
The
TOP 10
WAYS
To Protect
Your Privacy
Right Now
DATA DESTRUCTION, INC.

The **Top 10 Ways** to Protect Your Privacy Right Now

How much is your personal information worth?

You may think that you've got nothing to hide and that no one would be interested in your browsing data or the details of your last medical appointment. Unfortunately, that's not the case.

Hackers use personal information for the purposes of identity theft, medical insurance fraud, to gain access to your financial accounts, or any other number of nefarious schemes. But it's not just hackers and other stereotypical "bad people" who are willing to pay a lot of money for what you may consider to be inconsequential personal data.

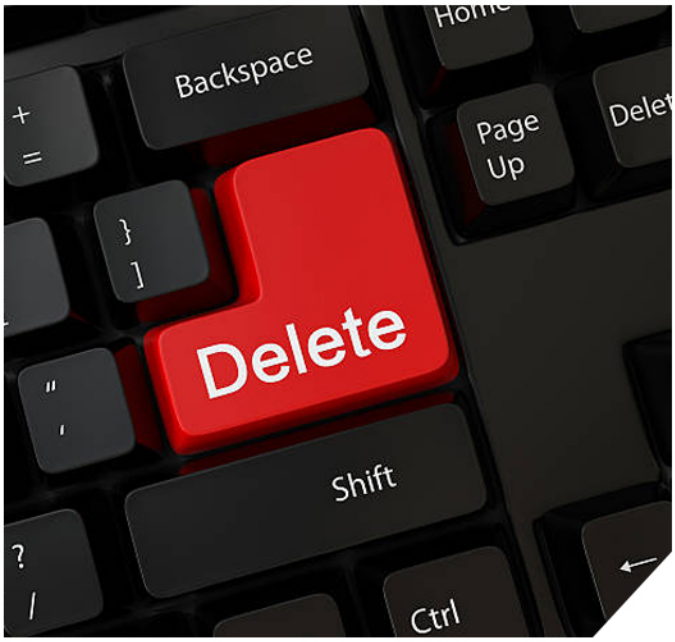
Companies want access to your personal demographics, your browsing history, shopping history, location, and whatever else they can get so that they can serve ads and attempt to sell products and services to you.

Anyone who uses the Internet or a mobile device is, to some extent, leaving themselves open to a privacy breach. But there are simple actions you can take that will go a long way towards protecting yourself and your privacy.

Here are our top ten ways to protect your privacy right now (plus one bonus tip).

Protecting Your Privacy Tip 1

Go Further Than **Deleting** Your Files



Did you know that moving a file to your Recycle Bin and then emptying the bin doesn't actually destroy the file?

Let's use a library as an analogy, where the books represent the files and folders on your computer. Back in the old days, when you wanted to find a specific book you would look it up in the card catalog, and these days you would use a computerized library database. When you "delete" a file on your computer, even after you empty the Recycle Bin, all you have done is remove the corresponding entry in the card catalog or computer database. The book is still sitting on the shelf right where it was before, and you have simply removed the record that tells you where to find it.

That might be enough to stop the majority of everyday computer users from finding the file, but a hacker is not your everyday computer user. They have the tools and the knowledge to find the file, along with everything else that you thought you had deleted in the past.

The only way to completely remove data from a hard drive is with hard drive data wiping or, if you don't intend to use the computer again, with hard drive shredding.

Protecting Your Privacy Tip 2

Be Aware of What You're **Syncing**

Most people's cell phones and other mobile devices contain just as much personal information as their home and work computers do, and there is a very common way that some people are inadvertently sharing data from their cell phones.

Many devices are set to automatically sync whenever they are connected to a computer via USB. This means that, while you may think that you are simply charging your cell phone when you plug it into your work computer, or a computer at

a friend's house, or even a public computer via a USB cord, there could be a disturbing amount of data being transferred between the two devices without permission and sometimes without notice.

Instead of charging your cell phone from a computer via USB, use an AC adapter to charge your device directly from the power outlet.

Protecting Your Privacy Tip 3

Separate Your **Email Identities**

It is a good idea to have at least three email addresses, each serving a different purpose. Your personal email address should only be given to family and friends and should never be used to create online accounts, or entered on competition entry forms or anywhere else. It should be treated with the same level of respect as you treat your physical home address.

A separate email address should be used for social media accounts, website sign ups, and any kind of physical form that requires an email address.

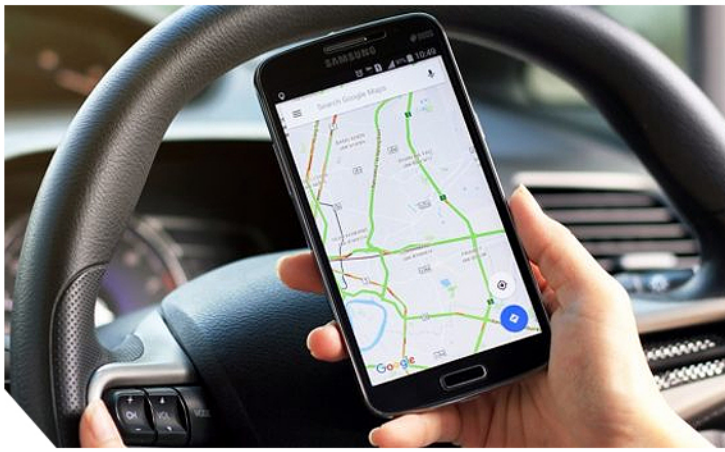
A third email address can be maintained for work, study, or customer service purposes as necessary.

Separating your email addresses in this way allows you to keep your social media profiles separate from your work, study, and other areas of your life. With only one email address, it can be disconcerting knowing that anyone who has your email address can, for example, look you up on LinkedIn or Facebook.

