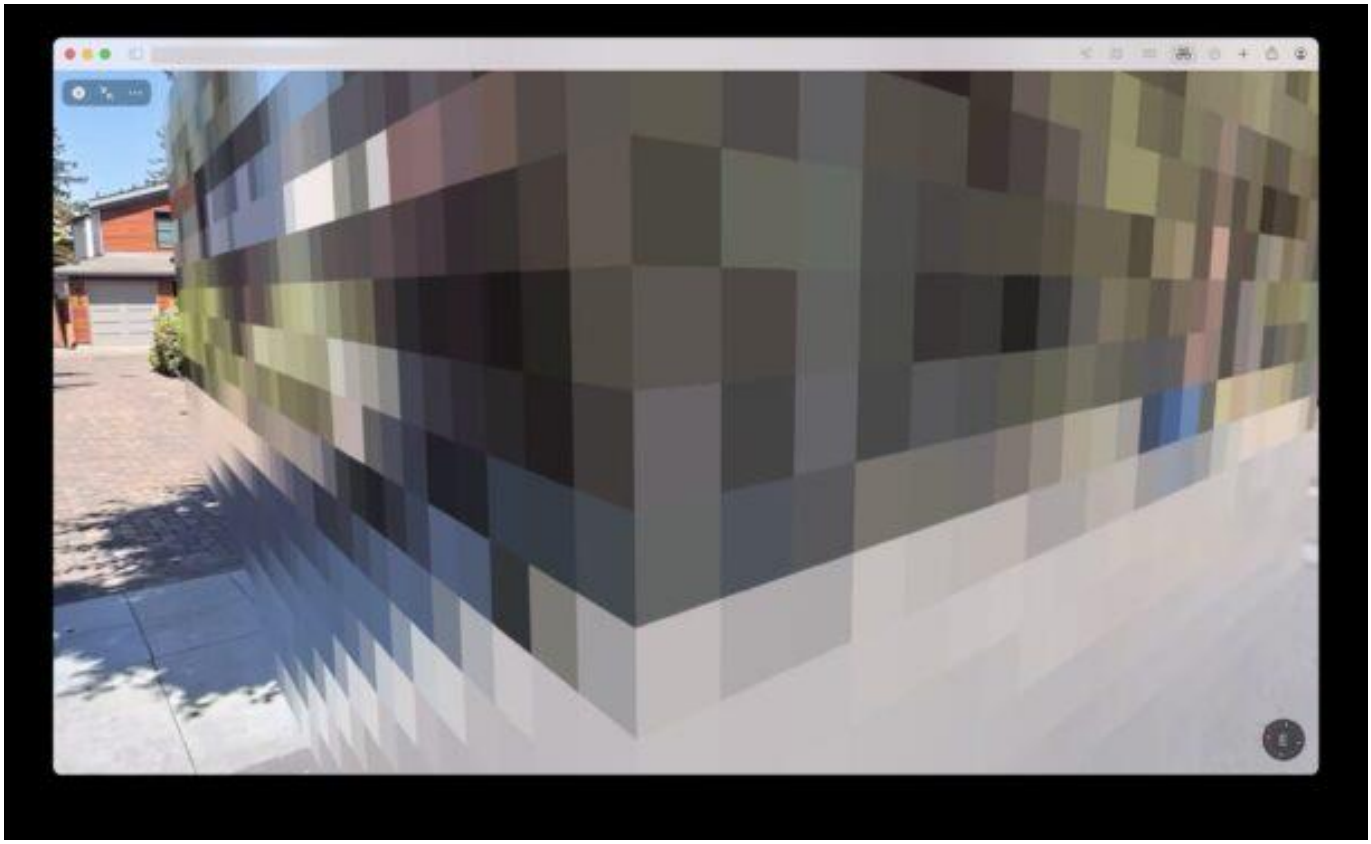
Note that blurring an address is permanent, and there does not appear to be a way to undo the blur.

You can also request to blur a face, car, or license plate on a car, but for our purposes here we are focused on blurring and hiding the home address.

How to Hide / Blur Home on Apple Maps

Blurring and censoring a home address on Apple Maps is done through email:

1. Send an email to MapsImageCollection@apple.com and request to censor and hide your home, provide the home address and any other information they'd need to locate the property



The Apple Maps approach is a little different requiring the email directly to Apple, and the Apple home censoring is a little more complex too, forming a large pixelated wall.

You can get more information about the process and image collection behavior of Apple Maps from Apple if interested.

Whether you're censoring your home address and home imagery through Google Maps or Apple Maps, or both of them, is up to you as the home resident.

This is an interesting capability that is probably mostly used by celebrities, executives, political figures, and others, but since it's open to everyone, anyone can blur their address if you'd like to.

Thanks to CultofMac for pointing this capability out in an article about Apple CEO Tim Cook, and how his house was hidden on both the Google Maps and Apple Maps services by using this feature. So, why not get the same digital security and privacy as Tim Cook? Blur your own house if you feel like it.

You Should Probably Blur Your House on Google Maps. Here's Why

It's a matter of privacy.

When I was a kid, my parents used those Thomas Guides street maps to navigate us around Los Angeles and Orange County. My dad would drive, while my mom would flip through the spiral-bound book and yell out exactly where to turn to get us to our destination.

Now, we all have Google Maps on our smartphones. It's so much more convenient to get directions from the palm of our hands, but as is the case with technology sometimes, there are certain aspects of it that can be a bit invasive of our privacy.

If you've ever used Street View, you know that you can enter almost any address into Google Maps and look at a recent image of that location, whether it's a business, government land or a residence. And it's useful for knowing what building or landmark to look for when you arrive, but this same feature also makes it easier for stalkers or criminals to plan their way inside your home.

Street View gives anyone a free ticket to examine your home on the internet -- maybe they want to look for any cameras or even find a side window to pry open. And sure, anyone can walk or drive by your home and do this in person, but Google Maps makes this process much simpler. Anyone with a phone or computer can do it.**How to blur your home on Google Maps**

You'll need to do this on your computer, as the blurring feature isn't available in the Google Maps application on iOS or Android, and while it is accessible through the web browser on your mobile device, it's rather difficult to use, so use a trusted web browser on your Mac or PC instead.

At maps.google.com, enter your home address in the search bar at the top-right, hit return, then click the photo of your home that appears.

Click on the photo of your home, right above your address, on the top-left part of the page.

Next, you'll see the Street View of your location. Click **Report a Problem** at the bottom-right. The text is super tiny, but it's there.

This is the Street View of your location.

Now, it's up to you to choose what you want Google to blur. Using your mouse, adjust the view of the image so that your home and anything else you want to blur is all contained within the red and black box. Use your cursor to move around and the plus and minus buttons to zoom in and out, respectively.

If you want to blur more than what's in the black/red box, use the + button to zoom in.

Once you're finished adjusting the image, choose what you're requesting to blur underneath:

- A face
- Your home
- Your car/license plate
- A different object

You'll be asked to give a bit more detail as to what exactly you want blurred, in case the image is busy with several cars, people and other objects.

Also, be completely sure that what you select is exactly what you want blurred. Google mentions that once you blur something on Street View, it's blurred permanently.

Finally, enter your email (this is required), verify the captcha (if needed) and click **Submit**.

You're required to provide additional information about what you want to blur, so be thorough.

You should then receive an email from Google that says it'll review your report and get back to you once the request is either denied or approved. You may receive more emails from Google asking for more information regarding your request. Google doesn't offer any information on how long your request will take to process, so just keep an eye out for any further emails.

The internet stole your privacy.
It's time to take it back.

25 Rarely Used Privacy Tricks

You'll Want To Do Today!

www.OfficerPrivacy.com

Table of Contents

Digital Privacy

Today, digital privacy is more important than ever before. With data being available at anyone's fingertips and growing hostility toward law enforcement, taking back your online privacy is critical. I want to share with you five concepts to start you down the path of becoming more private in your digital life.

Remove your personal information from the internet. This will make it more difficult for dangerous people to find you and hurt you or your family.

Secure your credit by freezing your credit accounts. This will make it more difficult for dangerous people to ruin your credit.

Secure your digital accounts and add an extra security feature. This will make it more difficult for dangerous people to hack your accounts, steal your money, or ruin your reputation.

Lock down your social media. This will make it more difficult for dangerous people to learn about you and your family.

Learn what social media corporations, primarily Facebook and Google, know about you. This will make you a more educated consumer and help you decide if you are comfortable sharing your information with them.

Who Am I & What's This About?

LinkedIn

I'm Pete James, and I retired after 25 years with a large law enforcement agency in California. My specialty is digital forensics and investigations.

I started OfficerPrivacy.com because I felt LEOs deserve privacy, but there wasn't anyone solving this growing problem.

Several years ago I decided to remove my information from sites that showed my home address and it took me over 6 hours. I didn't know where to start, where all the links were, and if it really worked. With all of this, I became frustrated. Then I realized, I had no way to monitor the sites when my information reappeared.

I created a system where I could make the process faster. Then I hired a programmer who made it even easier. What we have today is the result of years of effort. My goal is to help officers remove their personal information from these sites, so I make my software FREE. Yes, free, for 14 days. Most clients using our software can remove themselves from the top 50 people-search sites in about an hour!

If you need access for a longer period of time, I charge a minimal fee that helps offset the costs of keeping the software updated. If you need help, we offer a Premium service where our staff of current and former US law enforcement officers will remove your information for you, then monitor those sites. If you reappear, we remove your information again.

In this eBook, I've compiled what I consider to be 25 essential techniques you should practice to help you become more private and secure.

We hope you enjoy this eBook and take the steps explained. If you have any questions or comments, send me an email at ebook@OfficerPrivacy.com.

DON'T GIVE YOUR HOME ADDRESS TO CRIMINALS

Did you agree to have your home address published online?

Google your name, the city you live in, and the word "address" and you'll be surprised at what you see. People-search sites like WhitePages, Spokeo, and BeenVerified expose your personal information, including your home address, phone number, email, and names of relatives.

Removing yourself from these sites is a worthwhile investment.

It can take up to a month for your information to actually disappear from these sites. The earlier you start, the earlier you will enjoy an extra layer of protection.

"I'm a customer of OfficerPrivacy.com and I feel a lot safer. It's a great company, I'd recommend it for any police officer."

Scott Medlin, Police Officer and author of Mental Health Fight Of The Heroes In Blue.

Based on web traffic, here are top sites exposing your home address:

- WhitePages.com
- Spokeo.com
- BeenVerified.com
- TruthFinder.com
- FastPeopleSearch.com

You should also check for your information using a Google search. Don't just enter your name and city. Use these tips to get better results:

Use quotes around your name and separate quotes around your address.

"First name Last name" "Street Name" YourCity address

For example, if your name is Robert Doe and you live on Maple Street in Chicago, enter this: "Robert Doe" "Maple" Chicago address

And search this: "Robert Doe" "Chicago IL" "address"

Identify the sites that are showing your address and start removing your information from them.

If you need a little assistance, check out the resources I offer:

OfficerPrivacy.com offers two types of service:

- Access to OfficerPrivacy.com software so you can quickly remove yourself and your family from the top 50 people-search sites. We offer FREE access to our software for 14 days. This is Option 1 on the website.

- Premium Service where OfficerPrivacy.com's staff of current and former US law enforcement officers remove you from the top 50 people-search sites. The Premium Service includes monitoring these sites for reappearance. If you reappear, we remove your information again. This is Option 2 on the website.

"Privacy is one of our biggest issues right now with the threats toward law enforcement increasing every day, with officers being doxed and tracked down and harassed, you have got to protect yourself. The only way is OfficerPrivacy.com." Lt. Randy Sutton, Las Vegas PD (Ret) Host of Blue Lives Radio

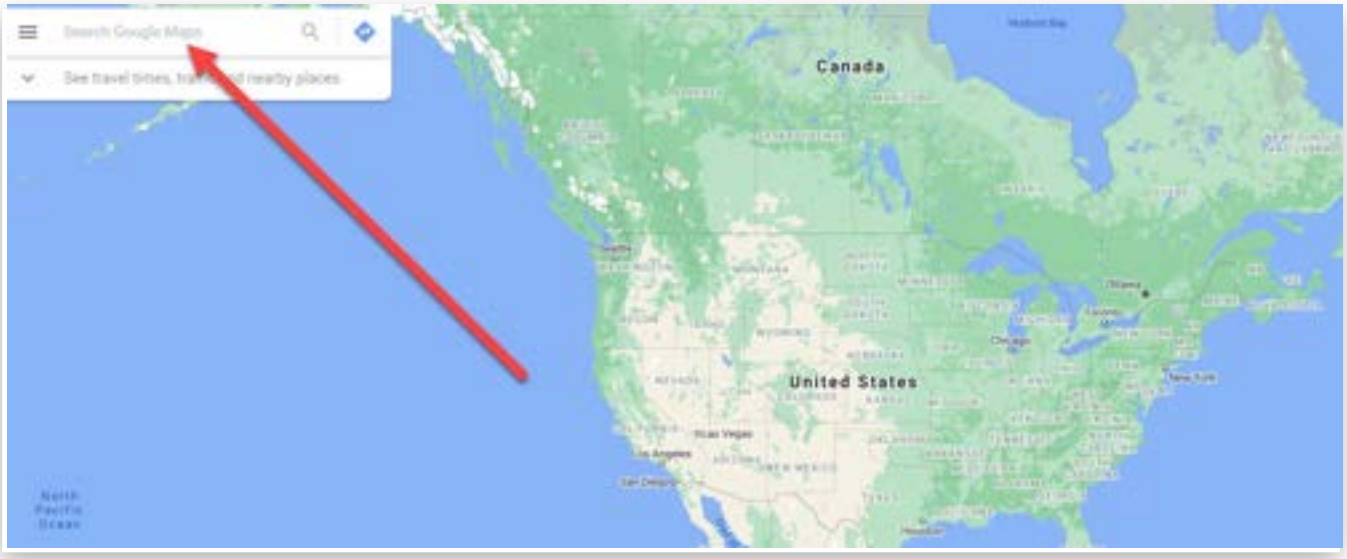
House Picture Blur Requests

A picture of your house is likely on several mapping websites. These pictures may include you, members of your family, your vehicles, or other potentially identifying information (items that would indicate children or hobbies, etc.).

These instructions will explain how to remove images of your house from Google Maps Street View, Bing Maps Streetside, and Apple Maps Look Around.

