Don't Make it Easy for Companies and Advertisers to Track You Online!

This article shows you how to:

- ✓ Avoid leaving a trail of personal data everywhere you go online
- ✓ Set your web browser to help prevent tracking
- ✓ Switch to a search engine that respects your privacy

You're leaking. Almost everywhere you go online, you're leaving little drips of information about yourself. These drips are mopped up by large companies that want to build a 'profile' of you. They do it to make money, of course, but all this data can be used for a more sinister purpose: to manipulate your views and behaviour.

It's time to plug these leaks! Read on to learn what you can do to stay more private and anonymous online.

What is My 'Data' (and Why Does it Matter)

Example: a typical Google search

Let's go back to those drips of information and explain them with an example. You visit Google and search for 'best investment funds' (or perhaps you simply type that phrase into your web browser's address box and your browser automatically searches with Google).

Looking through the search results, you click a link to an article that reviews several investment funds. A few minutes later, after reading that article, you go back to Google's results and pick another article on the topic.

It provides a lot of data!

You haven't done anything wrong – you're just using the Internet – but several companies have just picked up some valuable information about you:

Google knows what you searched for

- **Google** knows you've just searched for investment funds; followed a link about investments funds; seemingly stayed there long enough to have read the page; came back and followed another link. So clearly you're interested in investment funds.

Ad companies saw where you went

- **Advertising companies** have learned much the same. The two articles you read were probably accompanied by ads, even if you didn't notice them, and those ads were almost certainly placed there by one of a handful of advertising companies. They know you visited pages about investment funds.

So did social networks

- **Social media sites** such as Facebook, Twitter, LinkedIn and others may have had their own little buttons displayed on the two articles pages you visited. If so, they also know what you were reading about.

Websites have noted your visit

- **The two websites you visited** obviously know you were there too, and that you arrived as a result of searching for 'best investment funds'. Perhaps they'll store this information for future reference.

All this data is added and combined

To you or me this is 'information'. To the companies I've just mentioned, it's 'data': it's combined with what they already know about you, stored, analysed and comp-ared to data held about other people with similar habits to deduce a little more about you.

What these companies have just learned about you

It was one innocent search, but several companies now know you seem to be interested in investment funds. That suggests you have money to invest, which implies you're reasonably well-off. It also suggests you're financially prudent, which implies you're not young, and it shows you know something about investing.

All this might combine to say something about your education level, your employment status, and perhaps even your political leanings.

This builds a detailed profile of you

All that from just one search! Admittedly, some of it is guesswork, but how many other searches have you done in, say, the last year? What websites have you visited? What have you bought, booked or subscribed to online? What have you 'liked' on Facebook, who have you followed on Twitter or Instagram, what have you watched at YouTube?

This latest search may or may not have added new data about you, but it has probably helped to confirm or negate other snippets of data. All that data builds an increasingly-accurate profile of you – one that likely knows more about you than any human being does.

Your targeted with advertising – or worse

That profile is used to target you with advertising, even to the extent of receiving junk email with uncanny similarities to your recent web travels. But recent events have shown that it can have far more devious uses, such as targeting people with particular political views and swaying their voting decisions.

There's also the issue of what happens if this data is given or sold to third parties (as happened in the Facebook/Cambridge Analytica scandal), or is stolen by someone hacking into a website (as happens dismally often). Once our data is out there, we really have no control over who gets to see it or how it's used.

It's up to us to protect ourselves

For many large online companies, their whole business is based on collecting this data, so they're not going to stop voluntarily. Instead, it's up to us to stop feeding them our private information, so let's look at the most important ways of doing that.

Cookies: Don't Let Your Own PC Do the Dirty Work!

Our data is stored in 'cookies' on our PCs

If companies are going to track you, you might think they'd have the decency to store the data on their own computers. In many cases they don't; they store it in files named 'cookies' on your PC. Cookies are created and managed by your web browser, and one of the best ways to thwart tracking is to delete all your cookies. That way, next time you visit a certain website (or see ads supplied by a certain advertising company), they have no past data about you to build on: it's as if this is your first visit.

