In many cases, the online ads you see are based on your search engine activities, what you do on social media, which websites you visit, and what you buy online. This is an ad displayed at the top of the USA Today homepage (www.usatoday.com).
The focus of this chapter is online advertising and how to prevent advertisers from learning too much about you. Topics include:

- When and where you’ll see ads online
- How information about you is collected and used by advertisers
- How to control the advertising you’re exposed to
- How to block online ads altogether

How Web Surfing Affects the Online Ads You See

Whenever you watch television, read a newspaper, browse through a magazine, listen to the radio, take a walk, drive down the road and see billboards, or open your mail, you’re going to see and hear advertisements. As consumers, we’re continually bombarded by ads.

Today, consumers spend less time using traditional forms of media and much more time using the Internet from computers and mobile devices. Where consumers go, advertisers follow.

Online Advertising Tracks Your Searches and Purchases

Advertisers currently spend 40 percent more on online advertising than they do on traditional advertising. In 2018, global online ad spending reached a record $579 billion, which explains why every time you go online, you probably see a lot of ads. For advertisers, many benefits
exist for using online advertising instead of traditional advertising. The two biggest reasons are that online advertising is highly targeted, and it’s extremely cost effective.

Often without our knowledge, advertisers are using new and cutting-edge technologies and online ad networks to reach us when we surf the Internet. The advertiser’s objective is to learn as much about us as possible, analyze our web surfing and online buying habits, determine our wants and needs at any given moment, and then target ads directly to us. They see exactly when we’re researching or shopping for a specific product or service.

Suppose you’re in the market to buy a new car. Chances are, before visiting a car dealership, you’ll surf the Internet and visit websites for car manufacturers that interest you. You also might look up reviews of the cars, watch videos that demonstrate those cars, compare the safety or performance ratings for several vehicles, and do research to determine how much your current car is worth as a trade in.

As soon as you type any keyword or search phrase into an Internet search engine, YouTube, or many other car-related websites, within moments, and for the next few days or weeks, many of the ads you see online will have something to do with buying a new car. You’ll begin seeing ads from car manufacturers, local car dealerships, and financial institutions that want to provide you with a car loan.

Almost like magic, these ads will follow you from the search engine you originally used, to your favorite social media services, and to many other websites you frequent. Without your knowing it, these ads are part of a massive ad network that shares information about web surfers (along with their interests and activities). This is not magic, but behind-the-scenes technology and sophisticated programming used by online advertisers, website operators, and online service operators.

If you’re active on social media, you might have discovered that shortly after you’ve created or updated your user profile, highly targeted online ads based on content from that profile begin appearing. For example, perhaps you mentioned in your profile that you are single or widowed and you included your age, religious beliefs, and sexual orientation. These profile-related questions are asked when you create a profile on Facebook, for example. As a result, ads for dating services that cater specifically to you, based on your age, religion, and sexual
orientation, will start popping up. Again, this is not a coincidence. The information was simply lifted from your public social media profile.

A lot of debate has gone on recently about online advertisers going too far when gathering and tracking information not only about web surfers, but also the collaborations online advertisers have established with online social media services (including Facebook) and search engine operators (including Google and Yahoo!).

Until better laws and industry-wide guidelines are put into place, you need to understand that your online activities are often being tracked.

Taking proactive steps to control what information becomes available about you to advertisers, and then on an ongoing basis, managing what types of online ads you are exposed to, is also up to you.

As you learned in Chapter 2, “Safely Surf the Internet,” one way to do this is to manage the cookies that your web browser collects as you surf the Internet. Some of the settings you can also adjust in your web browser’s Settings or Preferences menus include:

- The ability to turn on or off cross-site tracking. This feature will not eliminate the number of ads you see online. It will, however, help to prevent online advertisers from gathering and sharing data about you and your online activities in order to target specific ads to you.

- The ability to request that the websites you visit avoid performing any tracking. Many website operators automatically track your online activities when visiting their website. This information is often shared with advertisers. By turning on this web browser feature, every time you visit a website, your web browser will (behind the scenes) automatically request that your activities not be tracked and shared. This is only a request, and it may or may not be granted by the individual websites you visit.