Google Maps

1. Go to google.com/maps and in the Search Google Maps box enter your address and press Enter.



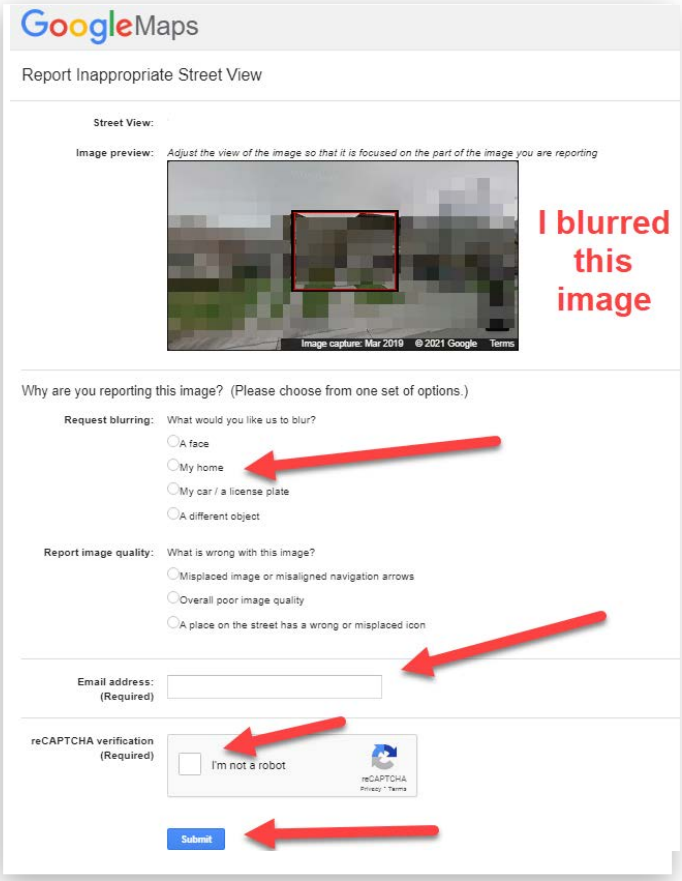
2. In the lower right corner, press the orange figure. This will show you the streets Street View has photographed.

3 Some streets are marked turquoise, others are not. If they are turquoise, they have been photographed. If not, there is no Street View imagery and there is nothing for you to remove.

4 If the street in front of your house has been photographed, click on the line in front of your house. You may need to move the image with your mouse to get a clear view of your house.

When you have a view of the front of your house, click in the lower left corner of the image "Report a problem."

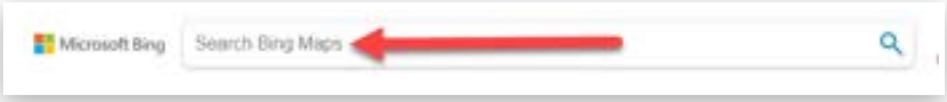
5 You will be taken to the following page where you should adjust the box to show the front of your house, select My home, enter your email address, complete the captcha, and press Submit.



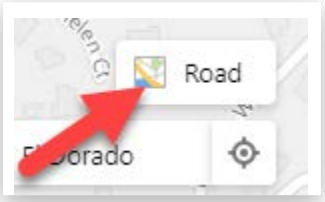
6 When you click on My home, the button will expand. Enter your address in this box.

Bing Maps / Streetside

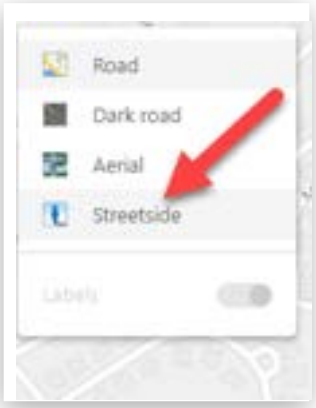
1 Go to bing.com/maps and search for your home address.



2 In the upper right side of the map is the icon Road.



3 Hover or click over Road and a drop down will appear. Select Streetside.



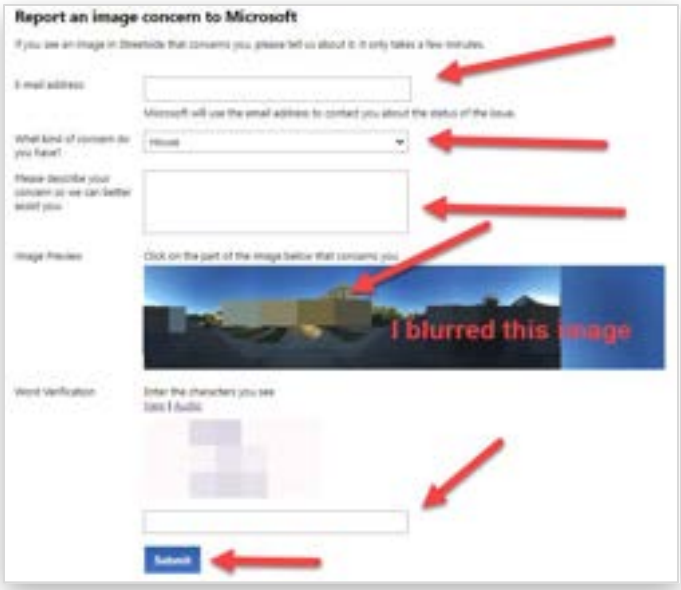
4 You will now see that some streets are shaded blue and some are white. If the street is shaded blue, your home has been photographed. If it is white, it has not been photographed.

5 If your house has been photographed, double-click on the street in front of your house.

You may need to use your mouse to navigate to look directly at your house. In the lower left corner of the picture, click on “Report a privacy concern with this image.”

6 You will be taken to this page.

Select House, and explain why you do not want your house on Bing StreetSide.



Apple Look Around

On your iPhone open Maps. If you don't have an iPhone, ask a friend to search for you.

Search your home address to determine if your house is shown.

If it is, send an email to:

mapsimagecollection@apple.com

Use the subject line below (or something similar):

Look Around Removal Request

Your text should be as below or something similar:

I am being stalked and harassed and believe having my home visible on Look Around increases the threat of harm to me.

Please remove all images of my home from Look Around and any other platform you have or control.

Thank you.

You need to tell them who you are and your home address.

You will receive a confirmation email from Apple.

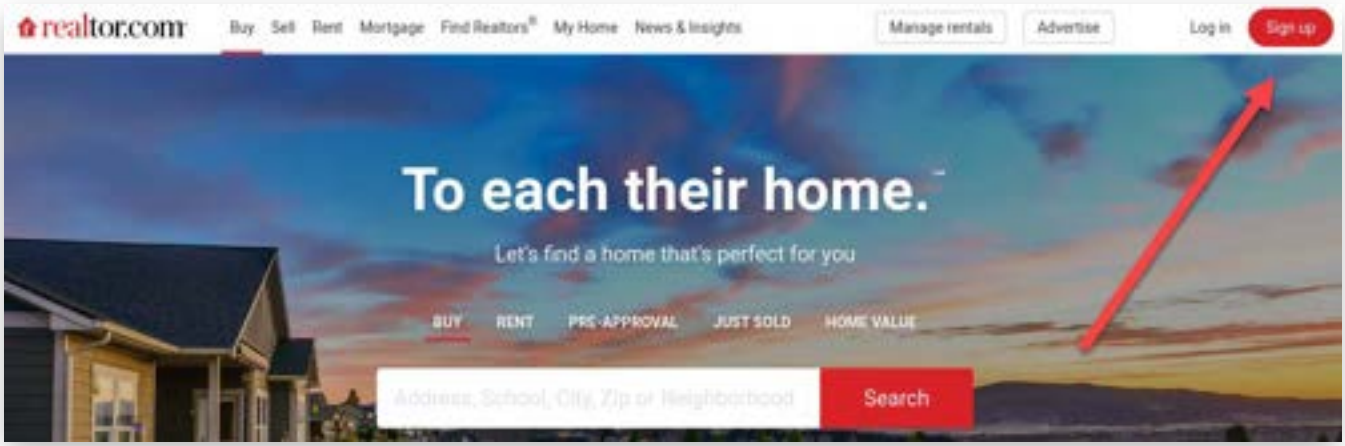
Check back a few days later to make certain your home is no longer showing on Look Around.

How to remove pictures of your home from real estate websites

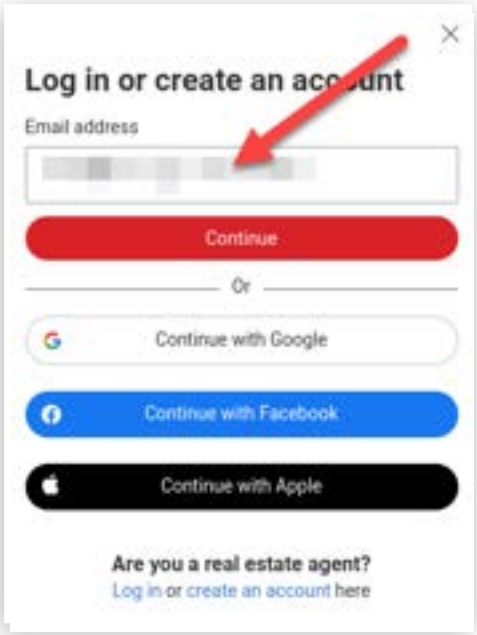
Realtor websites show the outside and inside of your house. The pictures of the inside of your house are probably from the people who owned the house before you, but if you are not comfortable with this, you can remove them by following these instructions:

Realtor.com

1 **Go to Realtor.com and select Sign Up (unless you already have an account).**

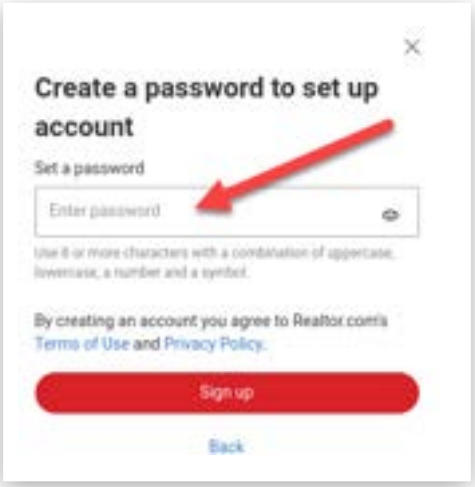


2 **Enter your email to create an account. I would create a unique email account just for the sites you are opting out of.**



3

Create a password.

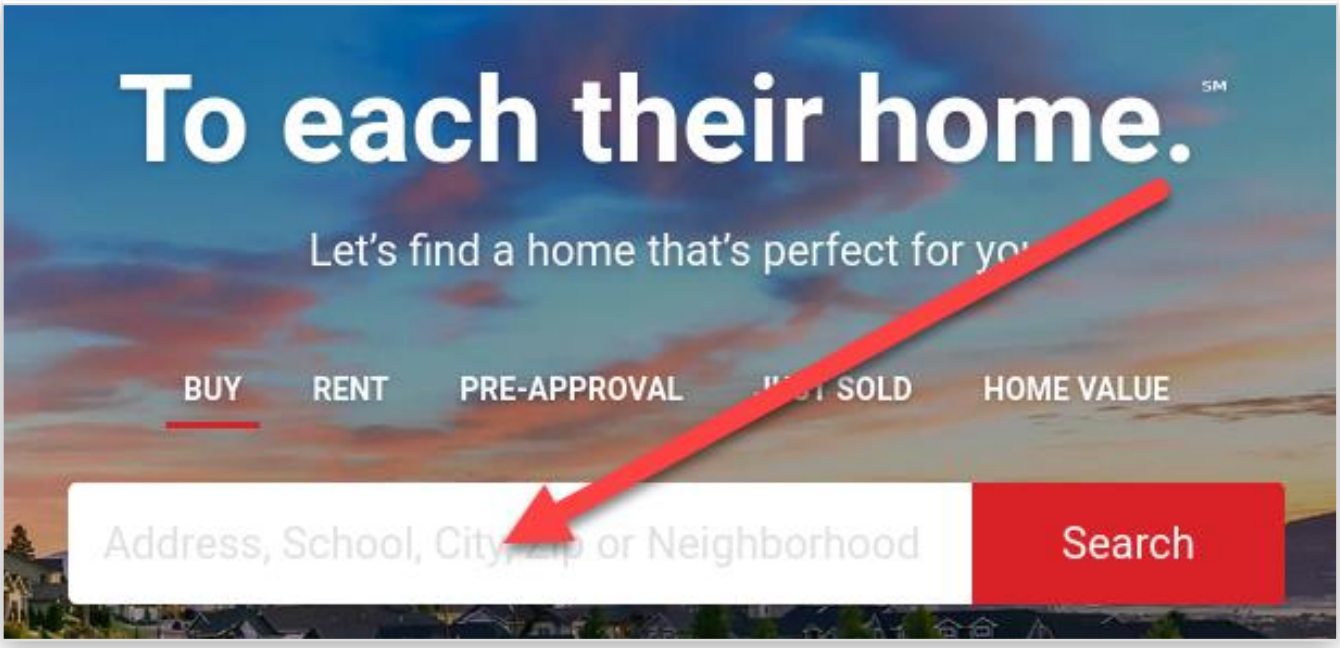


4

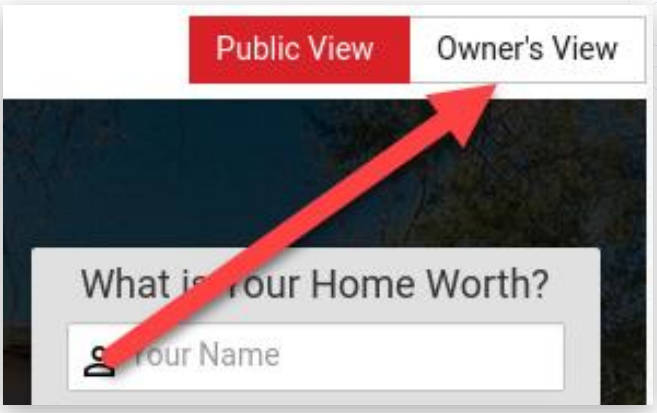
Select No, thanks.

5

Enter your home address.

