Smart Tips to Protect Your Identity in Search Engines

**The web is an open source model for your personal information to get into the wrong hands.**

“The police can't protect consumers. People need to be more aware and educated about identity theft. You need to be a little bit wiser, a little bit smarter and there's nothing wrong with being skeptical. We live in a time when if you make it easy for someone to steal from you, someone will.” Frank Abagnale

Identity theft, stalkers, lawyers waiting to serve you, collection agencies, nosy co-workers, potential employers doing background checks, data hackers, creepy guys on dating sites, and stalkers are sniffing for information to potentially abuse your personal information.

**How to protect your personal information from public view.**

Take a look at your privacy options when signing up for social networking sites. It is recommended to use an alias name as a screen name, and never place your date of birth, real zip code, real phone number, and address in any website that involves social networking or dating.

If you have no plans to use a particular social venue, it’s a preventative measure to register a profile with your real name if that name has not been taken. The same holds true for businesses looking to protect their identity. This way no one can try to duplicate your information and pose as you.

For example, Instagram is not for everyone, or every business. Think of the venue, or any other social networking platform as “free valuable real estate”, for your personal use or business promotional use.

***Is this* *Fail proof? Of course not!* Advanced data stealers have a more sophisticated way around this.**

Not all social networking sites work this way, as there are usually hundreds of people with the same name allowed, such as on Facebook or LinkedIn. If you’re lucky enough to get emails with all the free email sites with your full name, you can do that too- but this does not guarantee any cloak of protection to the sophisticated perpetrator, especially with spam bots that use email addresses for identity fraud.

**Intellectual Property**

 If you are a domain holder, it is best to register your domain as a private registration. Private domain registration will prevent email spamming, as your email, address and points of contact are hidden under the privacy cloak of private registration.

 If you are a trademark holder, or holder of any pending registrations and have not appointed an attorney with an address on the record, set up a corporation in a state, such as Delaware where owner information is not publically listed online. You can use a mailing address at a UPS store, or a U. S Post Office Box that is valid to receive correspondence. Everything listed in registering a trademark or patent is public information, even in the pre- registration application stage.

**It’s been noted that Twitter bots are stealing social media identities for profit.**

The IFTF is a research company that makes sense of merging trends that are forces in changing the world. The institute purchased thousands of retweets for a research test for a monetary fraction and the bots retweeted up to 10,000 times for the holder of their account within a few days.

Twitter says in their policies that it works to prevent this type of manipulation. In today’s plethora of fake news and scammers, web users must err on the side of caution and approach certain things with a subjective view. After all, the debacle of Cambridge Analyatica and Facebook should not be so surprising anymore. As of this writing- ***Cambridge Analytica Is Shutting Down.***

Was this a big deal? Yes- Personal information farmed out all over the web to app developers. Facebook will now tell users which websites are tracking them on the web and give the option to delete their personal data. The program is called “Clear History”, if you opt out your data is cleared and so will all the cookies stored, that actually make your user experience on Facebook a better one, as it already has your preference stored.

 The only people that should have personal information about you should be your family, your banks, your medical doctor, and the IRS. Make sure you opt out of any 3rd party affiliates at your bank soliciting for home loans, credit cards, and new business. If you need these services, contact the lenders directly. Don’t allow 3rd party affiliates have this information from you from your banks. Your information could be resold again and again.

***All banks are required by law to let you opt out of 3rd party. Contact each of your banks for the procedures to keep your info only within their database and not offered to affiliates.***

Your profiles on Facebook, Instagram, My Space, LinkedIn, and Classmates.com should be set to private so only your online friends can view your information. LinkedIn and Facebook allow you to keep parts of your profile private and some public. While these are still are not fail-safe solutions, as any data can be compromised, it is best to choose the most private options available to you.

 There is a real truth on how data from your social networks get into the hands of data mining companies. Data is usually collected by companies like Intellidyn, Tower Data, formerly Rapleaf, and Exelate. Exelate, a Nielson company. The company tracks your web searching and does have an online opt-out page to prevent your web searching from being analyzed. They don’t ask for information from you when you opt-out, it is quite obvious they can see your IP and cookies when opting out. Click the link to opt out of Exelate and then scroll down. You will see the data that they know about you, such as household income, age and demographics.