- The ability to block all cookies or block just third-party cookies (which are the ones typically related to online ads). Blocking advertising-related cookies makes it much harder (but not impossible) for a website operator and its advertisers to collect information about you and your surfing habits. As you read in Chapter 2, instead of blocking all cookies (which will negatively affect your overall web-surfing experience), block only third-party cookies, while
keeping in mind that not all third-party cookies are advertising related. Some could also impact the experience you have while visiting the website the cookie relates to.

Later in this chapter, you’ll learn about additional ways you can manage and control the online advertising you see. This includes installing and using an optional ad blocker.

>>>Go Further

MANY ONLINE SERVICES RELY ON ADVERTISING REVENUE

Many websites and online services, including all social media services, are provided to web surfers for free. These companies are able to stay in business by relying almost exclusively on advertising revenue. So as a web surfer, you forego paying to access many online services in exchange for being exposed to online ads.

Website operators and online services can charge a premium to sell highly targeted advertising, which is why they’re using all sorts of tools to learn as much about you, the web surfer, as possible.

Most consumers are willing to see a few ads in exchange for receiving free access to their favorite websites, online services, and online-based content, but draw the line when what they thought was private information gets surreptitiously used by website operators and advertisers to maximize their profits.

To help you better control your information and manage the ads you see, tools have been built into all the popular web browsers, and you can add optional plug-ins to your web browser to provide even greater control of protecting your information and managing the ads you see online.

Much of the information in this book is provided to help you protect your identity and information from cybercriminals and hackers. However, many web surfers are also concerned about how overzealous online advertisers are using private information and details about their online activities to maximize profits.
Online advertisers are typically not breaking any laws, and they’re working within the guidelines you agreed to when you set up your individual accounts with various websites and online services. Although it’s not always easy, you can take steps to block certain efforts by online advertisers to exploit or misuse your information and details about your online activities.

**Educating Yourself About Online Advertising**

As a consumer and web surfer, you have the ability to stop most of the tracking and information collection done by website and online service operators as well as online advertisers. At the very least, you can use optional tools to discover what’s happening behind the scenes, so you’re not subconsciously influenced by the online ads you see.

You can take the following approaches to prevent your online activities from being tracked by advertisers, including:

- Preventing your web browser from keeping a log of all online searches you perform
- Deleting advertising-related cookies that have already been added to your web browser and preventing new ones from being saved in the future
- Adjusting the advertising-related settings for online services you frequent
- Turning on the private browsing feature that’s built into your web browser to avoid the storage of cookies or the tracking history of your online activities
- Installing an ad blocker web browser plug-in to prevent most ads from being displayed while you’re surfing the web

**Turning Off Targeted Facebook Ads**

If you’re one of the two billion active Facebook users, you probably know that your experience using Facebook involves looking at ads. Sometimes these ads are displayed along the right column of the web browser screen (if you’re using a computer), but sometimes ads are disguised as posts and are displayed as part of your newsfeed, for example.
After receiving a huge backlash from its users related to how personal information was being collected and then used by its advertisers, Facebook has given its users additional tools to manage the ads they see and determine what information is shared with advertisers.

Adjust the Settings Related to Your Social Media Accounts

The focus of Chapter 7, “Use Social Media Safely,” is on how to customize the security and privacy settings related to popular social media services, including Facebook, Instagram, and Twitter.

In addition to whatever changes you make to your web browser (including the addition of privacy or security-related plug-ins), as a Facebook user, you should manually adjust your Facebook ad preferences and other privacy-related settings.

If you’re a Facebook user, be sure to manually adjust the privacy and advertising-related settings for your account.
Also, anytime you’re given the chance by a website or online service operator to adjust advertiser- or privacy-related settings pertaining to that site, you are responsible for adjusting them to a level you’re comfortable with. Note that the default option almost always gives the website or online service operator the most freedom possible to use your information in whatever ways it deems suitable.

Adjust Facebook Ad Preferences

To manage ad settings related to Facebook, visit www.facebook.com/ads/preferences and follow these steps:

1. From Facebook’s Your Ad Preferences screen, click each of the menu options, one at a time, and adjust each of the settings to a level you’re personally comfortable with. The options available from this main menu and related submenus get updated often and will vary based on the type of equipment you’re using to access Facebook.
2. Click the Your Information menu on the Your Ad Preferences screen, followed by the About You tab to prevent Facebook’s advertisers from using information related to your Relationship Status, Employer, Job Title, or Education from being used to determine what advertising you’ll see.