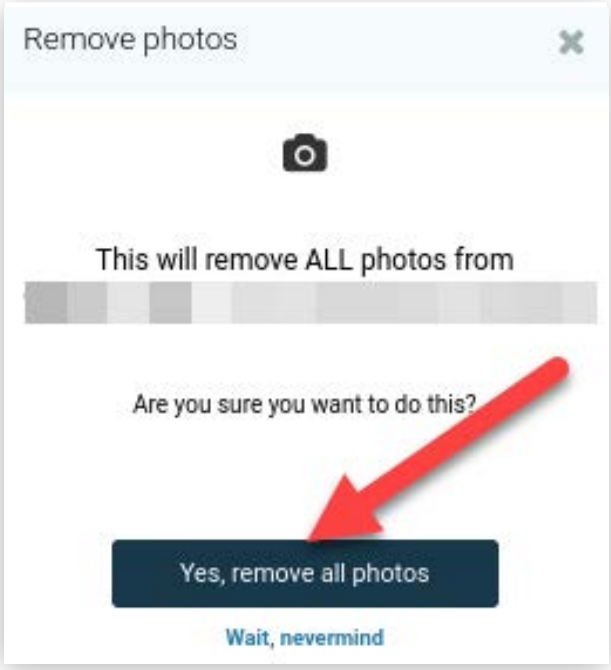


6 **In the upper right corner, click Owner's View.**

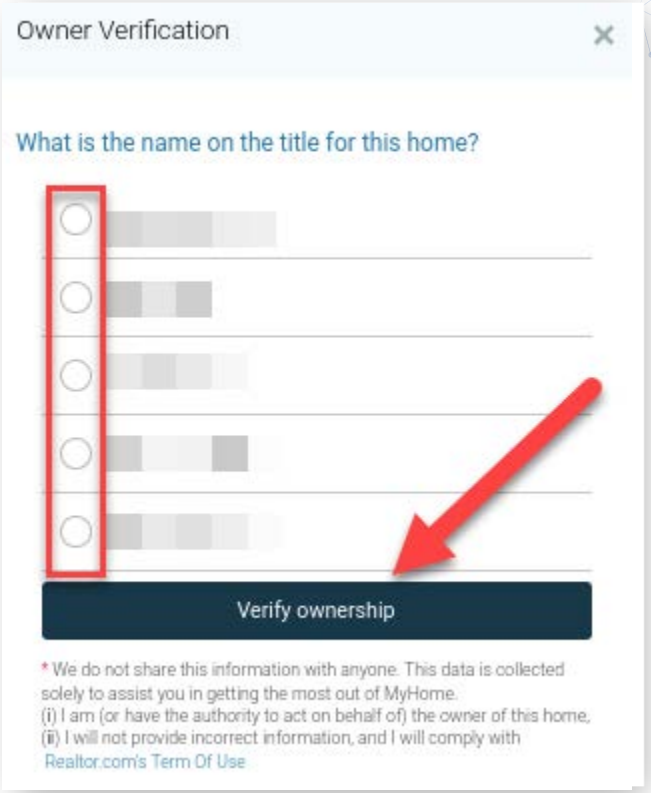


7 **Select Remove photos.**

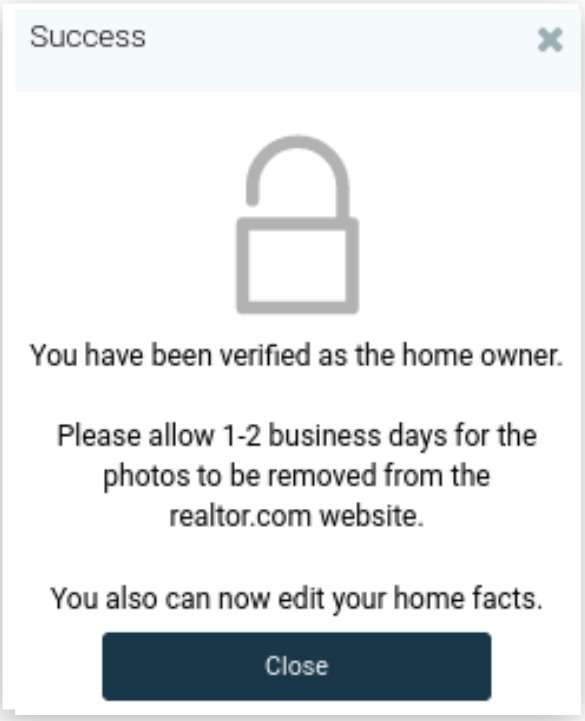
8 **Select Yes, remove all photos.**



9 **Select the owner and press Verify ownership.**



10 **You will now see this pop-up.**



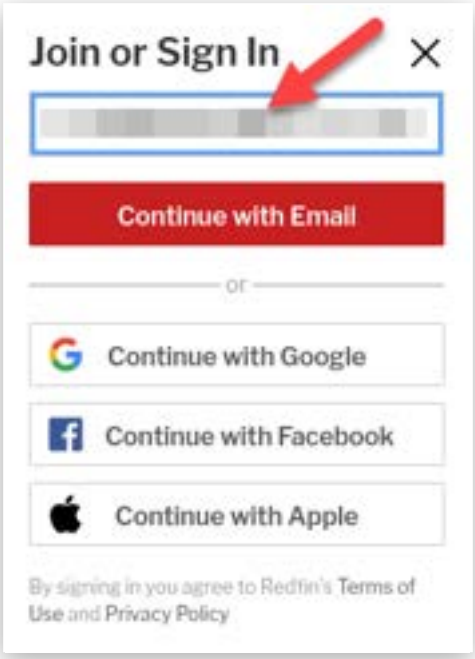
Redfin.com

1

Go to Redfin.com and Sign Up.

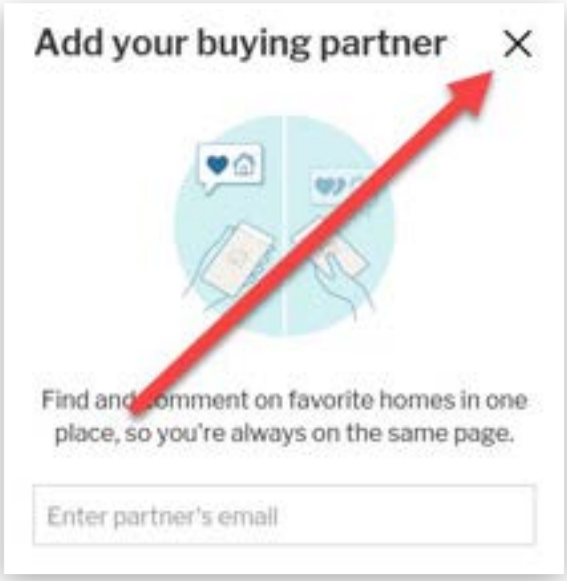
2

Enter your email address.



3

Hit the X



Redfin will send an email to this email address and you will need to create a password for the account and enter your name.

4

Enter your address.

5

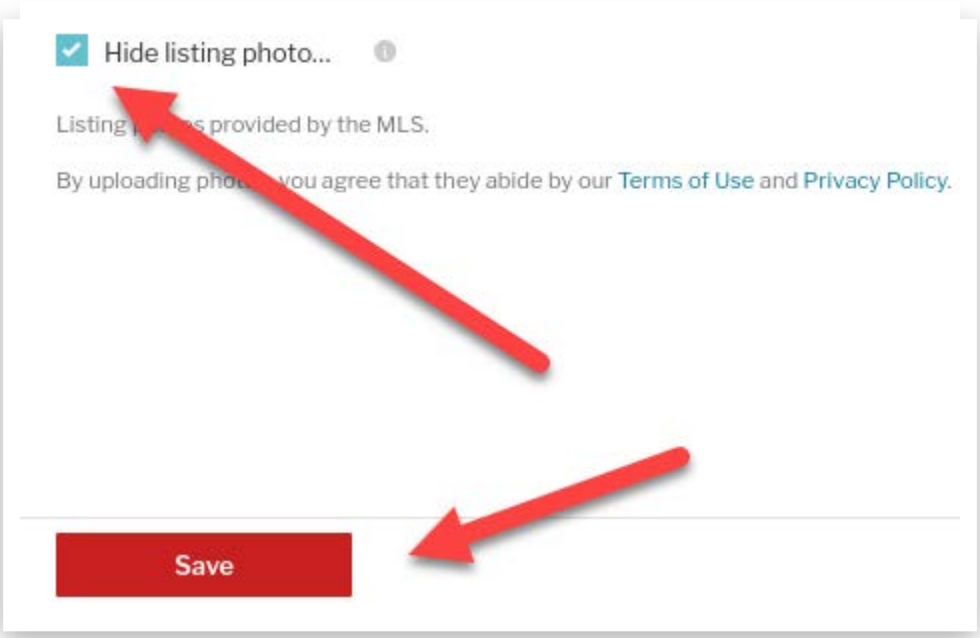
In the upper right corner, press Edit Photos.

6

Select your name, check the box confirming you are the homeowner, and press Verify.

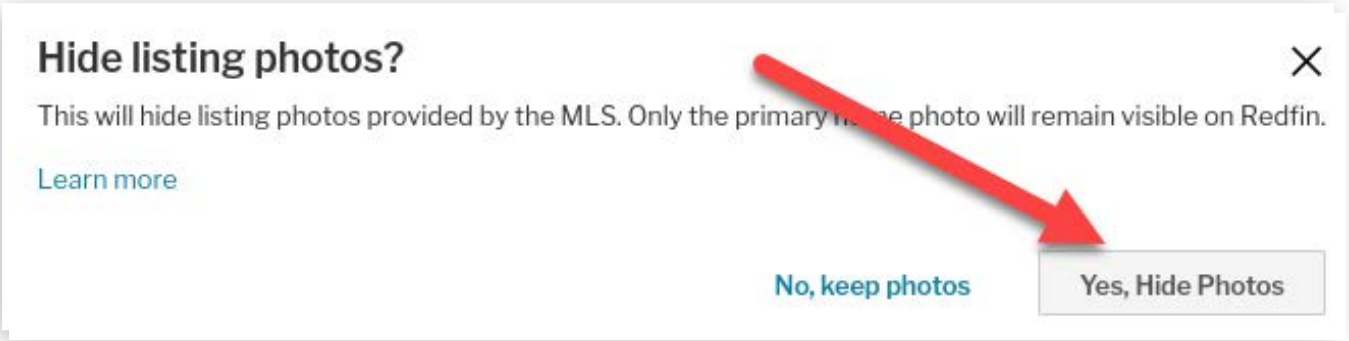
7

Select Hide listing photo... and press Save.



8

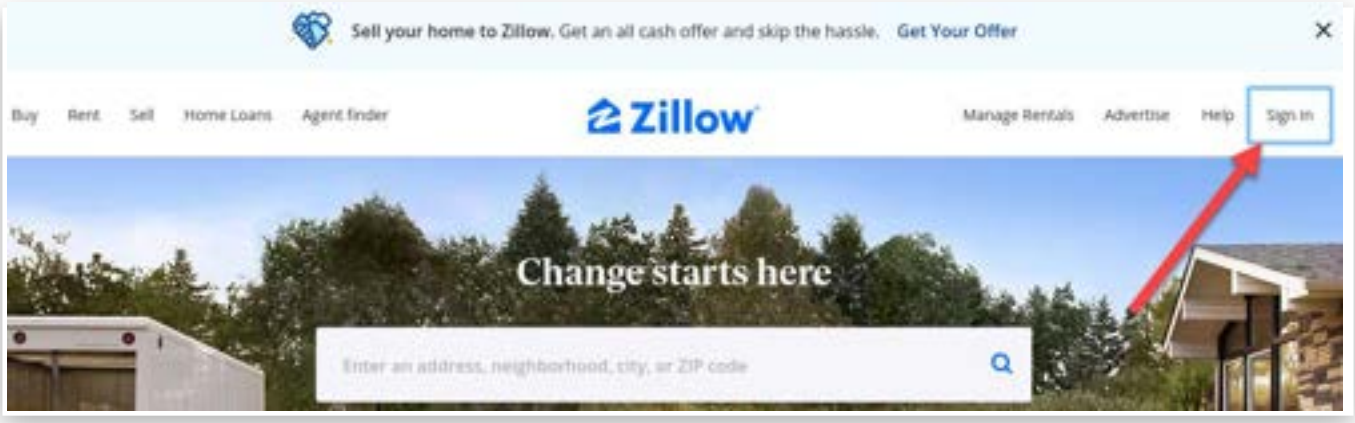
Press Yes, Hide Photos.



Zillow.com

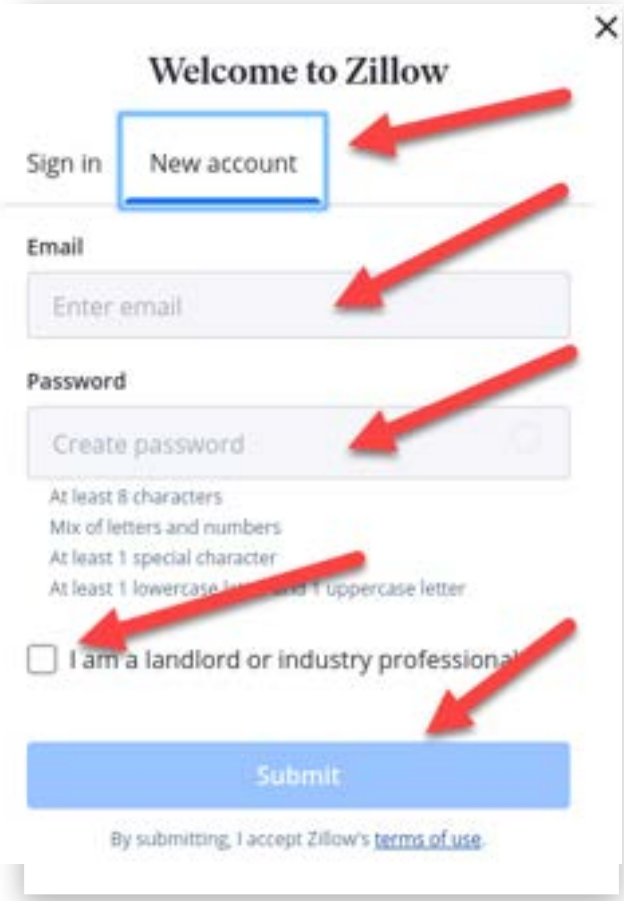
1

Go to Zillow.com and press the Sign In button.



