NNEDV

Tools for Safer Browsing

Internet browsers are the first step to accessing the internet. They are also the first step to both increasing your online privacy and controlling your personal information. This handout discusses various tools that you can use for safer browsing beyond the browsers' own privacy settings. This resource may contain language and terminology you have never heard before and may seem technical to you. Take your time reading through this document, ask questions, test the tools, and most importantly, be patient with yourself. We do not endorse products but through testing and research found that the tools mentioned may be helpful to protect survivor privacy. For more information about browser settings that you may be able to use to increase your safety and privacy online, see Safety Net's Browser Privacy Settings resource.

Before We Start: Prioritize Safety

Using these privacy options may increase your privacy and safety, particularly if you are concerned that an abusive person is physically monitoring your device activity. They can also help you to have more control over how your personal information is collected and stored when you are online. However, these options may not protect you from remote spying or monitoring if an abusive person is using stalkerware.

There isn't one "right" way to respond to abuse and online safety concerns, only ways that do or don't fit your situation. What works for someone else may not work or be safe for you. Always prioritize safety and trust your instincts. Making changes will often alert the other person. They might force you to unlock your phone or share your passwords. They might become more abusive. In some situations, making changes could also erase evidence. You may find these safety steps useful:

- Use a safer device. If you think that someone is monitoring your phone or accounts, use a different device (such as a library computer or a friend's phone) and account that the person cannot access (and that they have not had access to in the past).
- Get more information. Navigating violence, abuse, and stalking can be difficult and dangerous. Advocates can help you figure out options and local resources and help you create a plan for your safety. You can contact a national helpline to be connected with local resources.
- To get more tips about tech safety as a survivor, see Safety Net's Survivor Resources Toolkit.

Why Care About Companies Collecting My Browsing Data?

It can be hard to figure out how seriously we should care about companies having our browsing data and if we can even do anything about it. However, companies sharing, buying, and/or selling our data is one way that information gets to data brokers who collect and share personally identifying information such as names, homes address, email address, date of birth, health information, and more, from consumer data and public records (for more on data brokers, see Safety Net's resource on them). Companies may also use your browsing data to target ads to you or to make suggestions to you while you are using social media. If you are concerned about an abusive person looking through your social media accounts or monitoring your devices, these ads and suggestions may share detailed information about you that you did not want them to know. For example, they could show that you have been looking for legal help, reproductive health services, or information about a city to which you plan to move.

Tracker Blocking

There are numerous free browser extensions that can be used to block third-party trackers (if you aren't sure what this means, see the next paragraph). Websites use trackers to monitor users' activity and gather their data. A browser extension, which is also called an "add-on" in some browser menus, is like an app, but for your browser (if you use multiple browsers, you will have to add the extension to each one separately).

Third-party trackers send information about your browsing history to other companies besides the one whose website you are visiting. This allows them to track your activity across the Internet and build a detailed profile of you through your browsing history. They may collect not only what you do on the webpage you are visiting, but also your browser history, not just telling companies what you click on when you are on that site, but what sites you were visiting prior and after.

Many browser extensions meant to protect users from trackers are primarily focused on only blocking ads (which are often, but not always, the source of trackers). One exception is Privacy Badger, which is focused on blocking tracking behavior. Its website has detailed, user-friendly explanations. Unfortunately, it does not currently work with Safari, iOS, or Chrome for Android, but it does work with most other desktop browsers (Google Chrome, Microsoft Edge, Mozilla Firefox) as well as Firefox for Android (which you can also download for free).

If you use a browser that is incompatible with Privacy Badger and don't want to switch, or just want to get the extra protection of blockers that use different methods, you can try an ad blocker like uBlock Origin or AdGuard.

Techniques for Compartmentalizing your Online Identity

Different browsers have different mechanisms through which you can separate parts of your online life into different "compartments." For instance, if you have to use the same devices for personal and work life, you might want to avoid being logged into the same sites, or having the same browser history, in each "compartment." For example: If you are using one compartment to search for safety planning resources and also using it to browse Facebook (or any social media platform), ads related to your safety planning search may show up in your

Facebook feed. The person that is monitoring your social media may be able to guess based on the ads that you are looking for information about moving to a specific new town, researching legal remedies, searching for a shelter or anything related to your search. This could happen even if, for example, you had been searching on your laptop while the person monitoring your social media only has access to your Facebook through your phone.

