Brave Shields

and how to use them.

Brave browser seems like a normal browser when you first open it up. You type in a website into the URL bar, then press enter, and you're brought to the site you requested. However, over time you begin to realize that you no longer see as many target ads, or even any ads at all. You also notice that little Brave icon, indicating how many trackers and ads have been blocked. This icon is the Brave Shields control panel. But how does someone get the most out of this privacy control panel?

Brave has various different tracking prevention measures set in place, including an ad and tracker blocker, script blocking, and device recognition blocking. I'll go over each of these in sections to make it easier to understand.

Ad and tracker blocking

This shield is fairly simple to understand. Any ads or trackers on a page are automatically blocked. You can click the small arrow to the right of the dialog to view all trackers and ads that have been blocked on the current page, or you can simply glance at the number beside it to get a general idea of how many trackers and ads would have been on the site under normal conditions. The only two settings for this shield are on and off. To toggle it, just click the switch to the right of the dialog.

Connection encryption

The connection encryption shield is also very simple. Any network requests through HTTP will be automatically change to run on the more secure HTTPS protocol. All HTTPS requests are fully encrypted, so anyone spying on your internet connection would struggle to see what information is being transmitted between your computer, and the site you're connected to. The only two settings for this shield are on and off. To toggle it, simply click the switch to the side of the dialog. Just like the ad blocker, you can view all the connections encrypted by

clicking the arrow to the right of the dialog, or you can just glance at the number beside it to get a general idea.

Cookie blocking

Brave supports cookie blocking. By default all 3rd party cookies are blocked. This means that all cookies from external sites are automatically blocked. This drastically lowers tracking, while still leaving the user experience largely untouched. However, this setting will do nothing to stop tracking via cookies within the site. If you'd like to increase your privacy even more, you can choose to block all cookies. Keep in mind that this will likely break certain website features, including the 'Remember Me' feature on most websites with a login. If you would like, you can also completely disable cookie blocking, and allow all cookies from all sources. While this isn't recommended if you're concerned about privacy, it's certainly an option. To change this option, simply click the drop down menu, then select an option.

Script blocking

Script blocking will almost certainly break most modern websites, but doing so will greatly increase your security. Most websites use JavaScript to display alerts, manage menus, and display content. Unlike HTML, which is only rendered once, when you open the webpage, JavaScript can be updated in real time, which means it can detect when you take certain actions, including keystrokes and mouse position. For obvious reasons, this makes it really easy to track your activity. However, JavaScript is often essential to the operation of a site. While I'd advise keeping scripts on, you can disable them for certain, or all sites if you wish. To do so, simply click the drop down menu, then click 'Scripts blocked'. To turn scripts back on, toggle the setting back to 'Allow all scripts'.

Device Recognition

Device recognition is exactly what it sounds like: the ability for a website to identify your device. This setting is similar to the cookie blocking setting, in that there are three options: Block 3rd party recognition, block all recognition, or allow all recognition. I suggest blocking all recognition, but if not, blocking 3rd party recognition is a good idea too. So why would you want to block device recognition? I do it because of the reduced targeted advertisements. For

example, on the Microsoft webpage, you will often be shown ads for Windows 10 if you're on MacOS or Linux. Not only could this information be used to show you ads directly, but it could be sold to advertisers, which could use it to build a list of the devices you choose to use most often.