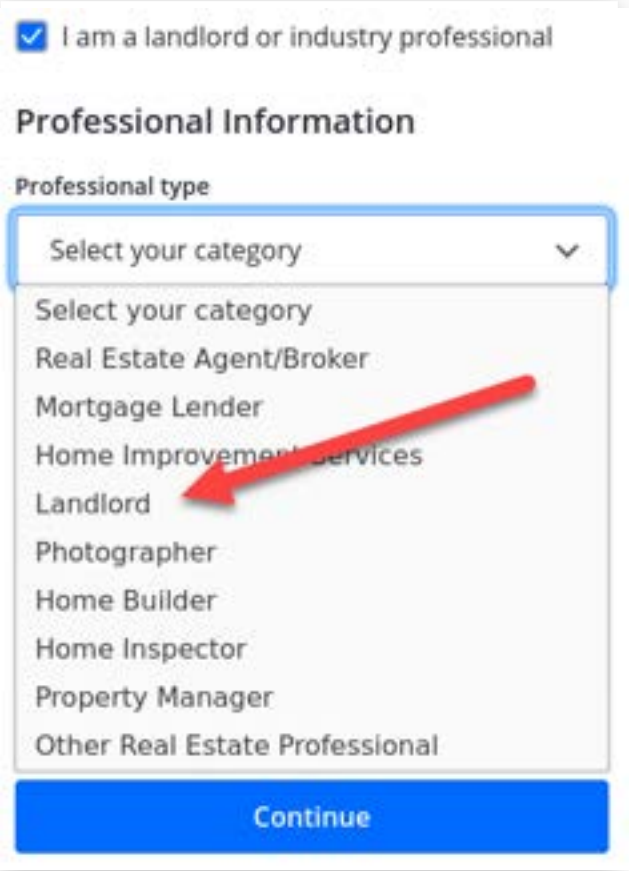
2

Press the New account tab, complete the form, and press Submit.



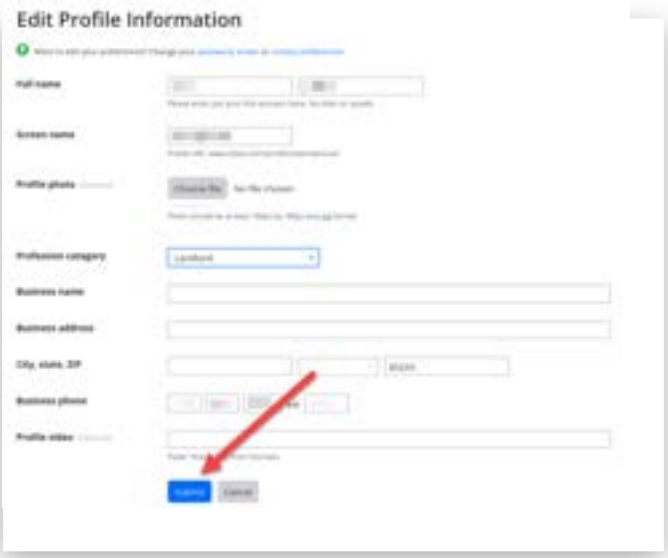
3

You are the Landlord.



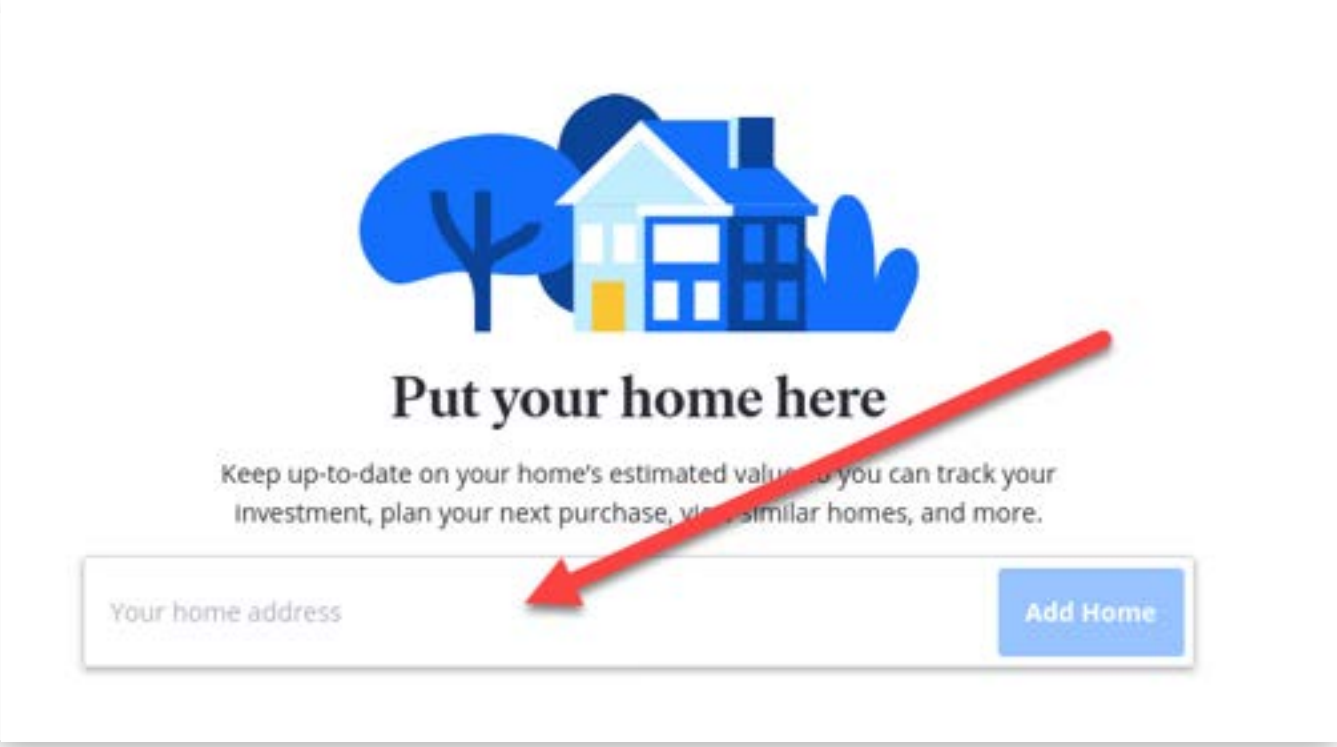
4

You will go to a populated page with your details. You can keep the unfilled fields blank and press Submit.



5 **Under your profile, Sign in & Security, Email, press Verify, and click on the link in your email to verify your account.**

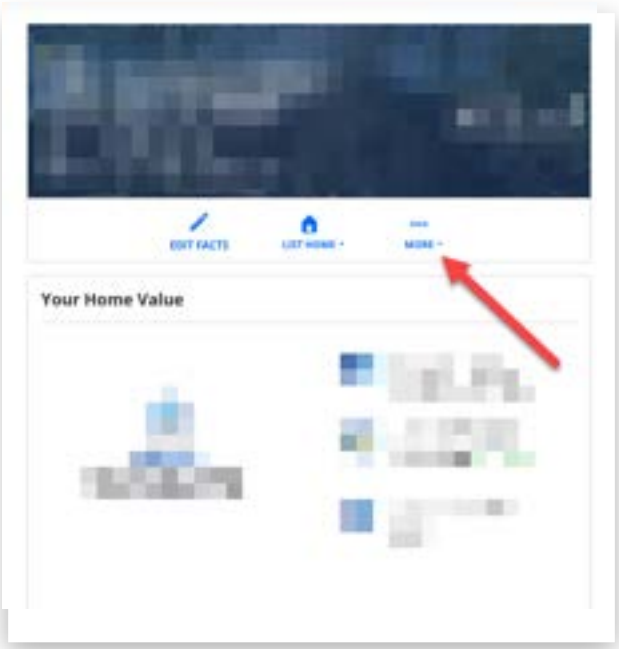
Under Account Settings, select Your home and enter your address.



6 **Your home will appear in a popup window. Press Yes, Add it!**

7

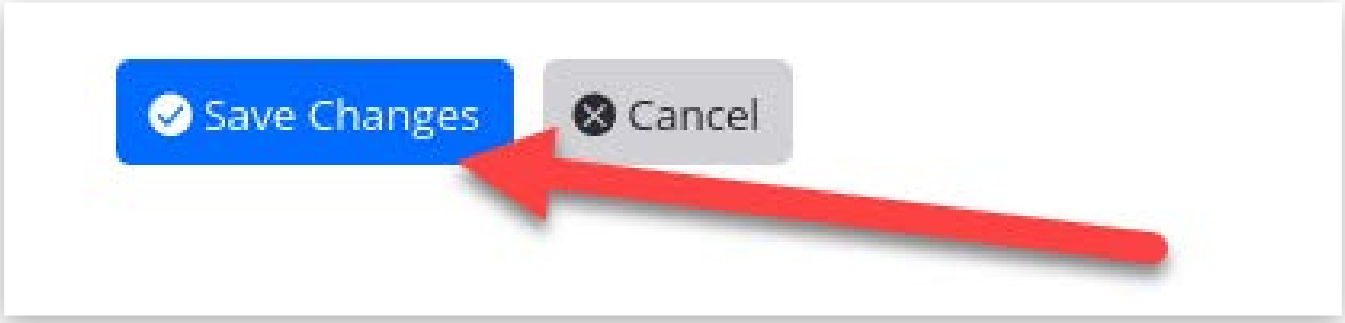
Select More.



8

Under edit home facts, scroll to the bottom and individually select each photo, and choose Remove photo.

9 **Press Save Changes when you are done.**



Check back after a few days to confirm your pictures were removed.

DON'T LET A CRIMINAL STEAL YOUR GOOD CREDIT

Placing a security freeze will not allow new creditors to query or establish a new credit account in your name. If you need to open a new account, you unfreeze the account as long as necessary to secure new credit.

This service is free and takes less than 5 minutes for each account. There are more than just the top three: Experian, Equifax, and Transunion. Remember Innovis, Chex, and NCTUE.

- Equifax
- Experian
- TransUnion
- Innovis
- ChexSystems
- NCTUE

REMEMBER WHO YOU ARE

In 2021, there were 1.4 million reports of identity theft, almost 4,000 per day.

There are many companies that offer identity theft services. You should look for the following:

- Alerts you of any credit bureau inquiries and any new accounts created.
- Allows you to track your credit score.
- Alerts you if your information is found on the dark web.
- Alerts you if your personal information was used by someone arrested.
- Alerts you if your personal information was found on online public or private databases
- Helps with the tasks necessary to fully restore your identity and minimize damage.
- Offers financial reimbursement for any losses due to identity theft.

Alerts you receive that someone opened a new credit account in your name is like responding to a crime scene to take the report. The crime has already been committed.

To prevent the crime (the theft of your identity) from occurring in the first place, follow the steps in this eBook to secure your accounts with two-factor authentication, don't reuse passwords, and minimize your exposure on social media and with everyone who stores your personal information.

STOP YOUR EMAIL FROM BEING HACKED

Set Up Two-Factor Authentication

You know when you log in to an account and you get a text message with a 6-digit code? That's two-factor authentication (2FA) and it's very effective at keeping your accounts secure.

You should set up 2FA on every account that offers it, especially your email accounts. Your important financial, shopping, and social media accounts use password-reset requests sent via email. If your email account is compromised, a hacker could intercept those password-reset emails and change the passwords to your important accounts, then lock you out!

Data breaches are common and they expose your usernames and passwords. If you have 2FA enabled, an attacker won't be able to access your account.

Another way to protect your email is by using temporary emails.

Use Temporary, Forwarding, And Encrypted Email Providers

Need a quick email account that isn't connected to your real email account? There are a few options. These sites provide short term access to email accounts, from 10 minutes to a couple of days. Some of these free services allow you to compose a new email (GuerrillaMail) and others only allow you to receive an email.

- GuerrillaMail
- 10MinuteMail

Don't use temporary emails for any important accounts and be careful what you communicate through them. Also, once they expire, you will not have access to them or any email they contain.

Forwarding Email Service

These services allow you to create a temporary email address which gets forwarded to your main email address. The benefit is your main email address is never shared with the recipient which increases your privacy. You can delete the temporary email address after you use it so you'll never get their spam. I use and recommend SimpleLogin.io.

Encrypted Emails

If you're not paying for your email service, it's likely the provider is reading, or at least scanning, your emails. If you use an encrypted email service, emails between you and others who use encrypted email services are unreadable by anybody but the sender and recipient.

There are several email providers who promise to use end-to-end encryption. I use and recommend ProtonMe.com.

YOUR MAILBOX IS SPREADING GOSSIP

Stop The Junk Mail

Your name and address are purchased, sold, and re-sold to junk mail distributors. Stop the cycle and opt-out by using these links:

- DirectMailAssociation
- DirectMail
- Valpak

Stop Getting Mail At Your Home (at least in your real name)

Start using a PO box or similar mail drop location. Get your Amazon packages delivered to a locker or store.

STOP THE HARASSING PHONE CALLS

Register For The Do Not Call Registry

Do Not Call Registry

Remember, if you use Gmail, you can use a Google Voice phone number that comes with your account. You can make and receive phone calls and text messages using the Google voice app installed on your cell phone.

ONLY REMEMBER ONE PASSWORD

DO YOU RE-USE PASSWORDS?

When your data is breached your password is exposed. You have heard the advice that you should not re-use passwords. If you use the same password on multiple accounts, the stolen password can be tried on other accounts you have, thereby allowing a hacker to access your other accounts with the shared password.

If you use a different password on each account, when one password is exposed after a breach, only that one account is compromised.

So how do you remember a different password for each of your accounts? You don't have to.

PASSWORD MANAGERS

When you use a password manager, you only need to remember one password and the password manager remembers the others.

The password manager creates unique, difficult-to-guess passwords to each account and remembers them all for you.

The password manager also syncs between your desktop and cell phone so you can log into all of your accounts from whichever device you are currently using.

You can sign up for a free password manager account, but most people find value in upgrading to the paid versions that offer additional features. I would consider this a necessity for our online connected world.

I use and recommend LastPass.com. It syncs across multiple computers and devices, imports passwords from browsers, reminds me if I'm reusing a password, and tells me if any of my passwords are weak.

PROTECT YOUR INTERNET TRAFFIC

Virtual Private Network

Do you need a VPN?

Maybe.

When you use a VPN to connect to the internet, your first hop from your computer will be to a server run by your VPN service. Your internet traffic is then encrypted so it is more secure. From there, the websites you visit will show your traffic as coming from the VPN server, not your home.

Here's The Good:

- Your internet service provider won't be able to see the websites you visit. They will just see you connected to a VPN service.
- The websites you visit won't be able to identify your home connection because they only see the VPN connection.
- You can also set up a VPN on your phone which is very useful when you connect via WiFi at a public location.

Here's The Bad:

- Many financial institutions and other important sites with enhanced security will not allow you to connect through a VPN.
- Your speed will slow down as you are adding an extra step to your internet travels. Sometimes this delay will cause websites to time out and you'll lose the connection.