The disadvantage of deleting cookies is that they can also be helpful. For instance, a website might store a cookie on your PC containing your username for that site, making it quicker to sign into it, or containing preferences you've chosen for how the site looks or behaves. By deleting the cookie, you lose those features. However, the privacy you gain by clearing out all your cookies tends to outweigh the few benefits of keeping them.

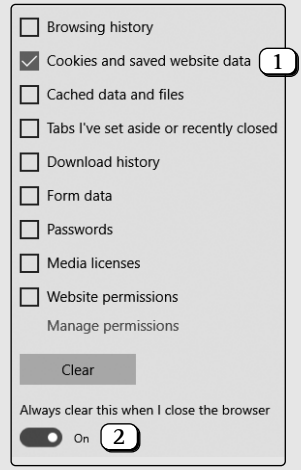
Delete cookies automatically

There are two steps I suggest taking. The first is to have all cookies deleted automatically each time you close your browser. The second is to refuse to accept 'third-party cookies', which are almost always cookies created by advertising companies whose ads appear on the pages you visit (and therefore a type of cookie you definitely don't want!).

Here are the steps to do both of those things in Microsoft Edge, Mozilla Firefox and Google Chrome:

Microsoft Edge:

1. Press Ctrl + H to open the Hub panel at the History section.
2. At the top-right of this panel, click **Clear history**.
3. You'll see a list of check-boxes, some ticked, some not. Untick items as necessary so that the only item that remains ticked is **Cookies and saved website data** (1).
4. Further down, below the words **Always clear this when I close the browser**, click the switch to turn it to **On** (2).
5. At the very top of this panel, click the double-chevron.
6. This takes you to the first page of Edge's Settings panel. Scroll down and click the **View advanced settings** button.



Have cookies deleted when you close Edge

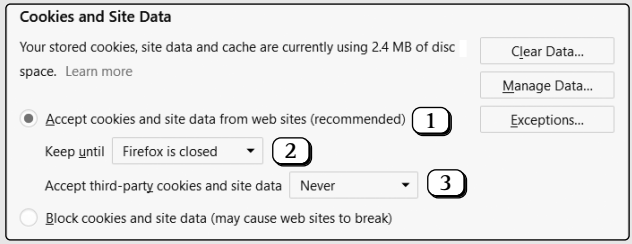
Block third-party cookies

7. Scroll down again and near the bottom you'll find a 'Cookies' heading. Below this, choose **Block only third-party cookies**.
8. Press the Esc key to close the Settings panel.

Mozilla Firefox:

Choose these settings in Firefox

1. Click the 'Open menu' (three horizontal lines) button at the far-right of the toolbar and choose **Options**.
2. At the left of the Options page that opens, click **Privacy & Security**.
3. Below the heading 'Cookies and Site Data', click the option **Accept cookies and site data from web sites (recommended)** 1 if it isn't already selected.
4. Just below that option, alongside **Keep until**, choose **Firefox is closed** 2.
5. Alongside the next option, **Accept third-party cookies and site data**, choose **Never** 3.



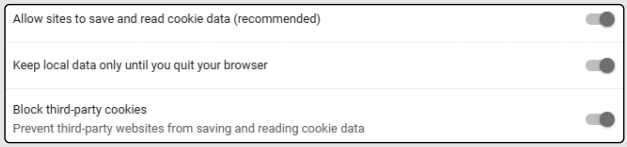
While you're here, Firefox offers two extra anti-tracking features that are worth switching on. A little further down the page, below the 'Tracking protection' heading, you'll see two groups of options: select the **Always** option in both.

6. Close the tab containing this Options page (for instance, by pressing Ctrl + W).

Google Chrome:

1. Click the menu button (three vertical dots) to the right of Chrome's address box and choose **Settings**.
2. Scroll to the very bottom of the page and click the word **Advanced**.
3. Now scroll down some more, and near the bottom of the white box containing the list of 'Privacy and security' options, click on **Content settings**.
4. On the page that opens, click on **Cookies**.
5. Now, if they're not already enabled, click the switches beside the first three options (pictured below) to turn them all on, causing them to turn from grey to blue:

Switch on all three items in Chrome



6. Finally, close the tab containing this Settings page (for instance, by pressing Ctrl + W).

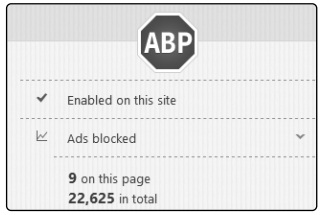
Avoid More Tracking by Using an Ad Blocker

Tracking doesn't always involve cookies

While blocking and/or deleting cookies is certainly a vital step in maintaining some privacy, not all companies rely on them. The fact that you've reached a web page on which they display an ad instantly tells them you were there, and they store that data on their own servers rather than in a cookie on your PC.