3. For data that appears within your Facebook profile that you don’t want used by advertisers, turn off the corresponding virtual switch. For example, if you don’t want to see online dating service ads because your relationship status is listed as single, divorced, or widowed, turn off the virtual switch associated with the Relationship Status option.

4. To reduce the amount of tracking Facebook uses related to your online activities in order to show you highly targeted advertising, click on the Ad Settings option on the Your Ad Preferences screen shown in step 1.
For each of the three submenu options—Ads Based on Data from Partners, Ads Based on Your Activity on Facebook Company Products That You See Elsewhere, and Ads that Include Your Social Actions—click on each option one at a time. Here I will click Ads Based on Data from Partners.

When the Ads Based on Data from Partners submenu option expands to explain what information is being tracked, click the Allowed pull-down menu and choose the Not Allowed option, as opposed to the default Allowed option.
7. For the third submenu option (Ads that Include Your Social Actions) shown in step 5, choose the No One option, as opposed to the default Only My Friends option, to prevent your online Facebook friends from seeing what ads you’ve liked and responded to.

8. On the Your Ad Preferences screen shown in step 1, click on the Hide Ad Topics submenu option. You can click options, for example, to prevent ads related to Alcohol, Parenting, and Pets from being displayed while you’re using Facebook. You can choose to hide relevant ads for six months, one year, or permanently.
Search Engines, Websites, and Facebook Share Information

The websites or online services you visit often share your data among themselves and their advertisers or the ad networks they’re working with. If you look up a topic using the Google or Yahoo! search engine, for example, you’ll almost immediately begin seeing related ads when you use Facebook or another popular online service (or vice versa).

To keep Facebook from acquiring or collecting certain types of information, be sure to customize your Facebook account’s privacy and ad-related settings. As you’ll learn from Chapter 7, this process begins by visiting www.facebook.com/settings.

Recognizing Online Ads

The online advertiser’s goal is to capture your attention while you’re surfing the Internet. After an advertiser gets your attention, it typically wants you to click the ad to visit a website and potentially place an online order for its product or service.

Online ads can take many forms, including:

- **Banner ads**: These typically rectangular or square-shaped display ads appear prominently at the top, bottom, and often on the sides of webpages that display ads. Some banner ads use animated graphics and contain sound that you can turn on or off.
• **Fake news or advertorials**: Some articles you’ll discover on the Internet, including those promoted by popular search engines and shared on social media, are not legitimate articles from a credible news source. Instead, they’re sometimes “fake news” articles written with a strong bias and paid for as an ad, but promoted to you as an article. On Yahoo! or Facebook, for example, these look like regular posts, but somewhere near the headline, you’ll see a tiny banner that says, “Ad” or “Sponsored.” You need to look carefully to see it.

This sample of Yahoo!’s main home page shows news headlines from a wide range of credible sources displayed. Mixed in with these headlines are sponsored advertorials, like the one shown here. Chances are, without looking carefully, you won’t be able to tell the difference.

**Fake News Is Sometimes Hard to Detect**

As you’ll discover in Chapter 7, telling the difference between real news articles from credible news sources and “fake news” articles that an organization is paying for you to see is sometimes difficult. Often the intention of these articles is to mislead you...
Educating Yourself About Online Advertising

into thinking you’re reading a fact-based, unbiased, legitimate news story, when in reality what you’re reading may be something else entirely. The goal for these articles is also to encourage you to share the fake news story with your online friends, in hopes your sharing will give the fake news story added credibility.

Just because something is posted on the Internet does not make it true or factual, regardless of how the information is packaged and presented. Some fake news articles you see published online are simply ads that use a different format or a biased advertorial that a company has paid for you to see.

- **Graphic display ads:** These ads can be displayed in many different sizes and shapes anywhere on a website you’re visiting. They often use animation and sometimes sound to get your attention. However, when an ad includes sound, you’ll need to click on a tiny speaker icon to turn on the sound.

![Example of a graphic display ad](image)

This is an example of a graphic display ad for Booking.com on the USA Today.com website.