Most VPN services offer free trials so try before you buy. I use Private Internet Access and recommend them. Another favorite is ProtonVPN.

LOCK DOWN YOUR SOCIAL MEDIA

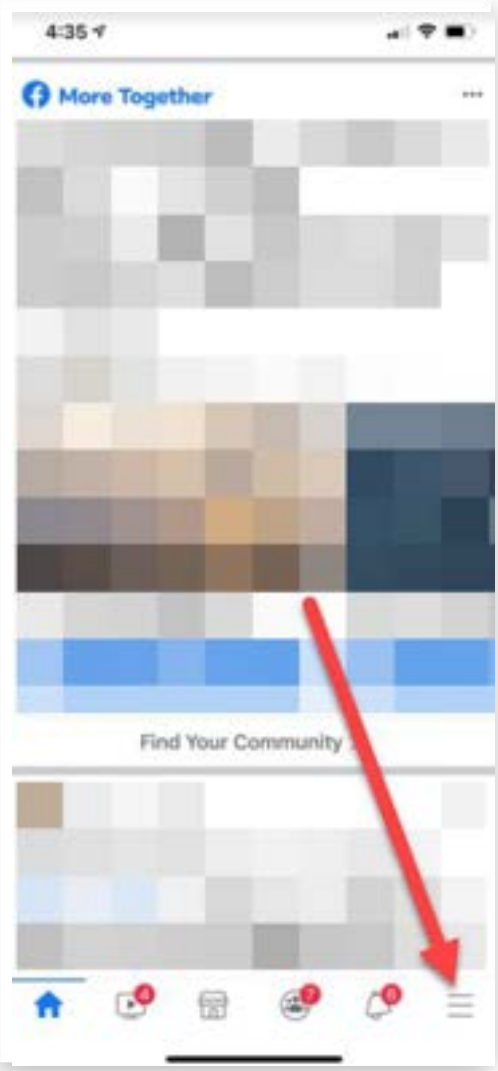
Lock Down Your Facebook and Instagram

Lock down your account and check back often to make certain your settings have not changed. Every time the software is updated, the settings are reset to the default (open) settings. This is beneficial to the app, not you. In the following example, I'll use the current Facebook app installed on an iPhone.

To make your Instagram private, go to Settings > Privacy and Security and check the box Private Account.

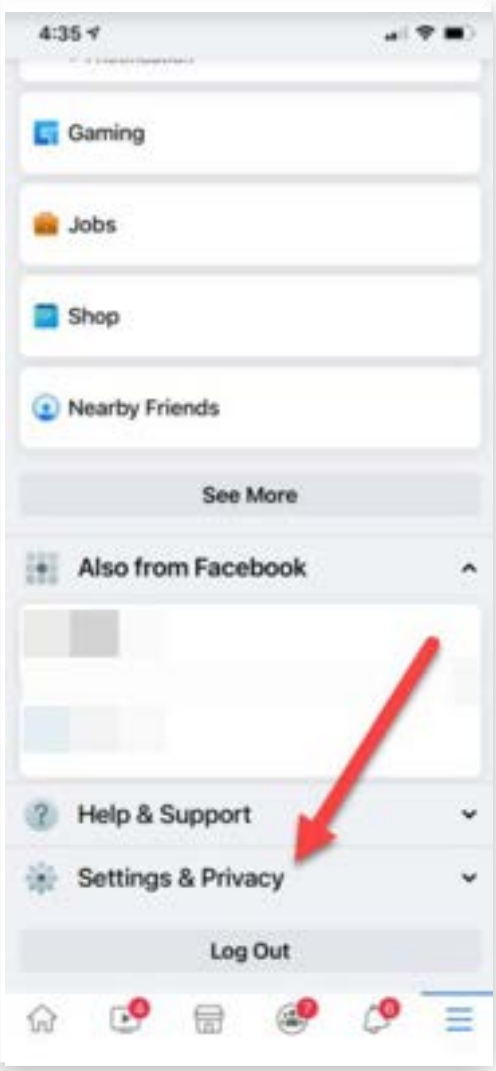
1

From the Facebook main page, press the hamburger lines



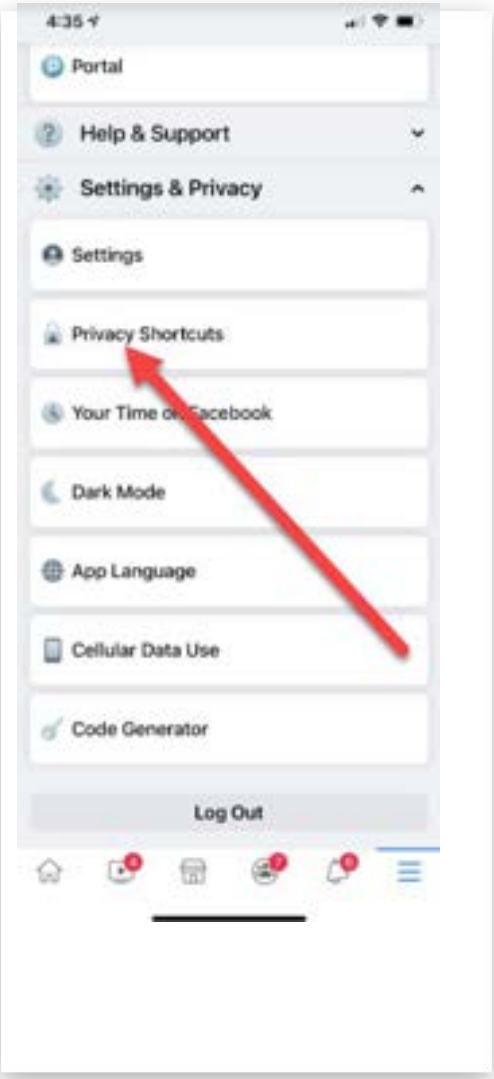
2

Select Settings & Privacy



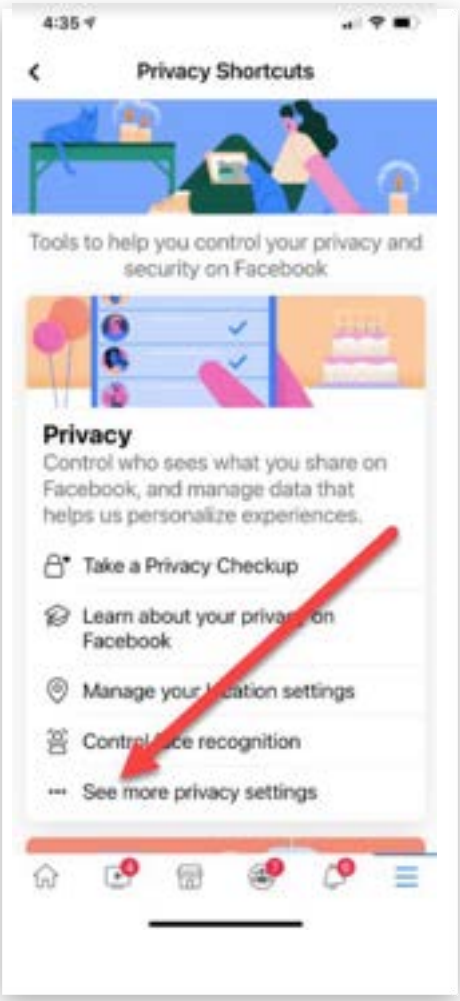
3

Select Privacy Shortcuts



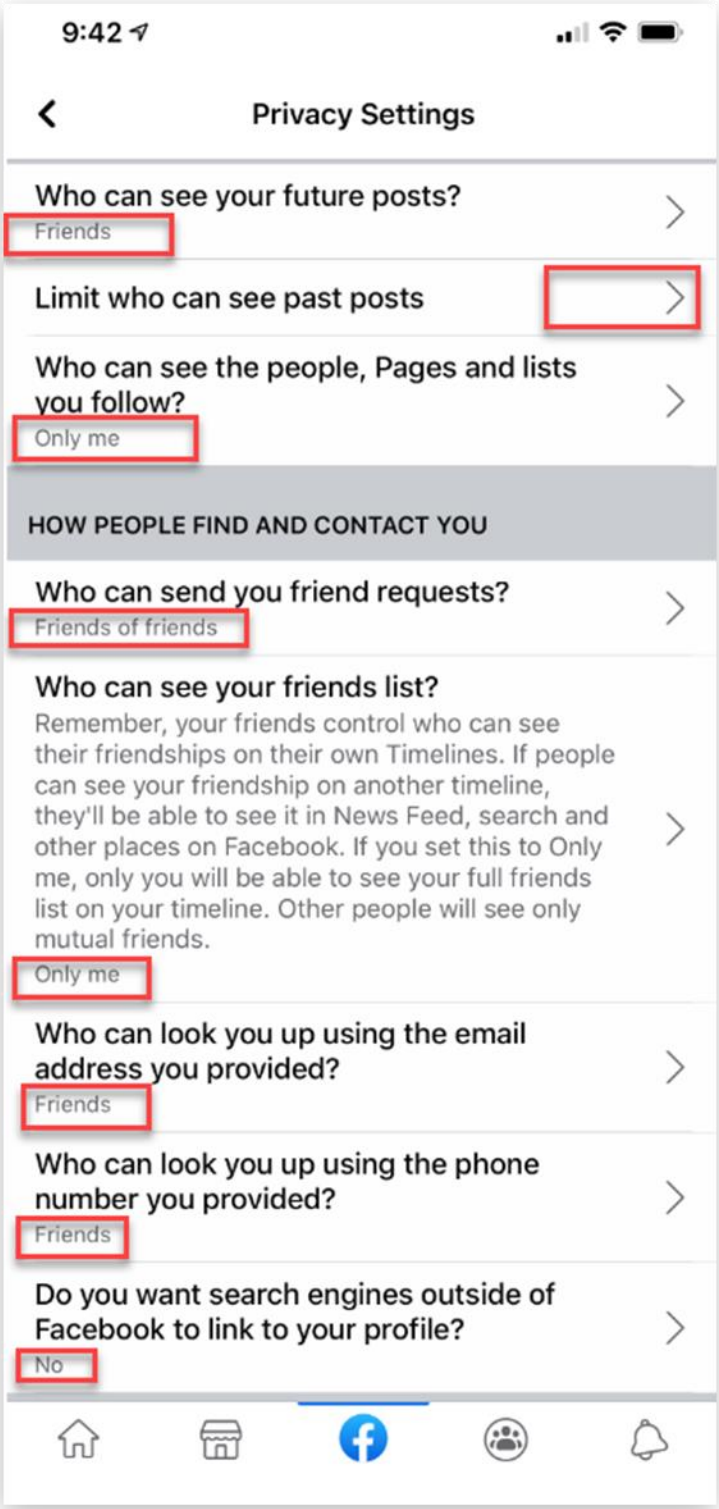
4

Select the See more privacy settings



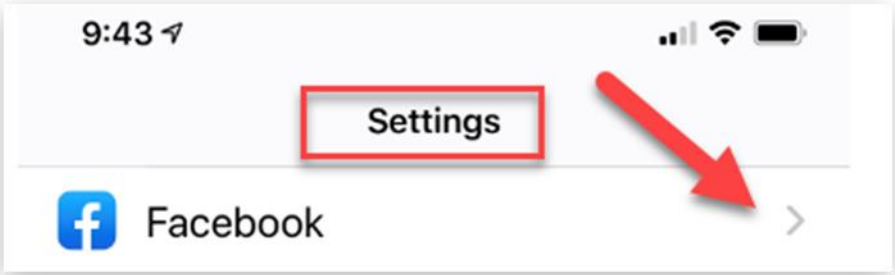
5

I'd recommend the following settings:



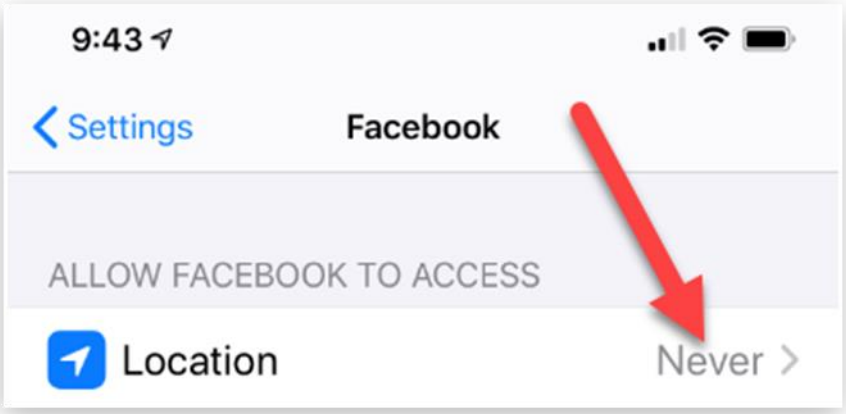
6

In your phone's Settings, select Facebook



7

Set Location to Never



WHAT DO THEY KNOW ABOUT ME?

If your information is being captured and stored, it can be viewed by unscrupulous people. Do you trust every employee at Facebook, Instagram, Twitter, and Google?

Follow these instructions to identify what Facebook knows about you?