A good ad blocker removes trackers from web pages

Therefore, another excellent step in thwarting trackers is to install a free 'add-on' (otherwise known as an 'extension') for your browser that blocks the majority of ads, along with anything else from companies known to engage in tracking and snooping.



Doing this gives you a double win: not only are you defeating a sizeable number of companies trying to track you, but you're also getting rid of all the most irritating ads!

Recommended: Adblock Plus

The ad blocker we rec-ommend is Adblock Plus, and it's available for Edge, Firefox, Chrome and Internet Explorer. Visit www.adblockplus.org to find out more about it, and you'll be able to follow a link to your web browser's own library of add-ons to install it. Once installed, Adblock Plus takes care of itself: you simply install it and forget about it.

Don't Tell Websites Where You Are!

Some websites want to know where you are

Here's a very quick and simple tip, but it's one that's worth pointing out. Every so often you'll arrive at a website that wants to know your location.

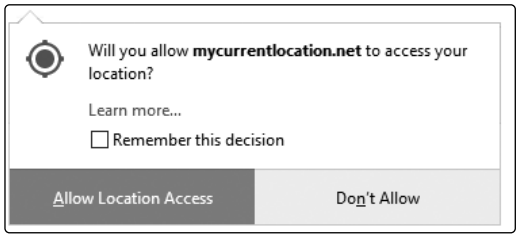
Your web browser may or may not be able to pass that information back to the website (much depends upon your PC, your version of Windows, which web browser you're using, and a few other things).

You should always be asked

However, the good news is that you should always be asked whether you're willing to supply that information. In the example pictured opposite, it's Firefox asking. Chrome shows a similar panel at the top of the browser, while Edge and Internet Explorer display a wide panel at the bottom of the window.

My advance is simple: always say No! Click **Don't Allow or Block** or whichever option means 'No'. The only websites that need to know your location are those that need to deliver something to you, and they will obviously always have to ask for your postal address.

Always refuse!



Lock Down Your Social Media Accounts

Do you use social media? In other words, do you have accounts at websites like Facebook, LinkedIn, Twitter, Instagram, Google+ and Snapchat?

If you do, you were probably encouraged to create a 'profile' containing a fair amount of personal information – not just your name and photo, but perhaps your date of birth, your employment and education history, your hobbies and interests, and so on.

Have you filled in social media profiles?

As I mentioned earlier, this may be 'information' to you, but it's 'data' to the companies who want to track you, and once you've supplied it there's no knowing who's going to get their hands on it (as demonstrated by the Facebook/ Cambridge Analytica scandal earlier this year).

They may not be as secure as you think!

My advice is to log into your social media accounts to review what data you're giving away and to whom:

- Make sure your profile is set to 'private' so that it's visible only to those people you've accepted as 'friends' or contacts.

Keep your profile private

Weed out unknown 'friends'

- Check through your contacts to make sure you really do know them all and weed out any that shouldn't be there.

Trim your profile to the bare essentials

- Check what valuable nuggets of personal data you're giving away in your profile. I'll touch on this more in 'Ask Yourself: Do They Really Need to Know That?' on page 13, but a key point to consider is this: your family and friends already know these things about you, so they don't need to be repeated here, and no-one else really deserves to know these things, so they shouldn't be here!

You might feel that with your profile set to private and a carefully-chosen list of friends, there's no harm in telling everyone more about yourself. But remember, this is the Internet: even ignoring the possibility of data theft by hackers, your information is only as private as this website wants it to be. (Rather than bringing up past scandals yet again, I'll just leave that thought with you.)

Have you posted any private details?

- Check your past posts to see whether you're giving away any valuable information about yourself, your friends or your family and delete anything that ought not to be shared.

Location: off!

- If you're prompted to give your current location when posting, don't.

