How to Delete Your Digital Footprint

In today’s digital world, there is no such thing as personal freedom and true privacy. With the advancement of the internet and technology that makes information readily available and trackable, there is nowhere you can hide that the government and cyber criminals can’t find you.

That is unless you work hard to delete your digital presence. The only way you can become untraceable today is to make it seem as if you never existed in the first place, which is a pretty hard thing to do.

However, though deleting a digital footprint is incredibly time-consuming, it’s not impossible. If you are truly committed to going off the grid, there may be a way to do so. And even if you don’t want to completely disappear, cleaning up your digital footprint is always a good idea as it can help protect your data and reduce your chances of being the victim of a cyber-attack or identity theft.

Going Off Grid: Is It Possible?

The term “big brother is watching” is more real today than it ever has been before, thanks to the internet and advanced technology. Everything is available, traceable, and connected. It doesn’t matter how far you go or what you do to cover your tracks; if someone really wants to find you and has the means to do so, they probably can.

Passwords, firewalls, and encrypted networks help, but ultimately, your information is readily available to anyone who has the skills to hack through those systems. And despite the notion that you have some semblance of privacy and protection from government spying, you don’t.

Thanks to the American Freedom Act, FISA courts and government agencies are allowed to violate our 4th Amendment protections. So that, combined with the invention of highly advanced tracking and surveillance technology, means there is really nowhere you can hide.

So this begs the question – is going off grid truly possible?

The answer depends on how far you are willing to go to become untraceable. If you want to continue living a "normal" life, but just want to have more privacy, this is possible, but you will 100% still be trackable. There is no way you can live in society without leaving some sort of trace behind.

However, if you move to some remote island or jungle and live as below the radar as possible, you can have much more privacy and be much less traceable. But even then, it will never be as if you never existed. If you do something to piss the government off, for example, they have a whole host of advanced systems at their fingertips that they can use to find you.

So is it possible to completely disappear? No. But for the average person who isn't on the run and does want some more privacy or at least wants to better protect and hide their information, this is possible. But again, even cleaning up or wiping out the majority of your digital footprint will take a lot of work.

Becoming Untraceable

If you have no ties to society and have the means to disappear to some remote location, that's the best way to live off-grid. However, most people today don't have the means or skills to do so. For the average person who wants to live off-grid, they will likely be capable of falling somewhere in between truly living off-grid and simply being less easy to track.

No matter where you fall on the "wanting to live off-grid" spectrum, however, it's helpful to understand first how different levels of privacy work when it comes to becoming untrackable.

- **Level 1:** The first level of privacy involves doing minimal work to cover your tracks. Family, friends, or acquaintances might not be able to find you at this level, but someone with a little more skill, like a PI, probably could.
- **Level 2:** At this level, a little more effort is required. You would need to place all accounts such as your car, phone numbers, utilities, and computer accounts under an alternate name. You would also want to destroy documents and anything else containing sensitive information to be untraceable at this level, as well as using encryption services. You can still be found, but it will cost maybe around $5k or more.
- **Level 3:** To obtain level three privacy, you are going to have to fork out a lot more money and more significantly alter your life. You will need to move somewhere new, pay cash for most things (especially property and vehicles), and use an LLC to cover up your name. You will also need to make sure your legal name is no longer on tax documents. At this level, you could carefully keep in contact with some close relatives or friends, but it would cost a significant amount of money and

effort for anyone else to find you.

- **Level 4:** At this level, you are attempting to become hard to track by government agencies. However, keep in mind that you would really only need to hide at this level if you have done something wrong and are a criminal. But, if it's the route you're going, you will need to move somewhere remote, change your name, and never work or pay taxes again. You won't be able to have contact with anyone you know, and you will have to completely change your lifestyle and avoid anything that could connect you to your previous life. This includes going anywhere where facial recognition cameras could detect you.

How to Protect and Delete Your Digital Presence

If completely going off-grid is not possible for you, but you still want to become more untraceable and keep your data safe, the following tips can help:

Encrypt Your Network

If you can't avoid using the computer and the internet, then make sure your network is encrypted. This will help protect your information by encoding the data that is transmitted and communicated over a computer network. When doing this, it can be incredibly helpful to first use a network diagram to get a visual representation of all the components that make up your network. There are a lot of ways that different devices are

connected and communicate, so having a map of your network and connected devices can give you a better idea of where your data is going and how to protect it.

Be Mindful of Your Operating System

Not all operating systems are the same, and some are more protected than others. Widows, for example, is one of the worst systems because it is highly vulnerable to security breaches. A Mac OS is a little better but can also get quite expensive. Linux is really your best option for best security and affordability.

You should also consider using an OS that doesn’t connect to the internet to protect certain private information. Even if you are storing your information on your computer hard drive and not in the cloud, your OS could still upload that information to the internet with the click of a button. So to protect your most private digital information, you may want to partition your computer and store the private data on the half that isn’t connected to the internet.

Find and Delete Old Accounts

Think back to when you first got a computer and started using the internet. Now think about how many different accounts and subscriptions you have signed up for since then. Probably hundreds, maybe even thousands – and every single one of those accounts, even if it’s no longer active or being used, is another way you can be traced or hacked.

This step can be one of the hardest because most people don’t keep a running list of all the online accounts they’ve ever signed up for. Your best option is to look through your emails. Anything you are still signed up for is likely still sending you emails. So start going through your current email account and following emails back to the source website to delete your accounts.

This includes trying to log back into old email accounts. If you can access all of your old email accounts, you can likely trace down most websites where you have an account with your information.

Use a More Secure Browser

Just as your operating system could be compromising you, so can the internet browser you use. Internet Explorer is notoriously one of the least safe browsers. But while Google Chrome is supposedly the safest, there has been evidence of Google using people's data for unethical purposes. So some better options include Brave, Tor, and Firefox.

Avoid Apps

The second you download and sign up for a new app, you are agreeing to give that company the right to use your personal data. So it's a good idea to go through and delete your account from old apps and get rid of current apps that you don't need. If you do need to use an app, make sure it has good privacy settings and allows you the option to opt out of giving them use of your personal data.

Don't Shop Online

Online bill paying and e-commerce is one of the easiest ways to track someone. Unfortunately, as the world becomes increasingly digital, more and more companies prioritize digital services over paper services. Still, if you want to protect your information, the best way to do so is to avoid putting it out there in as many places as possible.

The goal is to minimize your online presence. So if you can, avoid online shopping and using online bill pay. If you can't avoid it, make sure the company you are using has heavy protections in place to secure your private data.

Wrapping Up

Honestly, there are many other steps you can take to further protect your data and wipe out your digital footprint. The list could go on and on, including deleting social media accounts, managing privacy and location settings on your phone, using ad blockers, and more. The key is to avoid computers that can leave behind a digital trail as much as possible. And if you do have to use a computer, be extra mindful of privacy settings, encryption services, and overall where you put or give access to your information.