Additionally, you check the other sites for their options such as NetworkAdvertising.org and AboutAds.info. You can contact these companies to help manage your privacy online. They work with the clearing houses and offer information on how to opt out of member ad networks. You may search the term “opt-out of lists” in Google Chrome and Mozilla links to further the opt-out process with other types of reporting agencies.

**Solutions to keep you safer.**

 Search your name and see if it appears on a website like Spokeo.com, My Life.com, Intellius.com, People Search.com, Emailfinder .com. Archives.com and a host of other sites. You will need to contact these companies directly and tell them that you want your information removed.

Instead of paying some of these websites to remove your information such as Reputation.com, you can also ask Google to remove it. Maybe you see a dead link or want to ask Google to improve their Safe Search filter? Sign up a Google account, with Google webmaster tool a try. The webmaster tools help webmasters control information or images that appear in the Google search. If you find a page in Google search results that lists your personal info such as a credit card or social security number, contact Google to submit the request to contact the websites hosting company to request that the page, and have it taken down immediately. To start the process to remove the information from its search results, email removals@google.com to eliminate your personal information from Google index and cached pages.

If you see your phone number displayed in Google Search, fill out this form here for a removal request at .http://www.google.com/help/pbremoval.html

Google states this on the page exactly “To remove your residential listing information from the Google phonebook, please fill out the form below, entering all information exactly as it appears in your phonebook entry. Doing so will mean your residential listing does not appear in Google for any phonebook search, even searches conducted on your name instead of your phone number. Please note that this removal is permanent and that it's not possible to add your phone number again in the future.” Be cautious about this one if you are a business as business listings in Google with your business phone will enhance your visibility and exposure online.

Removing your listing from Google will not remove your personal information from other pages on the web, or from other reverse phone listing lookup services, such as SpyDialer.com, Anywho, White Pages.com Reverse Phone Directory, Phonenumber.com and Smartpages.com. These companies all have listing removal links to request the removal of your information. By law, they must comply when you are able to prove to them that you are the real owner of the data.

If you own property in your name it is likely to be searched and found on Zillow.com. Property records are not private. Type in the name of a property owner and their address, by city and state and the top listings are companies that list real estate property records.

There is browser extension that you can control ads and tracking technologies to speed up page loads, eliminate clutter, and protect your data. Downloading Ghostery at [www.ghostery.com](http://www.ghostery.com), which is a browser extension that lets you see who is tracking you when you visit websites allows you to block scripts from untrusted companies, delete local shared objects, and the ability to block images. **PrivacyChoice.org lists tracking data for over 250 sites and helps you opt out of them.**

Reputation.com claims to remove and or bury data in the Google search engine and others for a monthly fee. They will spend a lot of time adding back in positive data about you in the form of press releases and article mentions to essentially raise your reputation score higher than normal, so the other data gets buried. Only a legal action with the search engine can remove information that has caused defamation or libel against you. It is best advised to contact an attorney in those situations where they can execute a cease and desist request to the perpetrator.

Yahoo and Lycos's People Search are powered by Acxiom. To remove basic search info from Yahoo, visit Yahoo Privacy Policy and other search engines, and view their privacy policy links.

Be sure check your cell phone carrier and landline carriers. Verizon has told us that they no longer allow cell phone information of their customers to be purchased from companies that use your phone numbers in their public databases. The cellphone carriers were selling data to sites like Intellius and others that list phone number searches, and reverse lookups.

**Can You Remove Information from State and City Records?**

Yes, you can. Each state is different. It is advisable to call your local

Open Government Guide lists the open laws of each state

NASS.ORG has a published article on the steps needed to get the records that they have about you and place in their online databases

In final, search yourself on the web with reverse phone lookup websites. Check these sites periodically to see how all your telephone numbers, name and addresses come

It is also a good idea to monitor your credit report every 30 days. Sign up for a monitoring service that alerts you to changes in your report. There are many services out there such as Lifelock.com, Equifax-ID, Patrol, and ID Watch Dog to name a few.

Start with a free credit report at Equifax or Trans Union. By law, you can get a free one every year.

You may also register here https://donotcall.gov/ to keep your phone number on the Do Not Call List for telemarketers.

Set up a Google Alert with your name and phone numbers and when your name appears and gets indexed you will receive an email alert to see the link. Step Rep is also another monitoring system http://www.steprep.com/ Here you monitor how your business competitors stack up against you in online searches.