Protecting Your Privacy: Best Practices for Mobile, Social, and Search Settings
In a world of identity thieves, hackers, and cybercriminals of all types, it’s critical we take every step we can to protect our privacy. This guide is designed to serve as a roadmap when it comes to your mobile, social, and search settings.

**General Mobile Settings**

**Use a PIN**

Evildoers don’t just exist online. There are plenty of bad actors in real life too. Don’t be one of the 28 percent of people who don’t use a lock screen for their smartphone — protect your personal data by setting a Personal Identification Number (PIN) on your phone. Whether you use numeric codes, digital patterns, or some other combination, be sure to set a PIN that’s easy for you to remember but hard for others to guess.
**Turn off GPS tracking**  
If a hacker gains access to your phone and you have GPS tracking enabled, they can track your every move. Additionally, advertisers base the majority of the ads you see on your location data.

Navigate to your phone’s settings and review/edit the apps you’ve granted location access. If it’s not necessary for an app to know your location, disable the location access.

**Block IDFA**

Your phone’s Identifier for Advertisers (IDFA) allows apps to swap information with other apps like Facebook and view any other history tied to your IDFA. This means if you download an app designed to help you stop smoking, you could begin seeing ads for nicotine gum. To prevent this from happening, reset your advertising identifier and disable the function.

On Apple devices, you’ll need to turn on Limit Ad Tracking in the Advertising section of the Privacy menu. For Android devices, you’ll need to opt out of Ads Personalization in the Ads menu.
Lost phones
Both Android and iOS devices come with awesome features to assist you if your device is lost or stolen.

ANDROID
Google’s “Find My Device” feature is particularly powerful; just be certain it’s set up properly. To do this, navigate over to the Security & Locations menu and verify that Google’s Find My Device service has permission to erase your phone.

Now you can remotely lock your lost phone with a secure password, send a customized message to anyone who finds your phone, sign out of the device, and remotely wipe your entire data. You can also locate your device by searching “find my device” on Google.
APPLE

Apple's Find My iPhone provides features similar to Android's version. If your phone is lost, simply log in to www.icloud.com, and select “Find iPhone.” You can now view your device's location on a map, place your phone in lost mode, add a secondary number for someone to call if it's found, and even remotely erase your device.
Monitor your apps permissions

It’s critical you monitor the permissions of your apps and restrict their capabilities where possible. If an app doesn’t need access to your camera, calendar, or location to function, consider disabling these features.

**ANDROID**

Go to Settings, select Apps & Notifications, then tap App Permissions. You can now view and edit each app’s permission settings.
APPLE

Click Settings and then Privacy. You can now select which apps are allowed to access your contacts, calendars, photos, and more.

Stay up to date
Make sure you keep all of your software updated. This includes not only your operating system but also your apps. When they release updates, it’s in your best interest to install them, as they often include patches for known security vulnerabilities.

Protect your phone number
In addition to editing your phone’s privacy settings, you should also be careful who you’re sharing your phone number with. If you’re signing up for a store loyalty card, for example, it’s a good idea not to use a phone number tied to any of your online accounts.

If you’re truly concerned about ad tracking and your privacy, consider setting up a second number.
FACEBOOK

Keep your account secure
You can create a more secure account by visiting the Security and Login section of Facebook Settings. From this menu, you’re able to accomplish the following:

Identifier for Advertisers (IDFA) allows apps to swap information with other apps like Facebook and view any other history tied to your IDFA. This means if you download an app designed to help you stop smoking, you could begin seeing ads for nicotine gum. To prevent this from happening, reset your advertising identifier and disable the function.

Login settings
Change your password or choose to log in with an image.

Set up extra security
Opt in to two-factor authentication, sign up for instant alerts about unrecognized login attempts, and select up to five friends to contact if you get locked out.

Advanced options
Set up encrypted notification emails from Facebook, and view past notifications.
Edit who can view your posts
In addition to editing who can see your posts each time you share something on Facebook, you can establish default settings in the Privacy Settings & Tools section of Facebook.

- Edit who can view your future posts by selecting from the following: public, friends, friends except (which allows you to select which friends should be blocked from seeing your post), specific friends, and only me — an option that allows only you to see the posts.

- You can also limit the audience of your past posts by electing to share them only with friends; however, anyone tagged in the posts will still be able to view them.

- Curious about the content of your past posts or Facebook actions? You can view your activity log to see what you've shared, along with any times you were tagged in a post.

Edit how people find and contact you
On the Privacy Settings and Tools Page, you can edit the following.

- **Who can send you friend requests**
  We recommend “friends of friends”

- **Who can see your friends list**
  We recommend keeping this private

- **Who can look you up using the email address you provided**
  We recommend “friends”

- **Who can look you up using the phone number you provided**
  We recommend “friends”

- **If you want search engines outside of Facebook to link to your profile**
  We recommend opting out
Edit Facebook Ad settings
Adjust who can view your photos by changing the privacy settings at either the photo or album level. Just click the menu option where the globe is. Select a custom audience, allow the public to see, or set it so only you can view your photos.

Adjust profile settings
Finally, navigate to the About tab of your Facebook profile. Here you can not only edit identifying information — like what college you attended, where you work, and who are family members — but each item has its own privacy setting.

Just click the edit icon on the right side of each section to determine who can view this information.

TWITTER

Each of the following options can be adjusted within the Privacy and Safety section of the Settings menu.

Protect your tweets
When you select the Protect Your Tweets action, your future tweets will not be available publicly. However, your previous tweets will still be available to the public.

Tweet location
You can prevent your tweets from publishing your location, as well as delete any previous location details. We recommend doing this.

Photo tagging
Control who can tag you in a photo.
Discoverability
Choose whether you allow users to locate you by either your phone number or email address. We recommend opting out of these features.

Edit your personalization and data
You can deselect ad personalization, or whether Twitter can personalize content based on your apps. You can also force Twitter to forget other devices you've used to access the social media account, and to turn off personalization that occurs based on the places you've been.

Remember to deselect “share data through select partnerships.”

Edit direct messages
Choose who can send you direct messages and whether or not to send read receipts to users.
INSTAGRAM

Make your account private

On the mobile app, go to your profile settings by clicking your user icon. Scroll down and select Private Account. Privacy protection on Instagram is fairly lacking, so you'll want to remember that if you switch to a private account:

- Your followers will remain the same, and you'll need to manually delete any followers you don't want to view your account
- Your bio will still be viewable and any user can send you a photo or video directly

Protecting Your Photo Map

- When posting a photo, switch the Add to Your Photo Map option to off.
- You can remove geolocation data from previously posted photos by selecting the Photo Map tab on your profile page, choosing Edit, and then tapping the grid options at the bottom of the screen and selecting which photos to delete.
Search

While we recognize there are search alternatives to Google, their privacy settings are very limited. Google provides more robust privacy options, and this is why we have outlined them below.

GOOGLE

After logging in to Google, you can — and SHOULD — explore the following:

- **A map of where you've been**
  In addition to viewing your location alongside dates and times, you can also delete your records and elect to switch off location tracking

- **Your complete online search activity**
  This includes your search history across all devices, which you can manage and delete

- **Your advertising profile**
  View and edit your advertising settings

- **What apps you use**
  View and edit third-party apps that have access to your Google account — we recommend restricting access where appropriate

- **Your YouTube history**
  View and edit your entire YouTube viewing/search history

- **Download ALL Data**
  You can delete any data you don’t want a record of, or download it all in one giant file