DAY 3

Protect Your Browsing

Companies can track everything you do online: every ad you see, every button you click, your physical location, browsing habits and more. All that data gets collected together to reveal a picture of you for personally targeted ads for things ranging from shampoo to politics. Creepy? Yes. The good news is that you can partly defend yourself from this tracking without ruining the usability of the internet. Doing so is pretty simple.

Browser extensions are small add-ons that work inside a web browser and nowhere else. You can download them to your computer, set them up once and they will work to hide much of your browsing history. We recommend three different extensions to protect your privacy and security on a Windows computer, an Apple Mac computer or a Google Chromebook:

- uBlock Origin: Blocks ads and the data they collect (Chrome/Firefox).
- Privacy Badger: Blocks ad trackers (Chrome/Firefox).
- HTTPS Everywhere: Directs you to the most secure version of a website (Chrome/Firefox).

To install them, click on each browser extension and go to the link for your specific browser to download it. Then click the install button on the page that opens. If you use multiple browsers, you will need to download the extensions in each browser.

What about Safari?

Apple's Safari web browser does a reasonable job of protecting security, but in doing so it makes it difficult to install browser extensions. Both HTTPS Everywhere and Privacy Badger are unavailable on Safari because Safari lacks the extension capabilities required to make them work. The ad blocker, uBlock Origin, is available for Safari, but it's not made by the same

developer as the Chrome and Firefox version and may not receive updates as quickly.

What about Internet Explorer?

If you use Internet Explorer (now known as Microsoft Edge), you won't be able to use the extensions above. Edge also does a lot of eavesdropping on your browsing, and you're better off switching to a web browser like Firefox than trying to wrangle in the privacy settings in Edge.

On an iPhone:

On iPhone, you will use a "content blocker" instead of extensions. A content blocker is an app, downloaded from the App Store, that taps into the Safari web browser on your phone. Firefox Focus is both a web browser and a content blocker for Apple's default Safari browser. It works better as a content blocker than it does as a browser, and does the same work as Privacy Badger and some of what uBlock Origin does.

1. Download the Firefox Focus app for iPhone.

2. On your iPhone, open "Settings."

3. Tap "Safari."

4. Tap "Content Blockers."

5. Tap the toggle to enable Firefox Focus.

Firefox Focus blocks trackers and most ads. If you want more control over what type of content gets blocked and don't mind paying $5, get 1Blocker X, which works similarly to Firefox Focus but has more options.

On an Android phone:

Smartphones work differently than desktop browsers, but if you have an Android phone, you can use the mobile version of Firefox for web browsing. It

supports adding the same extensions linked above. Download Firefox onto your phone, then visit each extension page from Firefox:

- Firefox (Android)
- uBlock Origin
- Privacy Badger
- HTTPS Everywhere

Have you completed this?
Mark this task complete

Bonus

When you sign up for a new account for a service or online store, you often automatically opt into data collection about your shopping habits. Many sites, including Google, Amazon and Apple, allow you to opt out of this data collection. The website Simple Opt Out has a large list of how to opt out of data collection at different websites. You will have to do this manually, site by site, which can take a long time, but could be worth the effort long term, especially if you do it for the sites you use the most.

Why Am I Doing This?

Companies and websites invisibly track all of your web browsing. The data they collect reveals a lot about you. For example, you visit Brand A's website, then close the web browser, and you suddenly see ads for Brand A on Facebook and Instagram. That's because a third-party ad company embedded a tracker in the website and the tracker was able to figure out who you are and follow you around the web. At best these ads tend to creep people out and in worst-case scenarios

are used to manipulate behavior. Even if you don't mind any of that, it's still unsettling that companies take our data and then monetize it without our seeing a penny.

The browser extensions we recommend are the nuclear option for dealing with these ads and eliminating the worst offenders of security issues, like pop-ups that act as false alerts to get you to download bad software. **One note:** uBlock blocks all ads, which aside from preventing those sites from getting revenue, can also break some websites completely. It's easy to enable ads on websites you want to support: Click the uBlock Origin icon on your browser, then click the power button icon to turn it off on sites you want to support.

What About a VPN?

A virtual private network, or VPN, can double down on securing your web browsing, but it's not necessary for most people. If you travel frequently and connect to the public Wi-Fi found at airports, hotels and coffee shops, a VPN adds a layer of security. But it's important to understand the pros and cons of using one. If you decide you want a VPN, Wirecutter recommends Tunnelbear.