- **Pop-up ads:** These ads are displayed in a pop-up window that appears in the browser window you have open. These are being used much less frequently these days, because too many web surfers find them annoying, plus many web browsers now give web surfers the option to block pop-up windows altogether.
• **Search ads**: When you use an Internet search engine, such as Google or Yahoo!, and then view your search results, the results are intermixed with paid ads. To determine the difference between an actual search result and an ad, you need to look carefully for the word “Ad” or “Sponsored,” which will be part of the paid ad listing. Similar search ads often appear on other websites that are part of the same advertising network. A search ad typically includes a headline, one sentence of text, and a link to a website. Some also contain a logo or small photo.

• **Video ads**: These tend to be short, video-based commercials that either take over your entire screen, or that you view in a window on the website you’re visiting. YouTube, for example, often plays video ads before videos you’ve requested to watch, and occasionally as a “commercial break” during longer videos.

### Using an Ad Blocker

So far in this book, you’ve learned about methods to manage the online ads you see when surfing the web and visiting your favorite websites or online services. Another option is to install an ad blocker plug-in to block most (but not all) online ads.

### The Dilemma Related to Ad Blockers

Most online services and website operators rely on the money earned from advertising revenue to stay in business. By blocking ads, you’re still taking full advantage of the free online-based service or content that’s being offered to you, but you’re preventing that website or online service operator from presenting you with ads that allow them to earn money.

Whether or not you’re comfortable using an ad blocker to prevent most ads from being displayed when you’re surfing the web is a personal decision.
Defining Ad Blocker

In most cases, an ad blocker is an optional web browser plug-in that once installed and activated will automatically remove all ads from any webpage or online services you visit using that web browser.

A few web browsers (like Opera and Qliqz) have an ad blocker built in, while Chrome, Edge, Firefox, and Safari have a feature that works on some compatible websites that removes online ads and ancillary content from an online article, and then displays that content in a way that’s easier to read and print.

Some optional antivirus or malware protection software also includes an ad blocker feature. However, because so many different types of ads now exist that take on different text, graphic, video, and audio formats, no ad blocker will be 100 percent effective. Still, when you use one, you’ll be exposed to far fewer ads.

Finding an Ad Blocker

The easiest way to find an ad blocker designed specifically for your web browsers is to visit the online directory of plug-ins that’s maintained by the web browser’s developer. Chapter 2 provides a listing for these.

Figure Out What You Want

Before you start installing web browser plug-ins, figure out what you’re trying to accomplish and what additional functionality you want to add to your favorite web browser.

For example, this chapter focuses on using an ad blocker to prevent online ads from being displayed as you web surf.

However, if your goal is to manage cookies, you’ll need to install a different type of plug-in, in addition to or instead of the ad blocker. (See Chapter 2 for details on managing cookies.) To find a cookie manager plug-in, type the keyword “cookies” or “cookie manager” into the search field in the plug-in directory.
This figure shows the online directory of extensions (plug-ins) for the Apple Safari web browser (for Macs). You have hundreds of plug-ins to choose from, but there are several ways to quickly find and install exactly what you’re looking for.

The Safari Extensions Online Directory

These options, which are available from all the plug-in directories for the various web browsers, include:

- Type the name of a plug-in, or a keyword/search phrase associated with a type of plug-in, into the Search field, and press Enter. The related search results appear. Click one search result listing at a time to view detailed information about that plug-in, and then either click the related Install button or follow the provided link to download and install it.

- Access the Categories or Sort-By dropdown menu and click one of the listed categories to search for a particular type of plug-in.

- The extensions directory for Google Chrome allows you to narrow your search by choosing a filter, such as Runs Offline, By Google, Free, Available for Android, or Works with Google Drive.
• Browse plug-ins based on their rating. Like software or mobile apps, the online plug-in directories allow users to rate plug-ins using between one and five stars. When looking at the average star-based rating, also pay attention to how many individual ratings the average is based on. If a plug-in has 5,000+ five star ratings, that’s more credible than a plug-in with a five-star rating average that’s based on just 10 individual people who rated it.

• Check out what’s recommended. In the Google Chrome extensions directory (https://chrome.google.com/webstore/category/extensions), for example, Google offers round-ups of plug-ins that fit into specific categories and that the company recommends. You can find recommendations under the headings, “Recently Updated,” “Editor’s Picks,” or one of the narrower category-specific headings, such as “Get Started” or “Everyday Extensions.”

