7 Steps for More Online Privacy and Control

Tue, 03/09/2021 - 12:00

| IDShield

Steps that can help you to be in control of your online privacy!

Step One: Delete the accounts you don’t use.

Step Two: Delete apps you don’t use from your phone.

Before you delete an app, make sure to first delete any associated account you may have created alongside it. To remove the app once that’s done:

Android™[1]

- Open the Play Store.
- Tap the hamburger menu in the top-left corner.
- Tap My Apps & Games > Installed > Alphabetical, and change it to Last Used. For any app you don’t use anymore, tap the name of the app, and then tap Uninstall to get rid of it.

iPhone®[2]

- Head to Settings > General > iPhone Storage, to find a list of all your apps, organized by size. This section

also lists the last time you used an app. If it's been a while, there's likely no good reason to keep it around.
- Tap the app, and then tap the Delete App button.
- While you're at it, now's a good time to give the remaining apps a privacy audit to make sure they don't have permissions they don't need. Here's how to do so on Android and iPhone.

Step Three: Audit third-party app access.

If you use a social media account to log in to a service (like logging in to Strava with a Google account), you access social media accounts through third-party apps (like Tweetbot), or you use a third-party app to access data like calendars or email,
it's worth periodically checking those accounts to remove anything you don't need anymore. By regularly reviewing app usage, you can gain more control over your data.

All the major tech companies offer tools to see which apps you've granted access to your account. Go through and revoke access to apps and services you no longer use:

Facebook[3]

- Click the dropdown arrow in the top right, then select Settings and Privacy> Settings > Apps and Websites. This includes apps you've granted access to

Facebook, and apps you use your Facebook account to log in to.
- Go through and remove anything here you don't recognize or no longer need.

Google™[4]

- Log in to your Google account, and then head to the Security page (or click your profile picture > Manage Your Google Account > Security).
- Click on Manage Third-Party Access, and then remove access to any apps you do not use.
- On this page, you can also see any third-party services you've used your Google account to sign in to. Click any old services you no longer need, and then Remove Access.
- You can also check on app-specific passwords. Head back to the security page, then click App Passwords, log in again, and delete any apps you no longer use.

Twitter[5]

- Head to the Connected apps page while logged in (click on three-dot icon > Settings and Privacy > Security and Account Access > Apps and Sessions > Connected Apps).
- Revoke access to any apps you do not use.

Apple®[6]

- Log in to your Apple ID and head to the manage page.

- Under the Security tab, click Edit. Look for App-Specific Passwords, and then click View History.
- Click the X icon next to anything you no longer use.
- Then scroll down to Sign in With Apple, click Manage Apps & Websites, and revoke access to any apps you don't need anymore.

Step Four: Delete software you do not use on your computer.

Windows7

- Open Settings > System > Storage, and then click on Apps & Features.
- Under the Sort By dropdown, select Install Date.
- Go through and remove anything you don't need. If an app is unfamiliar, search for it online to see if it's something you need or if you can safely get rid of it. You can also search for it on Should I Remove It? (though we recommend skipping the Should I Remove It? application and just searching for the software's name on the site).
- While you're here, it's a good idea to go through your documents and other files too. Getting rid of big old files can help improve your computer's performance in some cases, and clearing out your downloads folder periodically can ensure you don't accidentally click on anything you didn't intend to download.

Mac®8

- Click the Apple icon > About This Mac, and then select Storage > Manage > Applications.
- Go through and see if there are any apps you no longer need and delete them. If you have many apps, it's useful to click the Last Accessed option to sort by the last time you opened the app.

Step Five: Remove browser extensions you don't use.

Browser extensions have a bad habit of taking all sorts of data, so it's important to be careful what you install. This is also why it's a good idea to periodically go through and remove any extensions you don't really need.

Chrome™ browser[9]

- Click the puzzle icon > Manage Extensions.
- Click the Remove button on any extensions you don't need.

Firefox[10]

- Click the three-dot icon > Add-Ons.
- On any extensions you no longer need, click the three-dot icon next to the extension, and then select Remove.

Safari®[11]

- Click Safari > Preferences > Extensions.

- Click the Uninstall button on any extensions here you do not need.

Step Six: Remove yourself from public records sites.

If you have ever searched for your own name online, you've probably come across a database that lists information like your address, phone number, or even criminal records. This data is accumulated by data brokers, companies that comb through public records and other sources to create a profile of people.

You can remove yourself from these sites, but it can take a couple hours of work to do so the first time you try it. Check out this GitHub page for a list of directions for every one of these sites. If you're short on time, focus on the ones with skull icons next to them, like PeekYou, Intelius, and PeopleFinder.

Step Seven: Reset and recycle (or donate) devices you don't use.

If you have electronics you don't use anymore—old tablets, laptops, smart speakers, cameras, storage drives, and so forth—factory-reset them (or if it's a laptop, wipe the storage drive), delete any associated accounts, and then find a place to recycle or donate them.

Older computers, tablets, and phones often have more life in them, and there's always someone who can use them. Sites like the National Cristina Foundation can help you find somewhere to donate locally, and the World Computer Exchange donates globally. If you can't donate a device, like an old smart speaker, most Best Buys have a dropbox for recycling old electronics.

The less cruft on your devices, the better your general privacy and security. But it also tends to improve the general performance of your hardware, so 30 minutes of effort is a win-win. Combined with a password manager and two-factor authentication, these steps can stymie some of the most common security and privacy breaches we all face.