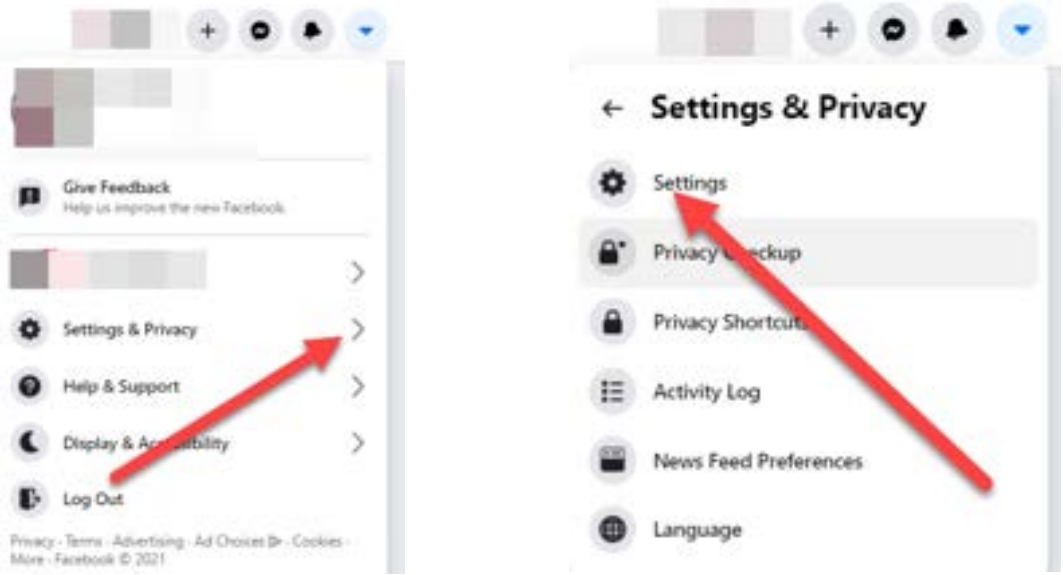
Facebook Export

1

Log in to your Facebook account and press the drop-down arrow on the right

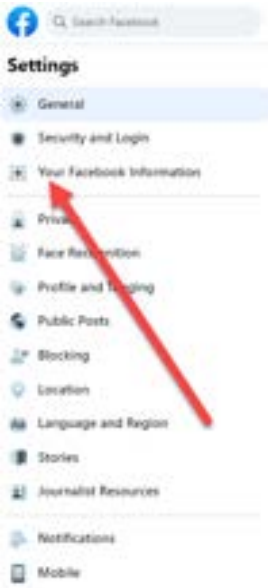
2

Select Settings & Privacy, then Setting



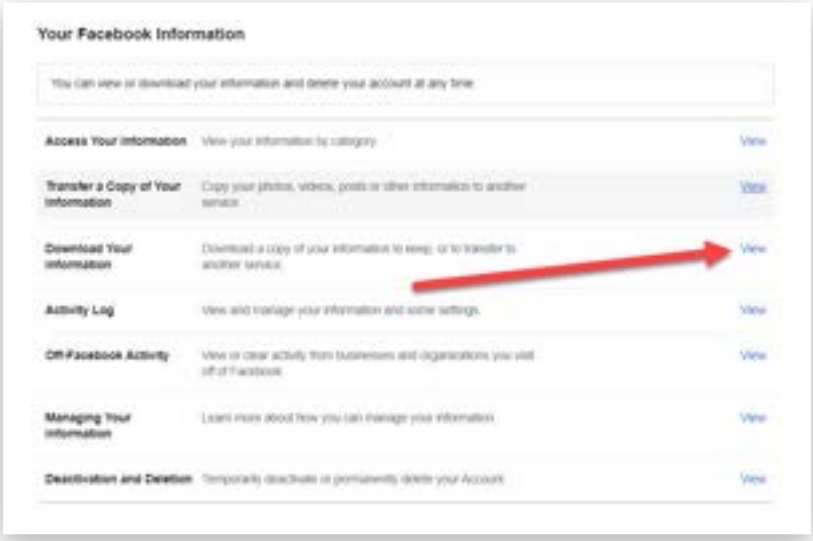
3

Select Your Facebook Information



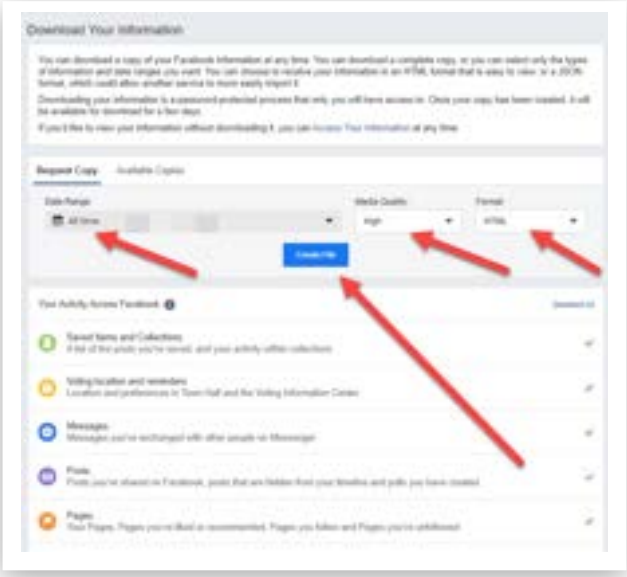
4

Select Download Your Information



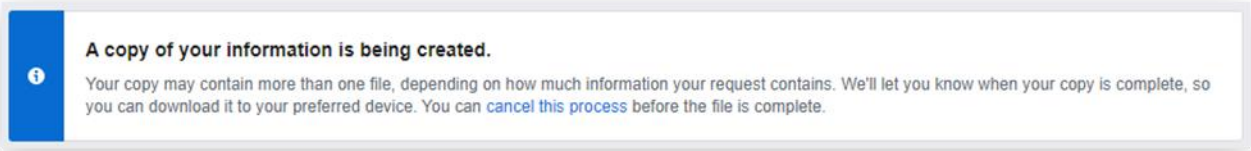
5

You can accept the defaults



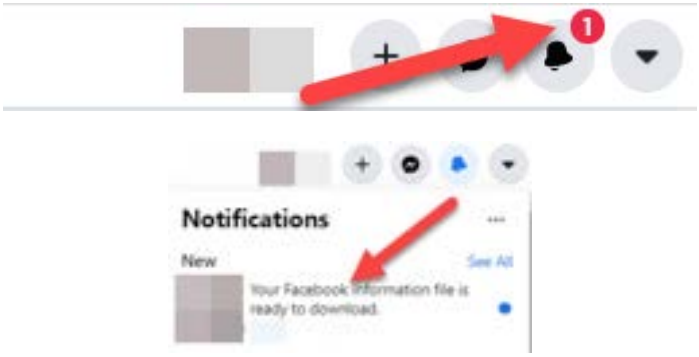
6

Facebook will confirm your request



7

When the download is ready, you will receive an alert

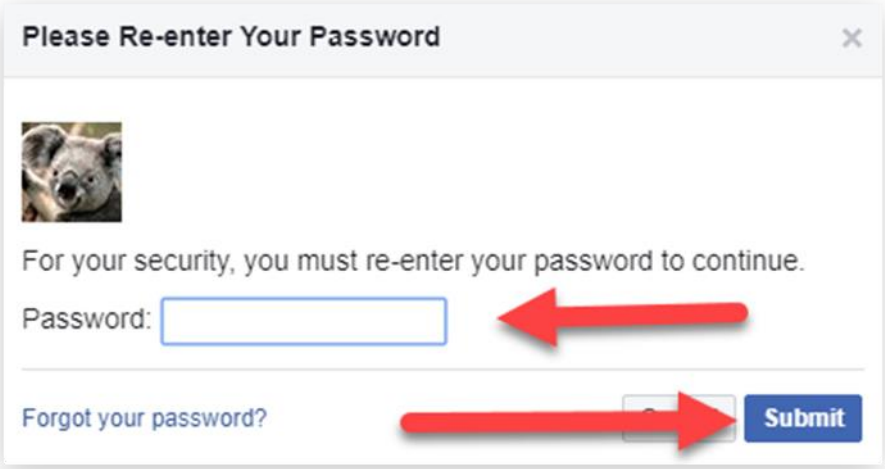


8

Press the button to download

9

You will need to enter your password



10

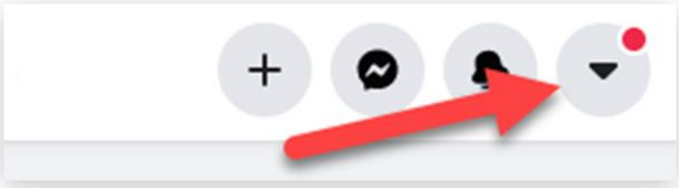
A zip file will be downloaded to your computer

Unzip this file, then double-click on the “index” icon and a browser will open. You’ll be able to look through all of the information Facebook knows about you.

Facebook Two-Factor Authentication

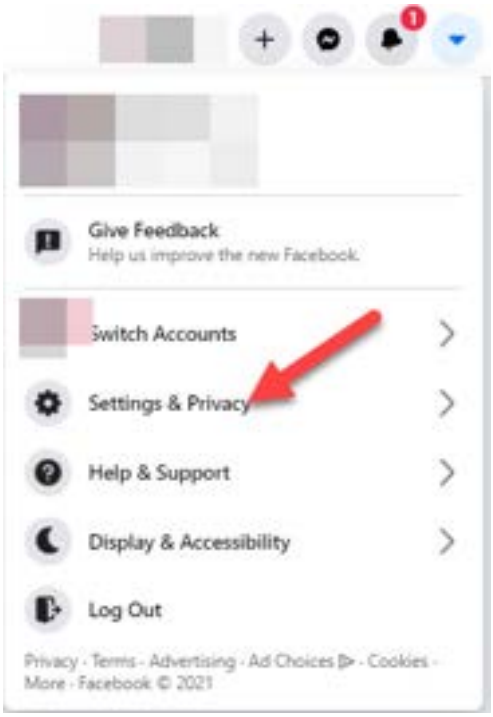
1

While you're in your Facebook settings, set up two-factor authentication. On the right side, select the drop-down menu.



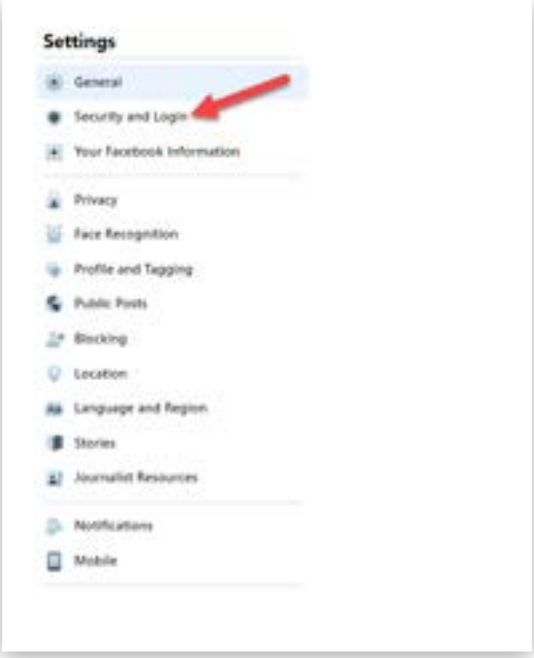
2

Select Settings & Privacy



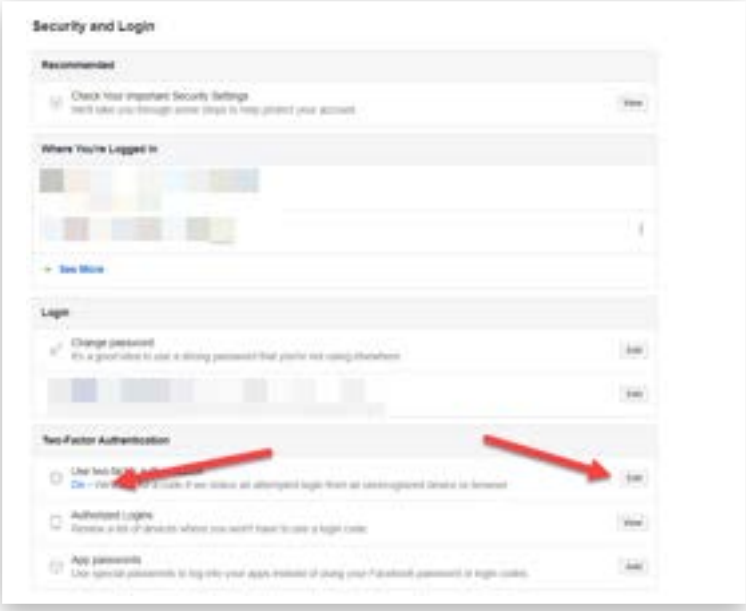
3

Select Security and Login



4

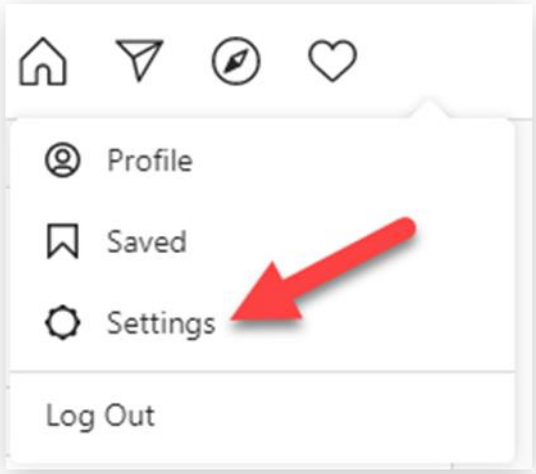
Under two-factor authentication, select your preferred option, an Authentication app, or a text message to your cell phone.