Click a plug-in’s listing to access its Description screen. From here, you’re able to read an overview of the plug-in and learn what it does, read its reviews, access support from its developer, or learn about related plug-ins by clicking the Overview, Reviews, Support, or Related tabs, respectively (when using the plug-in directory for the Chrome web browser, for example).

Click the link provided to download and install the plug-in. Most plug-ins are free. Others either have an upfront price associated with them to purchase the plug-in or require an ongoing paid subscription for the plug-in to fully function.

Find, Install, and Use an Ad Blocker Plug-In

Regardless of which web browser you use, the process for finding, installing, and then using an ad blocker is pretty consistent. The following are the steps for visiting the Chrome Web Store, and then downloading, installing, and using an ad blocker, called AdGuard AdBlocker, with the Chrome web browser. Each web browser has many ad blockers to choose from. This is only one example.

1. Launch the Chrome web browser on your PC or Mac. (Not shown.)
2. Visit the online directory of plug-ins for your web browser. For Google Chrome, the website address is https://chrome.google.com/webstore/category/extensions.

3. In the Search field near the upper-left corner of the browser window, type the search phrase **Ad Blocker** and press Enter.
4. In the search results that appear, click one of the extensions in the listing to access its Description screen. For this example, click AdGuard AdBlocker.

5. From this plug-in description screen, you can see it has more than five million users, and a 4.75 average star-based rating. Click the Add to Chrome button.
6 When prompted, click the Add Extension button.

In a few seconds, the Thank You for Installing AdGuard screen appears. You can now use the on-screen menu to configure the plug-in. In this case, there are five options that you can turn on or off. Based on the description for each option and your personal preferences, decide how you want to set each of them.

7 In a few seconds, the Thank You for Installing AdGuard screen appears. You can now use the on-screen menu to configure the plug-in. In this case, there are five options that you can turn on or off. Based on the description for each option and your personal preferences, decide how you want to set each of them.
8 Notice that the AdGuard logo now appears in the upper-right corner of the web browser window. This indicates the plug-in is installed and functional. Click the icon to access the menu to manage it.

After the plug-in is installed and functional, use the web browser to continue surfing the web as you normally would. When visiting websites and online services that typically contain ads, you’ll likely notice those ads no longer appear (or fewer ads appear).

The YouTube home page (www.youtube.com) typically displays ads. The ad blocker is not currently active, so you can see ads.
Each time you visit a webpage, if ads are blocked, a number will appear in the lower-right corner of the AdGuard icon located near the upper-right corner of the browser window.

A Plug-In Upgrade Option Is Often Available
What you’ll discover from many plug-ins is that the basic functionality is offered for free. However, to unlock a more robust set of features and functions, you’ll need to upgrade to a premium version of the plug-in, which typically costs money. Whether you choose to do this is optional.

Depending on the ad blocker plug-in being used, it will prevent most (not all) ads from being displayed, but it may not actually stop a website operator or online advertiser from tracking your online activities and gathering information about you.

Turning On a Pop-up Blocker
Some website operators and online services use pop-up windows to display certain content, including ads. These, however, are being used much less frequently, because most web surfers find pop-ups extremely annoying.

To help you avoid them, a pop-up blocker feature has been added to many web browsers. If your favorite web browser does not offer this feature, chances are an optional pop-up blocker plug-in is available.
Pop-Up Windows Must Be Manually Closed

After pop-up windows start opening when you’re surfing the web, you have to manually close each to get rid of it. This typically slows down your web surfing experience, and adds a lot of clutter to the screen.

As its name suggests, a pop-up blocker prevents pop-up windows from appearing when you’re surfing the web. If accessing the content being displayed in a pop-up window is essential to the functionality of a particular website, a message appears asking you to unblock the pop-ups for that website.

After you turn on the block pop-ups feature once, pop-up windows remain blocked until you manually adjust this setting in the future.