Browser Containers

The Mozilla Firefox browser has an available extension called Multi-Account Containers, that allows you to separate your browsing activity into compartments called *containers*. For example, you could have a "Personal" container, a "Work" container, a "Shopping" container, and a "School" container (the extension comes with some containers built in, but you can add and delete containers). If you are logged in to an account in one container, you will not be logged in to it in any other container.

Facebook Container

There is another extension that integrates with the Multi-Account Containers extension discussed in the previous paragraph, called Facebook Container, that compartmentalizes Facebook and Instagram activity – including blocking the Facebook tracking pixel, which is on about a third of websites and is used by Facebook to track your online activity and tailor ads and suggestions to you. Using the Facebook container, you increase your privacy by keeping Facebook from knowing your search and browser activity outside of Facebook and Instagram.

Browser Profiles

Google Chrome, Microsoft Edge, and Mozilla Firefox, all allow creation of multiple *profiles*, or compartmentalized personas, on the same device and browser. Each profile has its own separate cookies and browser history. Setting up different profiles can increase privacy in a similar way to containers, by keeping parts of your online life separated from each other – you might only log into certain accounts while using a certain profile, and you can log out of that profile when you are finished browsing. This can be a useful safer browsing feature, but it is important not to see it as an instant fix with no downsides. If someone has access to your device, they can still access any profiles you are logged into, not just whichever one you are using at the moment. For example: If you are logged into your Google account at work and searching for relocation resources, and if you are also logged into your Google account on your cellphone or desktop at home, a person that is monitoring your browser activity on your desktop at home or your cellphone will see that you were searching for relocation resources. Logging into a profile will log you into that profile on other devices connected to that account, which could accidentally expose a profile that you were using on a safer device to someone monitoring your activity on a less-safe one.

Encrypted Browsing

Using HTTPS (rather than HTTP) makes it more difficult for an abusive person monitoring your activity, a hacker, or anyone else, to read your Internet traffic remotely, as it is encrypted at every step of the way. HTTPS Everywhere is a free browser extension that will make sure that your communication with all websites uses HTTPS as long as it is technologically possible to do so. This is more useful to protect against someone who is trying to use technology to eavesdrop on your browsing activity. It does not hide your online activity from someone who can physically access your devices, or who has your passwords or other means of logging into your accounts or devices.

VPN Services

When you access a website or send an email, your unique IP address is shared and it can be used to get your approximate location. A VPN service (Virtual Private Network) hides your IP address from the websites you visit, and gives you a different public-facing IP address to increase privacy, as well as usually providing some level of encryption to prevent eavesdropping on your Internet traffic. This can protect you if a website where you have an account is hacked and the hacker publishes user data (something that happens relatively frequently).

How Do I Choose a VPN?

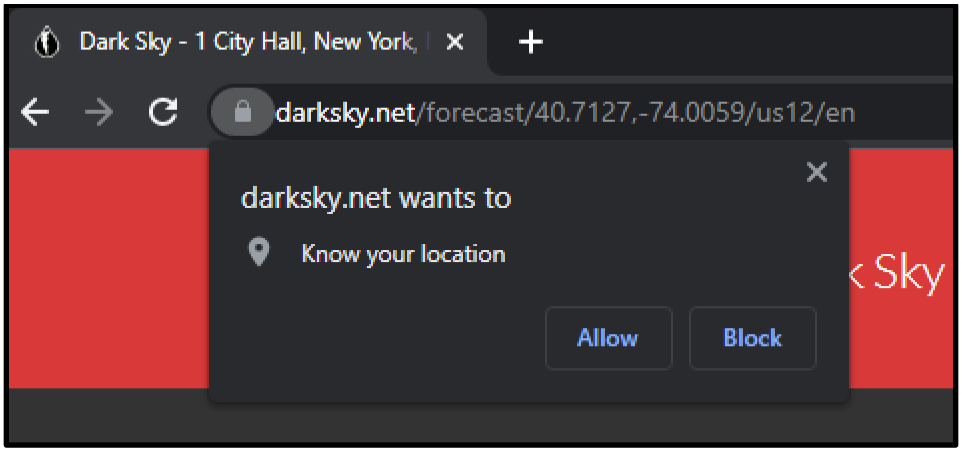
There are many options out there for VPN services. In general, paid VPN services will function better than free ones, and are less likely to be fronts for scams pretending to be a VPN service (though note that there are reputable free options, like the ProtonVPN, at the free tier). Most paid VPN services allow you to add more than one device to a plan, so one cost-saving option is to pool money with friends and purchase a plan that all of you can use. For instance, if a plan allows you to protect up to six devices, and three of you purchase it together, each of you can protect a phone and a laptop while only having to pay a third of the cost. In general, no-logs services, which do not keep records of your internet activity, like NordVPN, ProtonVPN, or Private Internet Access, are more secure than services that keep logs.