Instagram Download

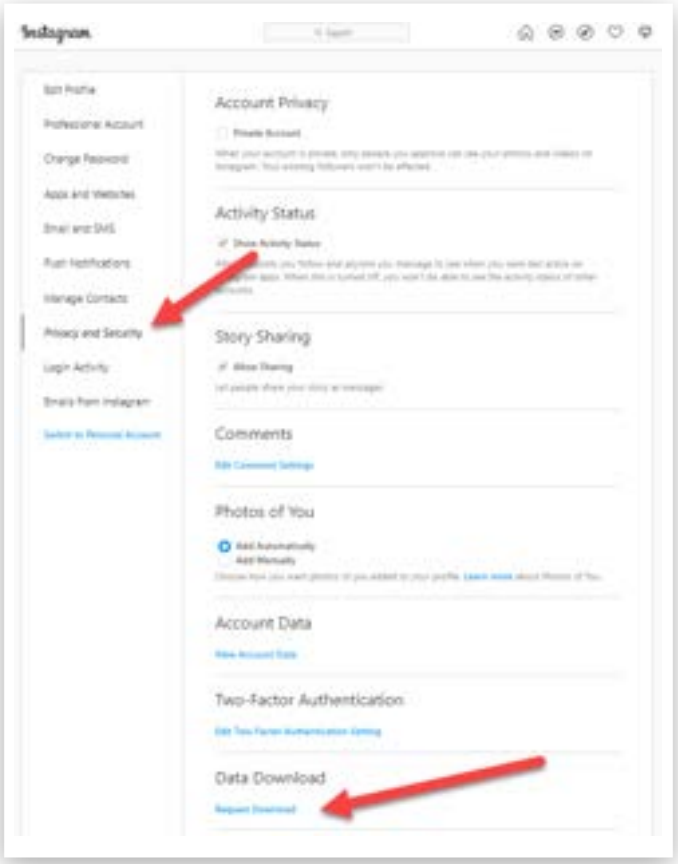
1

Log in to your Instagram account, click your icon, and select Settings



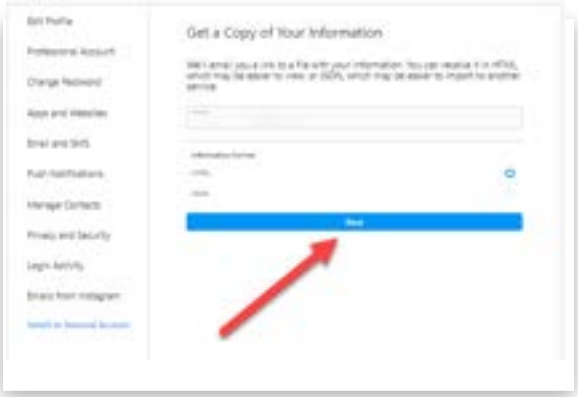
2

Select Data Download, Request Download



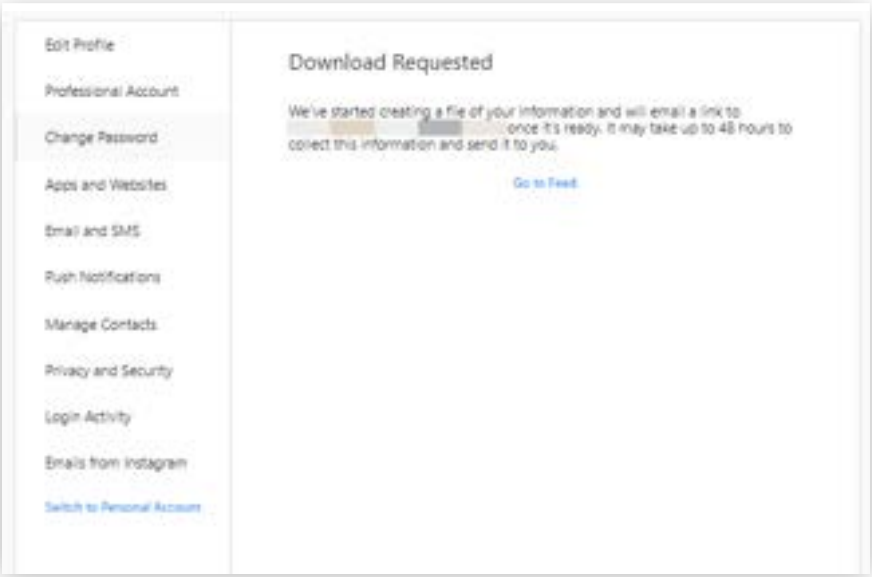
3

Enter your email address and select Next



4

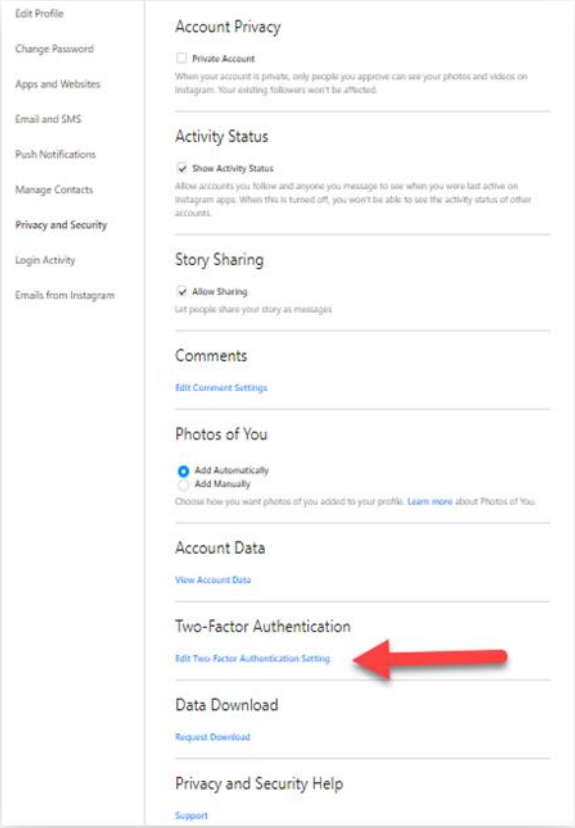
You will receive an email with a link to your data



Instagram Two-Factor Authentication

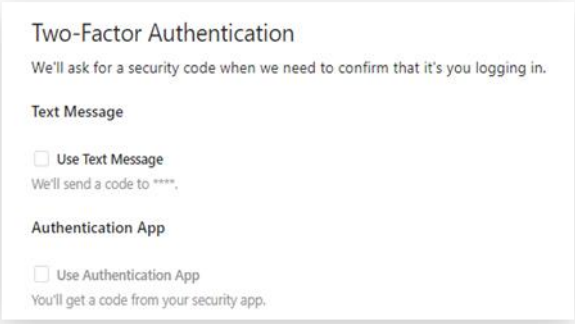
5

While in your Settings, select Two-Factor Authentication Settings



6

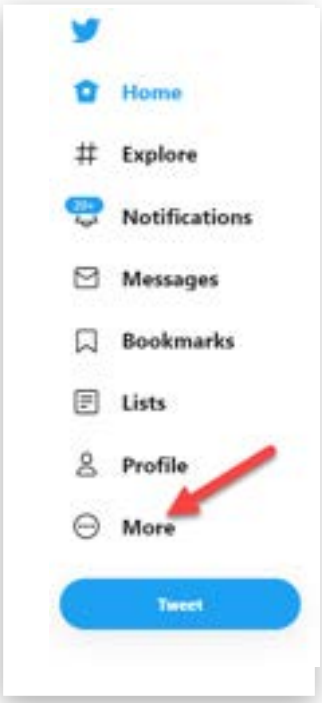
Select your choice, a text message sent to your cell phone, or using an authentication app, like Google Authenticator or Authy

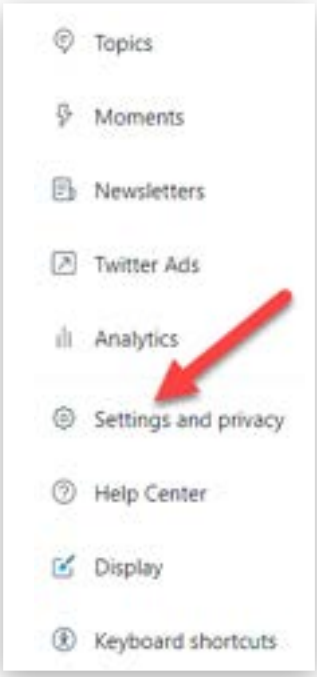


Twitter Download

1

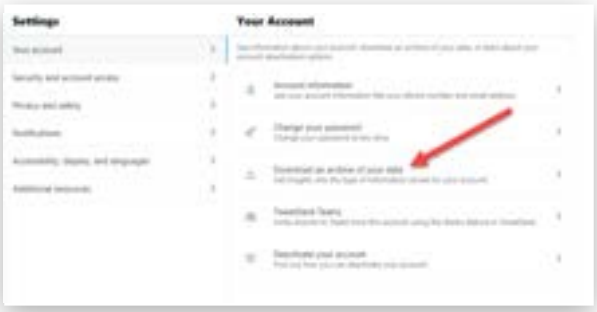
Log in to Twitter, navigate to Settings, select More, then Settings and privacy

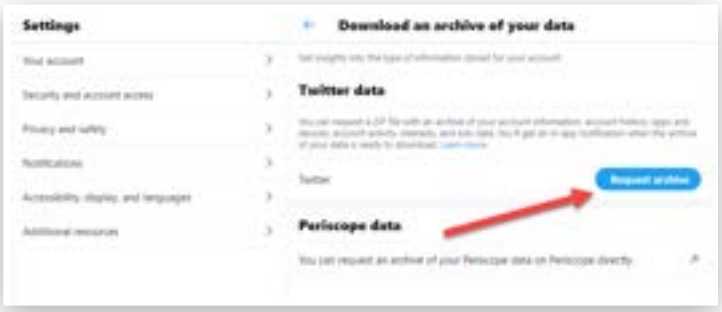




2

Select Download an archive of your data, then Request archive

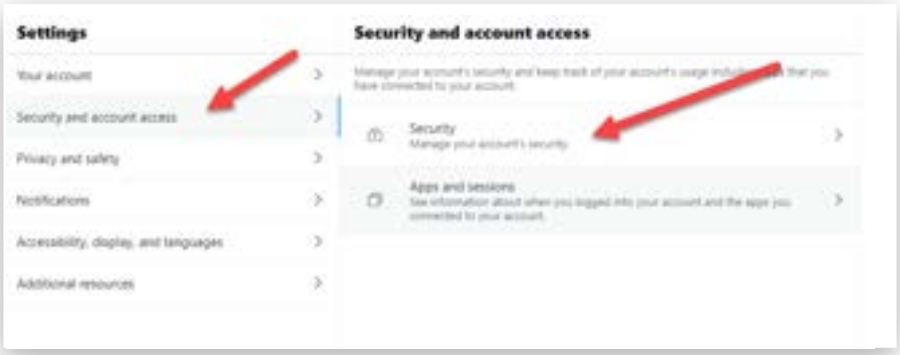




3

Review your Account access history to make certain only you are accessing your account.

Places you've been are the locations Twitter has recorded for your account.



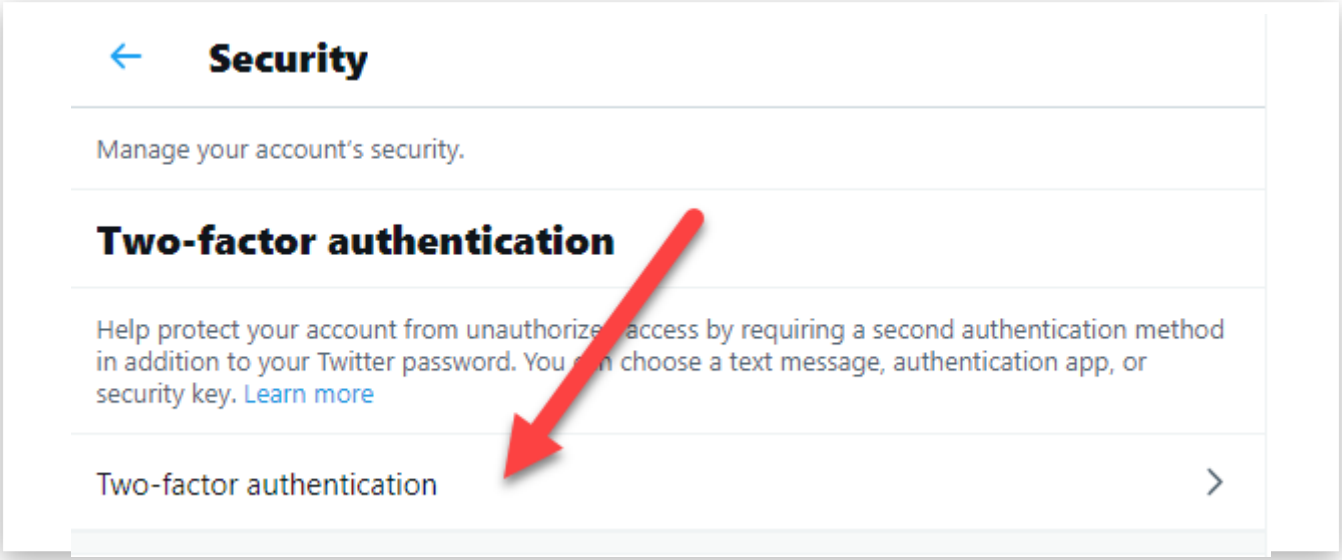
4

There may be additional apps that are tracking your location.

Twitter Two-Factor Authentication

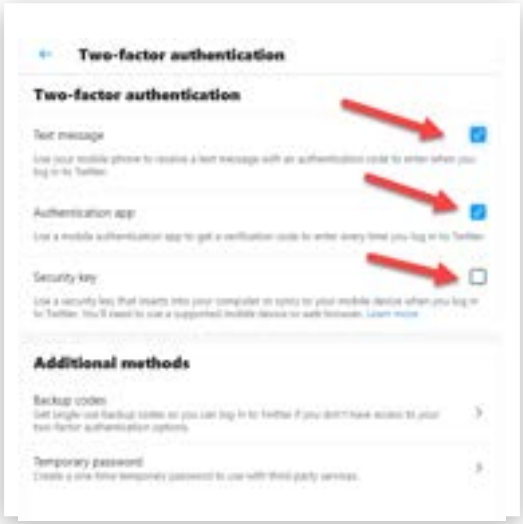
1

While in Settings, select Security, the Two-factor authentication



2

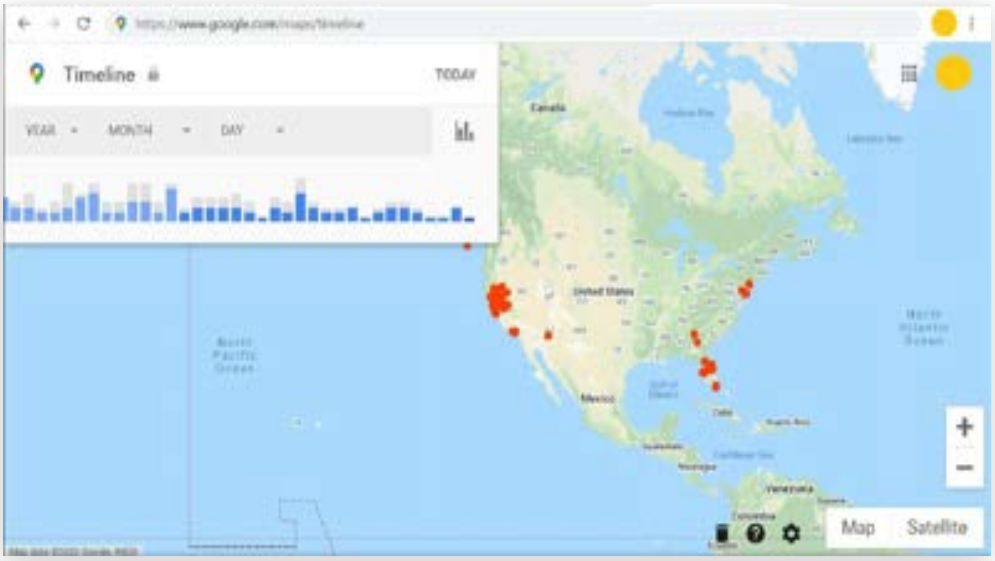
Select your preferred option



IS GOOGLE TRACKING YOU?