Turn on Edge’s Pop-up Blocker

To turn on Edge’s pop-up blocker feature, follow these steps:

1. Launch the Edge web browser. (Not shown.)
2. Click the Settings and More icon (three horizontal dots) displayed in the upper-right corner of the browser window.
3. Click the Settings option.
4 Click the View Advanced Settings button.
5 Click the Block Pop-Ups virtual switch to turn on the option.
Turn on Safari’s Pop-up Blocker

To turn on Safari’s pop-up blocker feature, follow these steps:

1. Launch the Safari web browser.
2. Click the Safari dropdown menu.
3. Select the Preferences option.
4. Click the Websites tab in the screen that appears.
5. On the left side of the window, click the Pop-Up Windows option.
6. In the lower-right corner of the window, select the Block and Notify option from the When Visiting Other Websites dropdown menu. Doing this blocks all pop-ups but gives you the option to open one when it exists.
Turn on Chrome’s Pop-up Blocker

To turn on Chrome’s pop-up blocker feature, follow these steps:

1. Launch the Chrome browser.
2. Click the Customize and Control Chrome menu icon (three vertical dots).
3. Click the Settings option.
4. Scroll down and click the Advanced option.
Scroll down and click the Content Settings option.
Scroll down and click the Pop-Ups and Redirects option.
Click the Blocked (Recommended)/Allowed virtual switch option to turn it off. The option should say “Blocked (Recommended).”

A similar pop-up blocker feature is built in to the web browser you’re using on your smartphone or tablet.

**iPhone or iPad**
To turn on the pop-up blocker, launch Settings, tap the Safari menu option, and then tap the Block Pop-Ups virtual switch to turn on the feature. From this menu, you’ll find many other privacy and security-related features that are equivalent to what web browsers running on computers offer.

**Android-based Smartphone or Tablet**
To turn on the pop-up blocker feature, launch the Chrome web browser. Tap the menu icon located in the upper-right corner of the screen. Tap the Settings option. Tap the Site Settings option. Tap the Pop-Ups and Redirects option. Tap the Pop-Ups and Redirects virtual switch to turn off the feature, so the option says, “Block sites from showing pop-ups and redirects (recommended).”
Choosing an Ad Blocker Alternative

Instead of removing ads from all your web surfing experiences, there’s an easy way to strip away ads and other clutter when you’re trying to read online-based articles or review a lot of text on a compatible webpage.

Safari (for the Mac as well as the iOS mobile devices) has a built-in feature called Reader. Microsoft Edge has a similar feature called Reading View.

When using Safari, any time you’re trying to read an article on a compatible website, simply click the Reader icon to the left of the Search/Website Address field, and all the ads, graphics, and other on-screen clutter that surround the text-based article will be stripped away, making the on-screen text much easier to read and/or print. Most news-oriented websites support the Reader or Reading View feature.

Use Edge’s Reading View Feature

When you visit a popular news-oriented website, such as CNN.com, and click a news story, you can read the article, but the screen often contains a lot of ancillary clutter, including ads.

1. After you find an article you are interested in, click it. The article appears in the browser window. As you can see, a lot of clutter is surrounding the article, including multiple ads.

2. Turn on the Reading View feature by clicking the book-shaped Reading View icon to the right of the Search/Website Address field. (This feature is not compatible with all websites, but it works with most news-oriented websites.)
After you click the Reading View icon, all the on-screen clutter is immediately removed, and the text and photos from the actual article are much easier to read.

To customize the on-screen appearance of the text being viewed with the Reading View feature turned on, as soon as you click on the Reading View icon, click the “aA” icon in the gray bar that temporarily appears below the Search/Website Address field. To make this gray menu bar reappear, click near the top of the screen.

From the menu that appears, you can adjust the font size and choose between three page themes. Click the printer icon to print the newly formatted page.
Use Safari’s Reader Feature

This example uses the USA Today website and the Safari Reader feature.

1. Click an article you are interested in. The article appears in the browser window. It is surrounded by a lot of on-screen clutter, including ads.

2. Click the Reader icon in the Search/Website Address field.

3. You can now read the same article and its related photos without the on-screen clutter and ads.
Click the “aA” icon to the right of the Search/Website Address field to adjust the font size, change the font, and/or alter the background color. This affects the appearance of the article you read on the screen, as well as the formatting if you choose to print the article.

**A Plug-In for Other Web Browsers Is Available**

Although the Reader or Reading View feature is not built in to all browsers, in many cases the same functionality can be added using a free plug-in. For example, the Reader View plug-in ([https://addon.com/chrome-reader-view.html](https://addon.com/chrome-reader-view.html)) is available for Chrome and Opera.