Protect Your Online Identity.

It is our responsibility to secure our own information and there are hundreds of sites that have your information available online. However, by following these simple steps, you can minimize the amount of information that is out there about you:

1. Cut Off Data Brokers.
Data brokers are self-regulated, which means they control how you can remove your information from their databases. Some require you to fax an opt-out request. Others require you to fill out a form on the web, and some even require a written request. Certain data brokers will even ask you to confirm or follow up via email. Others will say you must send in proof of identification, like a State ID. This process is complicated by design.

The Privacy Rights Clearinghouse maintains a list of data brokers (http://www.privacyrights.org/online-information-brokers-list) with links to their privacy policies or opt-out pages. But this list includes 147 companies. Fortunately, most of the companies listed are small, get no traffic, and are a poor outlet for your data. You're going to first want to target the big boys which include Acxiom, BeenVerified, MyLife, Intelius, Spokeo, Rapleaf, White Pages, and PeopleSmart.

2. Block the Cookies. Online ad networks often install a small file on the computers of people who visit certain websites. These so-called cookies can log your surfing habits, allowing advertisers to tailor ads to your interests. If you are trying to keep some online privacy then you should opt out. In the settings panel of your web browser make sure that you disable cookies from third party websites. Most advertising companies use this information to directly target you with ads of products that you use.

3. Lock down your social media profiles, and think before you post. Social networks are totally in your control and should never be a source of data leakage. Everything that you consider private (contact information, family, pictures, interests…) can become public if you're not careful. For starters, restrict your privacy settings to the most protective possible, such as allowing only your direct friends and connections to see anything at all. Basic information, such as your name, city, and profile photo may remain public, but anything beyond this should be off limits. Also:

- Don't accept requests from people you don't actually know. Bots masquerade as people now, for example, a friend request from a stranger may instead be an automated software app trying to steal your info.
- Don't use social logins — Facebook, Twitter — to log on to websites or apps if an alternative exists. If a website seems suspicious and they only allow social logins, forget it.
- When your friends use social apps, said apps can access **your** information. This is a massive vulnerability. Restrict this access by going to Privacy Settings -> Apps, Games, Websites -> How people bring your info to apps they use. Make the proper adjustments here.

Remember the Internet does not delete anything, so if it is something you wouldn't want your parents, children or employer to know about, DON'T POST IT.