Concerned About Privacy on the Internet? Here's How to Avoid a Digital Trail

Opinions expressed by *Entrepreneur* contributors are their own.

Have you ever just been on Facebook or Instagram and seen an advertisement that is eerily relevant to you? If so, you may be concerned about your digital footprint: What information are you giving away? Who is watching it? What do apps, organizations and even governments know about you? If you're an avid social media user and/or dealing with sensitive issues in your personal life, you may be worried about how you could be tracked online and how your activity may be used against you. In this article, I will list a few ways in which you can avoid leaving a digital trail — but first, it's important to understand how a digital trail is created in the first place. Here's how it happens:

- **Monitoring on the web:** Everything you do on the internet is being tracked. Your search history, your location, the apps you install, the content you interact with — everything serves as a data point in services like recommendation systems and fraud detection. If you're an individual experiencing mental health issues, you may search for therapy, psychiatric medication or potential complications. You may also be Googling symptoms that indicate depression or anxiety. You may (inadvertently) share information about your issues on social media or via messaging apps. All of this forms a digital trail; a company or app tracking you can use and sell this information.

- **Smart Monitoring and user profiling:** Recent trends in machine learning have made user profiling extremely powerful. Models can now determine who may like what products and in what colors and sizes. There are algorithms in place that systematically compute likelihoods of a user falling prey to certain marketing tactics or being susceptible to certain issues. A company that has access to sufficient information about you may be able to "predict" when you are pregnant, what tendencies you have or even what your sexual orientation is. This can be used to tailor advertisements you receive or even put you on certain watch lists.

So, how do you avoid leaving a digital trail? Follow these valuable tips below:

Share wisely on social media

Be mindful of the things you are posting on your Facebook, Instagram and Twitter. If asking about health concerns, be careful who your posts are visible to. Review your friends and followers routinely, and keep your privacy settings to the highest. As a general rule, avoid posting about any sensitive issues or information that you are not willing to share with just anyone. Even if you post it in a private group, and have the most restrictive privacy settings, your friends and followers may not – they could share it with their network, or their accounts could be compromised.

Related: Safeguarding Digital Identities: Why Data Privacy Should Matter To You (And Your Business)

Turn off location tracking

Many apps use your location for better recommendations and detecting fraud (for example, an unusual transaction on a credit card). Google Maps often stores the places you have

visited. Other applications (like Snapchat and Instagram) may also be passively using your location in the background. Be sure to take a look at location permissions in your phone settings, and disable it for all applications on a periodic basis.

Search in anonymous mode

When you're browsing the internet, I would suggest that you always browse using the anonymous or incognito mode. This ensures that your searches aren't recorded in the browser history. Any friends, family or even law enforcement who access your phone will not be able to check what search terms you entered or what pages you visited. No cookies (tracking elements placed by websites on your computer or phone) are retained – so those websites cannot track you. This prevents a website from profiling you and tracking your activity across different websites. An important thing to remember is that while your activity will not be visible to other users of the computer, your internet service provider (ISP) can still view and record what you are doing.

Use VPN services

A VPN service like NordVPN or ExpressVPN keeps your activity private and allows you to disguise your IP address as you use the internet. Your ISP or the websites you visit can no longer track you based on your IP (they can still record the IP, but it won't actually be yours!). You can change your IP address as frequently as you want. Since location is determined by a reverse lookup of the IP, this also effectively hides your location. It will also allow you to access geo-restricted content – if your state or country decides to block information on certain topics, you can choose an IP address from another state, and then gain access to that content.

Related: You're Probably Being Tracked Online Right Now.

Here’s How to Protect Yourself

Use encrypted messaging

If you are sharing any sensitive information with your friends, be sure to share it via a secure messaging app. Applications like WhatsApp are end-to-end encrypted – meaning that these messages cannot be intercepted and decoded, even by governments. Even better, use an app like Signal, which allows messages to “disappear” after a set time. Both Signal and WhatsApp are free to download and use.

Send documents using links

Often, you may want to share documents or medical reports with someone, and once you send it as part of an email or chat, it could potentially be used against you. If you want to send someone a document, first upload it in a secure cloud service like Google Drive, OneDrive or Dropbox. These services allow you to generate secure links to share with specific people. Once the other person has viewed the file, you can disable the link. Once disabled, clicking the link leads into nowhere. If you want to take it a step further, use a URL shortener like BitLy or TinyURL to generate a short, nondescript link, which even hides the actual website you are linking to.

Use throwaway email addresses

Many websites need you to sign up with an email address in order to access content. If you find yourself on such a website, do not use your real email for verification – use a throwaway email address. Websites like TempMail allow you to generate email addresses and receive emails on it for a short period of time. You can create as many as you want and use a different one every time. This way, you avoid sharing your real email – if the website is ever breached, your identity

will not be exposed.

Related: How to Be Invisible Online – Without Going Off the Grid (Infographic)

While it is nearly impossible to guarantee complete anonymity on the internet, these techniques should provide a good starting point. Be sure to follow other best practices of digital hygiene, too: Choose long, random passwords, do not share or reuse passwords, and do not click on suspicious or unknown links.

https://www.entrepreneur.com/article/431536