How to protect your "Digital Footprint"

Posted At : September 27, 2019 11:25 AM | Posted By : Admin
Related Categories: Internet, Security

The term "digital footprint" goes back to at least 2014. However, it's now become a popular term and it's something that everyone that uses the Internet for anything has.

Your “digital footprint” includes all traces of your online activity, including your comments on news articles, posts on social media, and records of your online purchases.

When you know the boundaries of your digital footprint and take steps to contain it, you can help protect your identity and your reputation.

What is a digital footprint?

Every time you post something online, share content, or even when a website collects your information by installing cookies on your device, you are creating a digital trail. This includes your IP address, your login details, and other personal information that you reveal online. Information that is posted about you also gets added to your data trail.

What your digital footprint can say about you?

It’s a good idea to have a positive digital footprint. This information is your digital identity, and it could show up when someone searches for your name online.

Your online identity can influence different aspects of your life. For example, employers, schools, colleges, and law enforcement officials could use your digital footprint as a basis for character assessment.

Types of digital footprints

Digital footprints can be classified into two broad categories — active and passive footprints — which depends on how your information is acquired.

Active digital footprints

Active digital footprints consist of the data you leave when you make deliberate choices on the internet. For instance, posts you make to your social media channels are a form of active footprint. When you are logged into a project management or similar site, changes you make that are connected to your login name are also part of your active footprint.

Here are a few examples of active digital footprints.

1. Posting on Facebook, Instagram, Snapchat, Twitter, and other social media platforms
2. Filling out online forms, such as when signing up to receive emails or texts
3. Agreeing to install cookies on your devices when prompted by the browser

Passive digital footprints

Passive digital footprints are those you leave behind without intending to or, in some cases, without knowing it.

For instance, websites that collect information about how many times you've visited recently are adding to your digital footprint in a passive fashion. That's because you don't choose to give them this data. They collect it when a device at your IP address connects with their website. This is a hidden process, and you may not realize it is happening at all.

Here are three examples of passive digital footprints.

1. Websites that install cookies in your device without disclosing it to you
2. Apps and websites that use geolocation to pinpoint your location
3. Social media news channels and advertisers that use your likes, shares, and comments to profile you and to serve up advertisements based on your interests

Both active and passive footprints can be tracked and observed in multiple ways and by multiple sources.

6 steps for protecting your digital footprint

Organizations like the Family Online Safety Institute recommend tracking your digital footprint and taking steps to control it. Recommended steps include:

1. Enter your name into several search engines.

Use multiple search engines to perform a search for your first and last name. If you've recently changed your name, look up both your prior name and your current one. Try the common misspellings as well.

Review the first two pages of results. Are they positive? Do they show you in a professional and respectable light? If anything comes up that you don't like, ask the site administrator to take it down.

Setting up Google Alerts is one way to keep an eye on your name. Every time it is mentioned somewhere you will get a notification. If you have a common name, it may help to attach keywords to your search, such as your location or activities that may associate your name with a Google alert.

Real estate websites and whitepages.com may have more information about you than you might want disclosed. Personal information like your phone number, address, and age tend to show up. Get in touch with the websites and have that information removed.

2. Double-check your privacy settings, but don't trust them.

Privacy settings on social media allow you to control who sees your posts on your social media streams. Spend some time getting to know these settings so you can use them fully.

For example, Facebook allows you not only to limit posts merely to friends, but also to make customized lists of people who can see certain posts. But don't assume that privacy settings will protect you anywhere but on the social media site that uses them. For instance, recently New York's highest court ruled, regarding private Facebook posts, "even private materials may be subject to discovery if they are relevant." In this context, "subject to discovery" simply means that the opposing party has a right to see the material at issue.

You can access Facebook's privacy settings here.

3. Create strong, memorable passwords.

Any time you need a password, create one that uses a combination of at least ten numbers, symbols, and upper- and lowercase letters. Avoid using common words, as password cracking tools can use every word in the dictionary to try to access your password. Make it a password that's easy for you to remember, but that would be hard for someone else to guess. Avoid the most popular choices, like birthdates and anniversaries, or the names of your spouse, children, or pets.

If remembering unique passwords for different websites is hard, then a password manager may come in

handy for you. A password manager creates unique and complex passwords for all your favorite websites. Norton Identity Safe is one such reliable password manager.

4. Keep all your software up to date.

Many viruses and malware programs are specifically designed to mine your digital footprint, and they are constantly being updated. To help protect yourself, make sure that your antivirus software and your other software programs are up to date. Older software can be more vulnerable to attack by hackers.

Outdated software could house a wealth of digital footprints. Without the latest updates, cybercriminals could gain access to this information.

5. Review your mobile use. If you don't need it, delete it.

Set a password or lock pattern on your mobile device. That way, your device can't be accessed by other people if you accidentally lose or misplace it. From time to time, review the apps on your phone or tablet. What are their privacy or information-sharing settings? If you don't use an app anymore, delete it.

When installing an app, read the fine print. Many apps disclose what kind of information they collect and what it may be used for. Personal information like your email, location, and online activities may be mined by these apps.

6. Build your reputation through your behavior.

Contribute to your positive, professional digital footprint by posting only those things that contribute to the image of you that you want your bosses, banks, or professors to see. Skip the negative tweets, un-tag yourself from questionable Facebook photos, and keep critical comments to yourself. Instead, consider building a positive reputation by starting a blog or website that showcases your work or a hobby you're passionate about.

Keep in mind that employers, colleges, and others can look up your online identity to access your digital reputation. Keeping a clean online presence may help you in the future.

Help secure your digital footprint today

Think of your digital footprint as an extension of who you are. It is the image you create for yourself for the world to see.

Be careful about what you share, like, or comment on. Avoid sharing too much personal information online. If there is something distasteful about you online, contact the website's administrator to request that the information be taken down.

Keep track of all the accounts you have, and keep an eye on the privacy settings from time to time. Privacy settings can be changed when an app is updated by the developer. It may be impossible to erase your digital footprint, but you can work toward making it a positive one.

How a VPN can help shield your digital footprint from prying eyes

One more way to help safeguard your digital footprint is to use a virtual private network, or VPN, to protect your privacy online and even to prevent websites from installing cookies that can track your internet browsing history.

A VPN gives you online privacy and anonymity by creating a private network from your home or public internet connection.

VPNs mask your IP address so your online actions are virtually untraceable. Norton Secure VPN, a trusted VPN service, can help secure your private information and prevent websites from collecting your personal

data.