Check what information Facebook apps and games are collecting

- Facebook allows you to add apps and games to your page, most of which are offered by third parties. The first time you use one of these apps, you give it permission to access certain parts of your profile. In most cases it wants to know your name, which is fairly harmless, but some apps might ask to access quite a lot more. If so, consider whether the app has a justifiable need for that information, and whether you trust it. For

apps you've already used on Facebook, check the permissions you've already granted them and remove any permissions you feel a particular app shouldn't have, or remove the app itself.

- Don't take part in surveys and quizzes on Facebook and its equivalents. In doing so, you're handing over your profile details along with your answers, and (if you read the small print) possibly agreeing that it can be sold or shared with third parties.

Don't trust quizzes and surveys

- At some websites you visit, you can choose either to set up an account with that site itself or sign in using one of your social media accounts. The second option is often tempting: it saves you the palaver of having yet another account and one more password to remember. However, by signing into sites using your Facebook or Google account, for instance, you're giving that site access to your profile, your posts, your contacts... and potentially your friends' information too. That's far more data than any website deserves to have handed to it on a plate!

Don't sign into websites with a social network account

Use a Search Engine that Isn't Tracking You

It's tempting to think of Google as a search engine company because that's how it started and that's what it's become famous for. It isn't though – it's an advertising company.

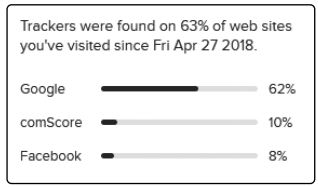
Who knows you best? Probably Google

The key to successful advertising is putting your ads in front of the very people most likely to click them, and to do that you need to know as much as you can about as many people as possible. If you're fortunate enough to be running the world's favourite search engine, handling 65,000 searches per second, you can learn a vast amount about an individual by tracking what they search for and which links they click, building a profile that's being updated and refined every time they search. Indeed, it's often said that Google knows us better than our closest friends or relatives!

Use a search engine that respects your privacy

So another excellent way to claw back some privacy is to stop using Google for your web searches and to use a different search engine instead – one that doesn't track you. There are several dozen of these to choose from, but here are two of the best:

- **Startpage** (www.startpage.com) is essentially a private version of Google. It sends your search term to Google and displays the results, but without providing Google with any identifying information about you (or, of course, storing any itself).
- **DuckDuckGo** (www.duckduckgo.com) is my personal choice for its privacy and simplicity. For Firefox and Chrome users there's also an optional DuckDuckGo add-on available which silently defeats most attempts to track you at any website you visit.



Don't Use Just One Web Browser

How do they know it's you?

Something you may have wondered about this tracking business is: 'How do they know it's me?'. How can Google tell that the person who searched for 'spanish villa rentals' last week is the person who visited a web page about tooth whitening this morning?

Your web browser is a big giveaway

Chiefly it's your web browser. Although it's basically the same browser that's used by millions of other people (Firefox, perhaps), it has some distinctive features, such as the combination of add-ons installed. This information is available to Google (and every other website you visit), along with details of the exact version of Windows you use, which country you're in, who your broadband supplier is, and more.

With this information, plus the use of cookies and a few slightly-sneaker tricks, a website can distinguish your browser from everyone else's with near-certainty.

Alternate between two or more browsers

That leads to another tip worth considering: use two or more web browsers! For instance, have one browser devoted to Facebook, but do all your other surfing in a second browser. That way, Facebook has no way to connect the data they've picked up about you in 'Browser 2' with the Facebook profile you've logged into in 'Browser 1'.

Popular, free web browsers

As a Windows user, you already have Internet Explorer (and, in Windows 10, Microsoft Edge). To those, you can add one or more of these popular free browsers and simply start whichever you want to use at any given moment:

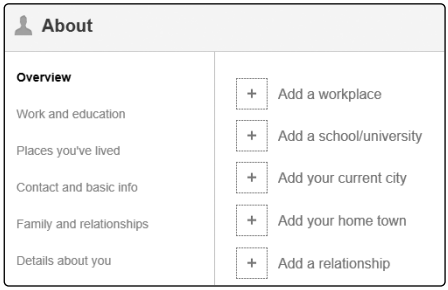
- Mozilla Firefox: www.firefox.com
- Google Chrome: www.google.com/chrome
- Opera: www.opera.com
- Maxthon: www.maxthon.com
- Avant Browser: www.avantbrowser.com

Ask Yourself: Do They Really Need to Know That?