VPNs for Routers and Smart Devices

If you have smart devices (everyday objects that can be connected to the Internet and controlled remotely) such as Google Home or Alexa device, a smart thermostat, a smart fridge, or an internet-connected doorbell camera, these also have IP addresses. As mentioned above, IP addresses indicate your approximate location, and tech companies often store your IP address in your account data. If you are concerned about an abusive person finding your IP address, you may want to hide these devices' public IP addresses with a VPN service as well. This is possible by using a VPN-compatible router and protecting it with a VPN service, which will then protect the devices connected to it. Many VPN services can be used with VPN-compatible routers, though as of this writing, ExpressVPN has a reputation as having the easiest setup among router VPN options.

Precise Location Data: What Is It and What Does It Mean for Me?

Sometimes as you browse, websites may ask for your permission to view your location. Most commonly, this looks like a pop-up request.



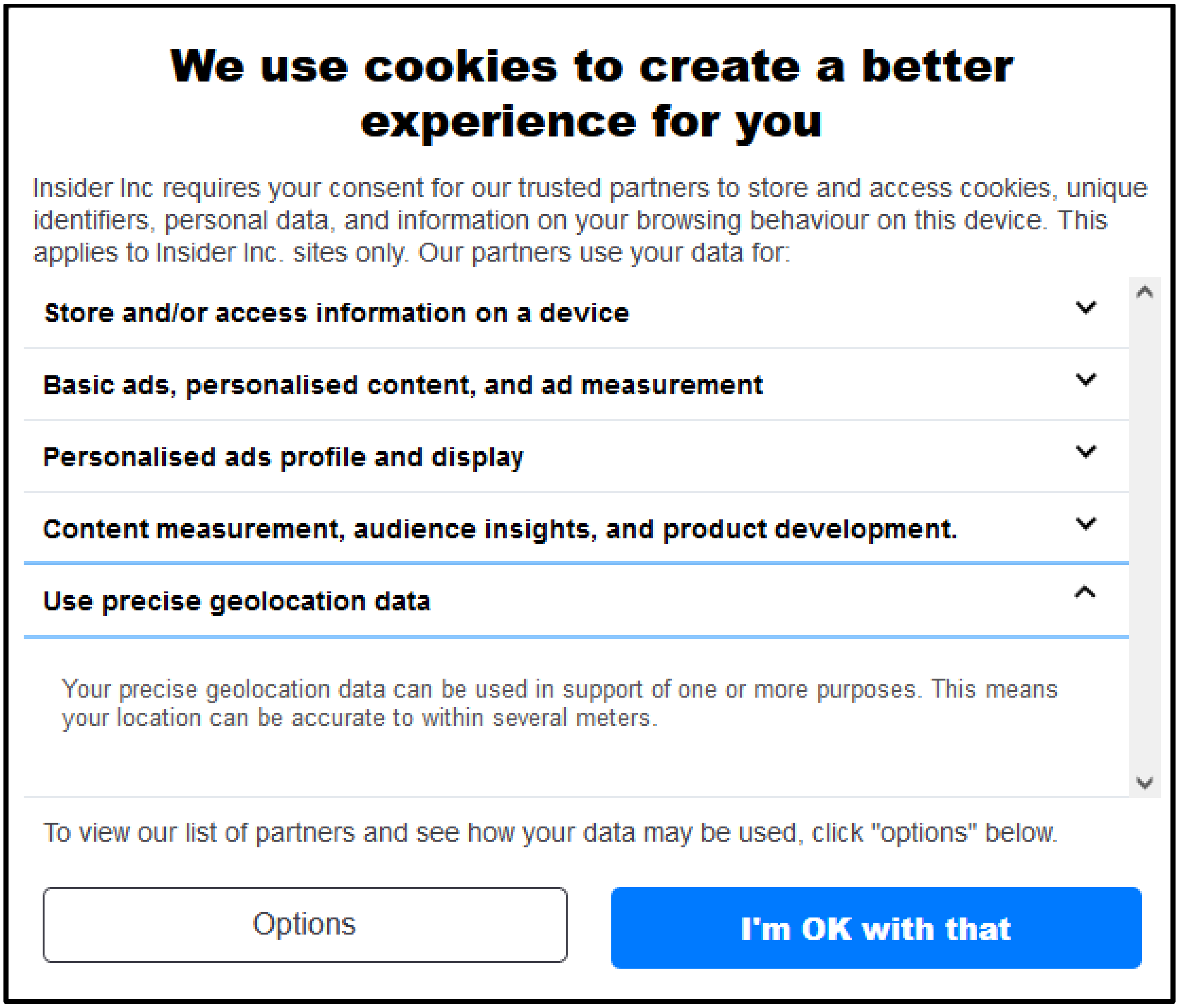
darksky.net wants to

Know your location

Dark Sky - 1 City Hall, New York,
darksky.net/forecast/40.7127,-74.0059/us12/en
Allow
Block
Sky

This type of request is not asking for an IP address – websites do not have to ask permission to record that. It's asking for location information provided by your browser, which is much more accurate (often within meters of your actual location). Websites are required to ask users for permission in order to read such precise location data.

Sometimes, the request looks different, as in the next example below. In this case, it is part of the website's general request to use your data so that they can collect, store, and sometimes sell information about you. It is often good privacy practice to reject these requests as much as possible, but because many websites make it more difficult or time-consuming, many people understandably click the "Accept All" button. Any given website may or may not be asking for precise geolocation data, but users typically don't see the *types* of permissions they're granting if they click "Accept All" without clicking whatever button may be available to see more information first. For instance, many people visiting the site from which this screenshot was taken (a news site) may not, if they do not click a button to view this information before clicking "Accept All," realize that they could be giving the site permission to record exactly where they are.