Protecting Your Privacy Tip 4

Keep Your **Location** to Yourself

Wherever possible, turn off location or tracking data. While location data can legitimately be used to help you find local services, to deliver targeted advertisements, and even to track your daily movements, it can also be used to track your everyday movements.



It is a good idea to use a proxy server or virtual private network (VPN) at all times, making it impossible for your real location to be tracked and recorded.

Protecting Your Privacy Tip 5

Turn Off Fingerprint Phone Unlocking

The advent of fingerprint sensors to unlock cell phones and mobile devices seemed like a boon for personal privacy, but it has also come at a price. While law enforcement and federal agents cannot force you to reveal a PIN or passcode to gain access to your cell phone under your Fifth Amendment rights, they can in some circumstances force you to use your fingerprint to unlock your phone.

This has turned out to be an unexpected side effect of fingerprint sensors, making it a good idea to bypass fingerprint technology altogether and stick with a secure PIN or passcode.

Protecting Your Privacy Tip 6

Keep Your Software **Updated**

You've chosen your software based on its reputation and safety features in addition to its usefulness, now the next step is to keep your software updated. Hackers are always looking for the tiniest loophole or vulnerability to exploit software, and software developers do their best to fix small issues before they become major problems.

Most modern software solutions feature auto updates, and it is vital to allow auto-updating to occur and to manually check for updates on any software that doesn't update automatically. Sure, it can be annoying installing updates, especially if it involves restarting your computer, but this minor inconvenience could save your personal privacy.

Protecting Your Privacy Tip 7

Take Removal Media One Step Further Than **Formatting**

Do you remember when USB thumb drives stored a maximum of 256 MB of data and cost well over $100? These days, removable media is infinitely smaller and of phenomenally higher capacity, for a much cheaper price. As useful as thumb drives and SD cards can be, they also pose a security risk should they go missing or be stolen.

As we discussed in Privacy Tip 1, simply formatting removable media doesn't actually erase the data. Treat removable media with respect while it is still being used, and then use **certified equipment destruction** to destroy it once it is no longer needed.

Protecting Your Privacy Tip 8

Stay Away from **Public Wi-Fi**

If you're running low on mobile data, free public Wi-Fi can seem like the perfect solution. Unfortunately, public Wi-Fi is unsecured and an easy target for hackers to gain access to other people's devices.

The best advice is to avoid public Wi-Fi altogether. If you do still choose to use it, keep in mind that it is not too far-fetched to think that every page you visit and every piece of data you enter is being monitored and possibly even recorded. At the very least, turn off file sharing before connecting to any public Wi-Fi network.

Protecting Your Privacy Tip 9

Protect Your Browsing Data

Have you ever had the experience where you've used your regular web browser to search for something like flight prices, then when you perform the same search the next day the prices have increased? That's because ad networks have the ability to track your every move while you're using a web browser, and they'll use this information to deliver targeted advertisements as well as taking the opportunity to raise the prices on products or services they know you're interested in.

The solution is to block all Internet trackers, making it so much harder for anyone to track your browser and search history back to you. Google Chrome features the Incognito Mode, and if you prefer another browser you can install an extension such as Ghostery which will serve the same purpose.

Protecting Your Privacy Tip 10

Be **Password** Proactive

Passwords: the simplest way for anyone to gain access to your online accounts. It is unfeasible for anyone to create and memorize unique, highly secure passwords for every account they create online, which is why most people tend to use the same password for everything. While this does make life simpler, it also means that anyone who finds out your password to one site can potentially have access to every membership site you use.

The solution is to use a password manager like Dashlane, LastPass, or 1Password. These managers can not only help you to store and catalog your passwords, they can even create highly secure, 10 digit-or-longer passwords for your accounts. All you need to do then is to create and memorize one highly secure password to operate your password manager, then let it take care of the rest.

It is also a good idea to turn on two-factor authentication wherever it is offered, which sends a code to your mobile device which must be entered whenever you log in from a new location. Yes, this can be annoying, but it can also be the difference between hackers gaining access to your account or not. At the very least, turn on two-factor authentication for your password manager.

BONUS Protecting Your Privacy Tip 11

Know What to **Shred**

Do you need to shred every piece of paper that has your name on it? Not necessarily, but it wouldn't be going too overboard if you did. **Paper shredding** is accessible and affordable, and it makes sense to use secure document destruction to securely dispose of any documents if you would feel uncomfortable having them in the hands of a stranger.

At a minimum, shred any paperwork that contains medical information; financial, banking, or credit card account numbers; your birth date; or any part of your Social Security number.

Moving Forward

It may be tempting to think that your data and your online browsing is so mundane that it would be of little use to anyone, or that hackers prefer to large corporations than an individual user. But hackers are little more than opportunists and will strike whenever they can. In addition, companies and ad trackers aim to gather as much information as they can about everybody, not just a small section of society.

Your bank accounts, social media accounts, and even your browsing history is your business, and it is well worth any minor inconveniences to implement the above tips to protect your privacy.

Resources

Data Privacy Day: Easy Tips to Protect Your Privacy (https://www.forbes.com/sites/gordonkelly/2017/08/13/apple-iphone-8-design-specs-camera-price-release-date/#61fbaaa811f7)

5 (Not So Obvious) Ways To Protect Your Privacy Online (https://www.forbes.com/sites/willhayes/2016/01/28/five-ways-to-protect-your-privacy-online/#d96b63a118c6)

66 Ways to Protect Your Privacy Right Now (https://www.consumerreports.org/privacy/66-ways-to-protect-your-privacy-right-now)

11 Simple Ways to Protect Your Privacy (http://techland.time.com/2013/07/24/11-simple-ways-to-protect-your-privacy/)