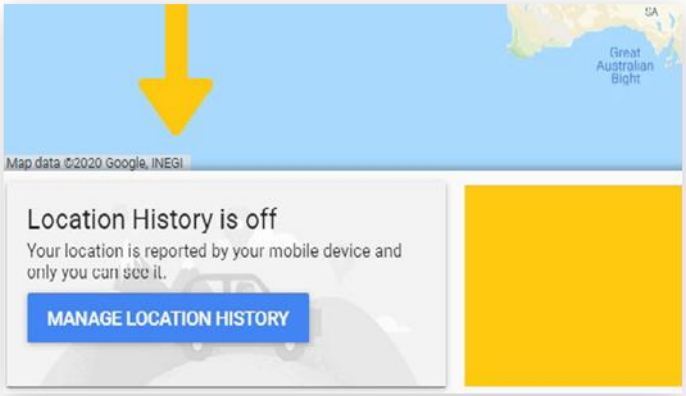
1

When you're logged in to your Google account, go to google.com/maps/timeline
If you see red dots on the map like below, you're being tracked.



2

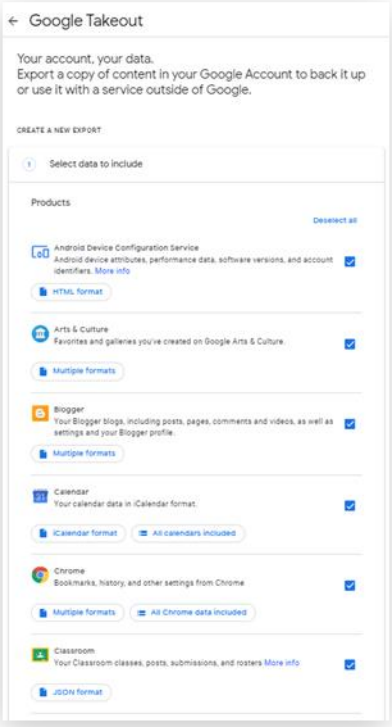
If you don't see any red dots on the map and you have a message in the lower-left corner, tracking is off.



Takeout.google.com

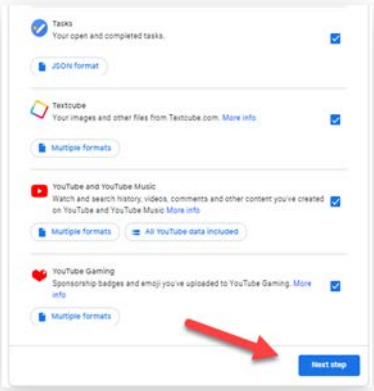
1

What does Google know about you? While logged in to your Google account, go to takeout.google.com You will see a screen like this. The default is to download everything. Accept the default.



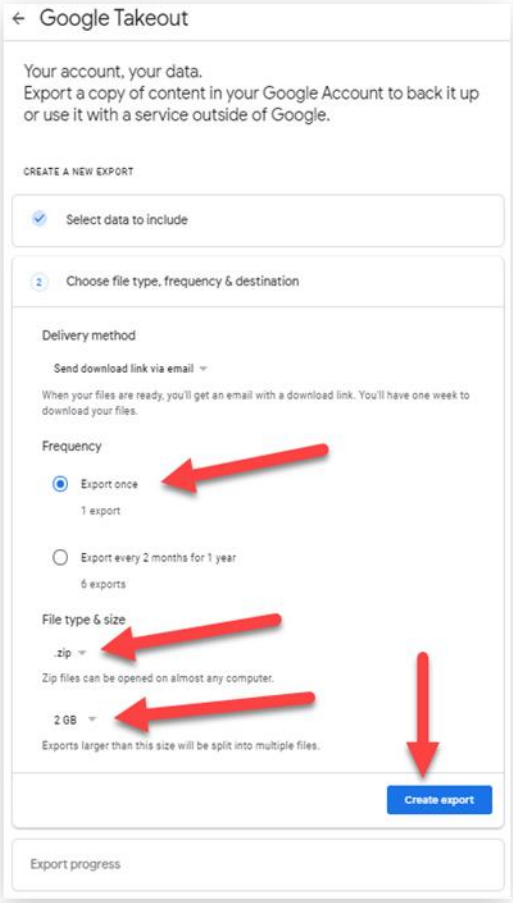
2

At the bottom, press Next Step



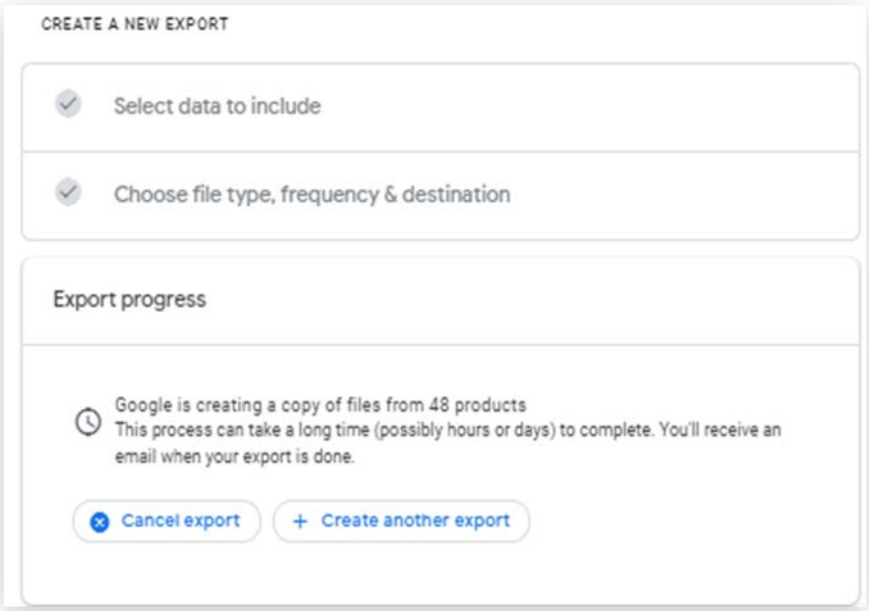
3

Accept the defaults and press Create export



4

After it has been completed, download your export.

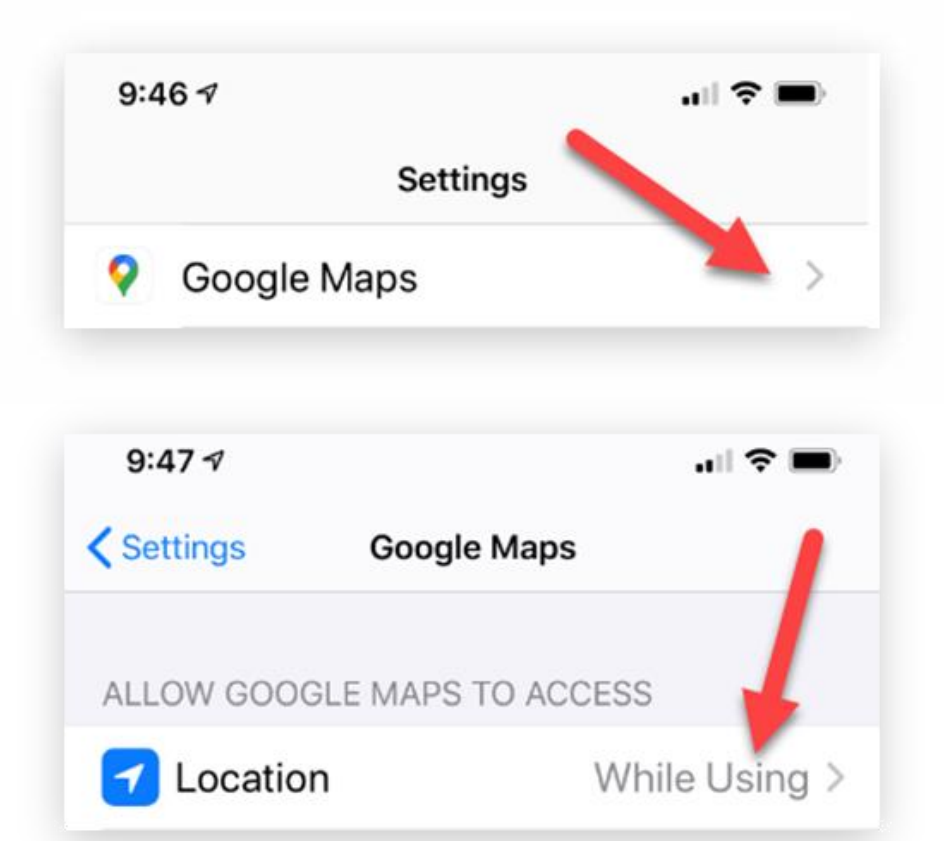


Unzip this file, then double-click on the “index” icon and a browser will open. You’ll be able to look through the information Google knows about you.

Disable Google Tracking

1

In your cell phone settings, select Google Maps and select While Using. While you're there, change your other mapping apps to only track you when you are using the app



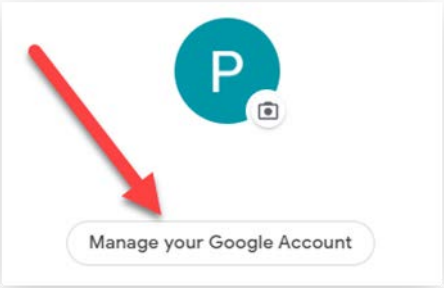
Set up Google Two-Factor Authentication

1

While logged in, on the right side, select your icon

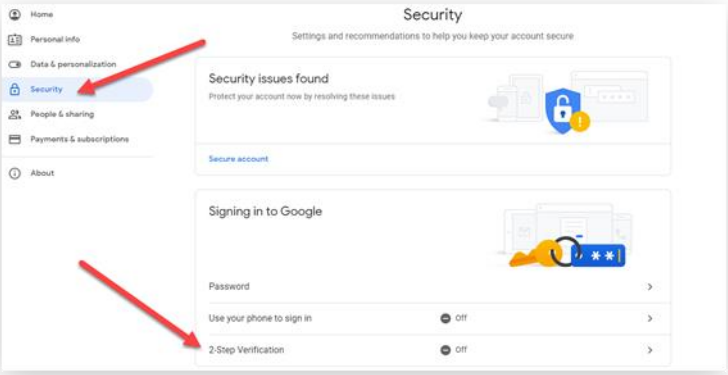
2

Select Manage your Google Account



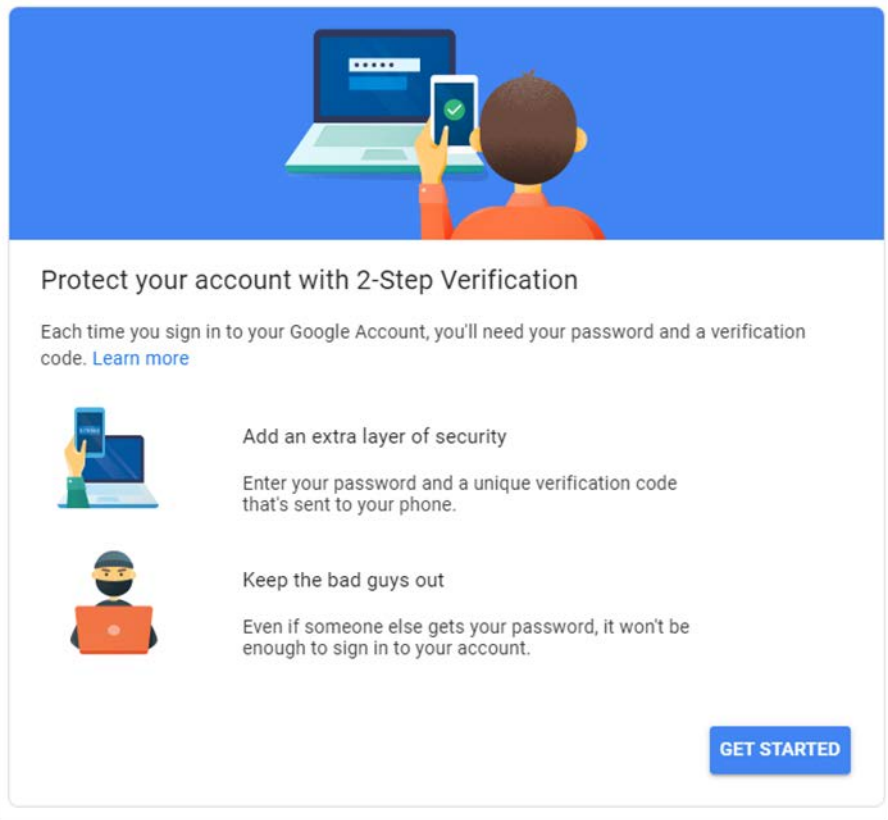
3

Select Security then 2 Step Verification



4

Follow the instructions



"OfficerPrivacy.com is one of the best tools to come along to protect my privacy. As a former law enforcement officer, author, and speaker for first responders and the military, it is important to have the peace of mind that OfficerPrivacy.com provides."

Adam Davis, Author of *Behind the Badge* and *Bulletproof Marriage*, Speaker, and Former Law Enforcement Officer

With the growth of the internet, information is readily available. Take some simple steps and you'll feel a lot more secure. Those who protect and serve should feel protected while at work and home.

If you need a little assistance, check out the resources I offer:

OfficerPrivacy.com offers two types of service:

- Access to OfficerPrivacy.com Quick Removal Software so you can quickly remove yourself and your family from the top 50 people-search sites. We offer FREE access to our software for 14 days. This is Option 1 on the website.

- Premium Service where OfficerPrivacy.com's staff of current and former US law enforcement officers remove you from the top 50-people search sites. The Premium Service includes monitoring these sites for reappearance. If you reappear, we remove your information again. This is Option 2 on the website.

> *"I advise every law enforcement officer to sign up for OfficerPrivacy.com immediately. OfficerPrivacy.com is a basic survival resource that every cop needs to put in place right now before you are under attack!"*
>
> *Lt. Col. Dave Grossman, U.S. Army (Ret)*
> *International trainer and author of On Killing, On Combat, and On Spiritual Combat*

Note: I only recommend services I use and am happy with. I recommend the password manager LastPass, the VPN service Private Internet Access, and the encrypted email service Protonmail.

I don't receive any compensation by recommending these services.

25 Rarely Used Privacy Tricks

- **Inside you'll learn:**
- **People-Search Sites That Expose Your Home Address**
- **Credit Freezes and Their Effectiveness**
- **How Much Google and Facebook Actually Know About You**
- **How to Stop Getting Junk Mail**
- **And So Much More!**