We use cookies to create a better experience for you

Insider Inc requires your consent for our trusted partners to store and access cookies, unique identifiers, personal data, and information on your browsing behaviour on this device. This applies to Insider Inc. sites only. Our partners use your data for:

Store and/or access information on a device

Basic ads, personalised content, and ad measurement

Personalised ads profile and display

Content measurement, audience insights, and product development.

Use precise geolocation data

Your precise geolocation data can be used in support of one or more purposes. This means your location can be accurate to within several meters.

To view our list of partners and see how your data may be used, click "options" below.

Denying permissions as much as possible is one way to control who stores or shares your precise location. However, there may be times when you want to use location-based website features – perhaps, for instance, you want to quickly see your local news or weather, and don't want the site to store your precise location, but don't mind if it stores your general area. Tools like the Location Guard browser extension can be strategically used to increase location privacy. Location Guard lets you set a fixed location for yourself, so if you wanted to give a weather site permission to know your general area but not your precise location, you could fix your location to the next town over.

Further Information

These tools are not the only means to increase your privacy while browsing. Browsers also have many privacy settings built into them. To learn about browser settings and how you can use them strategically, see our Browser Privacy Settings resource.

Supported by US DOJ-OVW Grant #15JOVW-21-GK-02216-MUMU. Opinions, findings, and conclusions or recommendations expressed are the authors and do not necessarily represent the views of the U.S. Department of Justice.

We update our materials frequently. Please visit TechSafety.org for the latest version of this and other materials.