We often hand over data willingly

Companies don't always have to be sneaky to gain information about us. Sometimes they just ask for it innocently, and we hand it over.

Facebook and other social sites ask for your work and education history, past and present addresses, phone numbers, notable life events, family details and more. If you were to fill in all those sections, the sites would probably know more about you than even your closest friend! And that's before you post anything, 'like' anything or add contacts.



Why should you trust this website with your information?

Hence my earlier advice to 'lock down' your social media accounts, deleting anything that needn't be included. Here's a good way to approach this: imagine an unknown person telephoned you and started asking for all these details. Would you tell them? If you wouldn't, then you don't want to tell this website either, and you certainly don't want to tell its 'carefully chosen partners' or the criminals trying to steal its data.

Your date of birth should be secret

Other data you hand over comes in smaller chunks. You might be asked for your date of birth by sites that require you to be a certain age, but there's no reason to be honest about it – just pick a date at random. Or, like the Queen, have an 'official birthday' you use online.

Your date of birth really is valuable information. As I discovered to my cost, criminals now need only a name, address and date of birth to set up a bank account in your name. Since names and addresses are quite easy to find, your date of birth has suddenly gained a role similar to that of your bank card's PIN number.

Likewise, some websites ask you 'security questions' such as your mother's maiden name, the town in which you were born, or name of your first school. Again, there's no reason

to tell the truth and it's safest not to: invent whatever you like and keep a note of your answers.

Check what Windows 10 apps can learn about you

If you use Windows 10, there's one other situation to be cautious about. When you install apps from the Microsoft Store, they need your permission to access certain information from your PC – your contacts list, your location, your email, your calendar. Always ask yourself whether these requests seem reasonable, and refuse them if you they don't. For example, if an app you're installing wants permission to access your contacts, is that really necessary? For an email or mess-aging app, yes. For a photo-editing app? Certainly not!

You can check what permissions you've given to apps you've already installed in Windows 10, and withdraw any that don't strike you as necessary. Open the Settings app by pressing ⊞ + I (the letter 'i') and click **Privacy**. Click **Location** at the left, and if you scroll down a little on the right you'll see a list of apps that have permission to know and track your location, with simple On/Off switches for each. There are similar lists of apps that can access your contacts, calendar, account info, camera and so on – click the appropriate item at the left to see those lists and make any changes you like to apps' permissions.

What Secrets is Your Phone Passing On?

It's not only PCs that matter!

Here at *PC Knowledge for Seniors*, we're chiefly concerned with PCs, of course, but an article like this wouldn't be complete without mentioning mobile phones (and some of what follows applies to tablet computers such as iPads as well).

Some of the advice I've given above takes on a whole new significance with mobile phones, for two reasons: they're always on and they go everywhere with us.

Your phone can pass on detailed information about your habits

Take location as an example. On your PC, you're probably always in the same place, so all anyone could learn is roughly where you live. But they could learn a vast amount from the location service on your phone: you're always out from 10–2 on Thursdays; you favour Starbucks for coffee; you do your weekly shop on a Tuesday morning; you take a regular walk or jog; you're currently in Tenerife...

Are your apps collecting more data than they really need?

As in Windows 10, apps you install on your phone (or tablet) must ask for permission to access your location, contacts, messages and so on: always refuse permissions that seem unnecessary for a particular app. For example, it's understandable that a maps app would need to know where you are, but if a card game wants to track your location, you should be suspicious that its maker has ulterior motives.

Note too that your phone gives you a way to review and change the permissions you've given to apps you've already installed. And, before installing an app, read its reviews and the permissions it's going to request. Remember, too, that some apps exist primarily to harvest data from you.

Keep your phone's Wi-Fi switched off!

Here's one final tip that's specific to mobile phones. When you're out and about, switch off the Wi-Fi connection when you're not actively using it. As you move around, your proximity to different Wi-Fi networks can be used to track your location (sometimes with almost as much accuracy as your phone's location service), regardless of whether your phone connects to any of those networks or not. With Wi-Fi enabled, an app that hasn't asked to know your location might still be able to track you everywhere you go.