How to remove yourself from Internet search results and hide your identity

zdnet.com/article/how-to-erase-your-digital-footprint-and-make-google-forget-you

By Charlie Osborne for Zero Day | December 7, 2020 -- 03:16 GMT (19:16 PST) | Topic: Security

No right to be forgotten? A step-by-step guide to reducing your digital footprint online

Watch Now

There is now a very thin line, easily broken, which separates our physical and digital identities.

Social networks have evolved from the days of MySpace to valuable, data-slurping machines that have information on everything from our friends and family to our voting habits.

When you apply for a new job, many employers will try to find and evaluate your social media presence to ascertain if you are a suitable candidate.

A misjudged tweet from years ago or an inappropriate Facebook photo can destroy future job prospects or ruin a career. A Google search that reveals an old conviction can make it more difficult to become hired, and -- whether true or not -- allegations of criminal conduct spread online can cause misery.

How to protect your privacy from Facebook

There's the idea that once something is online, it is immortal, immutable, and almost impossible to contain. In other words, you should not put anything online you wouldn't want your grandmother to see, in case the consequences damage you or your prospects further down the line.

However, keeping your digital information in check is not just about information that you put online. Monitoring the passive data collection conducted by companies from you is important, too.

Abuse, stalking, and bullying may also factor as reasons to erase our digital footprints and seize control of our devices. If you suspect your mobile device has been compromised by spyware or stalkerware, you can check out our guide here.

Google is your 'friend'

In 2019, the European Court of Justice ruled that Google is not required to apply the same privacy standards worldwide as it does in the EU.

In the EU, if a request for a name or specific links connected to an individual is deemed acceptable, the tech giant scrubs away these links. However, Google has long argued that extending the "right to be forgotten" on a global scale could set a dangerous precedent and clash with laws implemented in other countries.

The company also claimed that extending the law could turn the request feature into a "censorship tool" -- in what appears to be in direct contrast to reports of the tech giant's plans to woo China with a censorship-friendly search service.

Also: Social media cannot be trusted without these features

Nonetheless, the Google search engine can be used to uncover exactly what information about you is public and what the average person can quickly find out without the need for advanced tools, social engineering, or reconnaissance.

Once you know what is online, you can start tackling the problem. Run a quick search and make a note of any website domains that flag you, social media account links, YouTube videos, and anything else of interest.

You may have the right to be forgotten

In the EU, citizens are able to request the removal of information from the Google search engine, as well as from Blogger and other related Google-owned products.

After filling in this form, de-listing requests are reviewed manually by Google employees. Since 2014, Google has received 846,327 requests to delist related to 3,338,864 URLs.

Also: Do we know where to draw the line with co-workers on social media?

Google may not accept every request to remove links relating to you. Reasons given for refusal include technical reasons, duplicate URLs, information deemed "strongly in the public interest," and whether or not the content on a web page relates to professional lives, past convictions, work positions, or self-authored content.

"When you make your request, we will balance the privacy rights of the individual concerned with the interest of the general public in having access to the information, as well as the right of others to distribute the information," Google says. "For example, we may decline to remove certain information about financial scams, professional malpractice, criminal convictions, or public conduct of government officials."

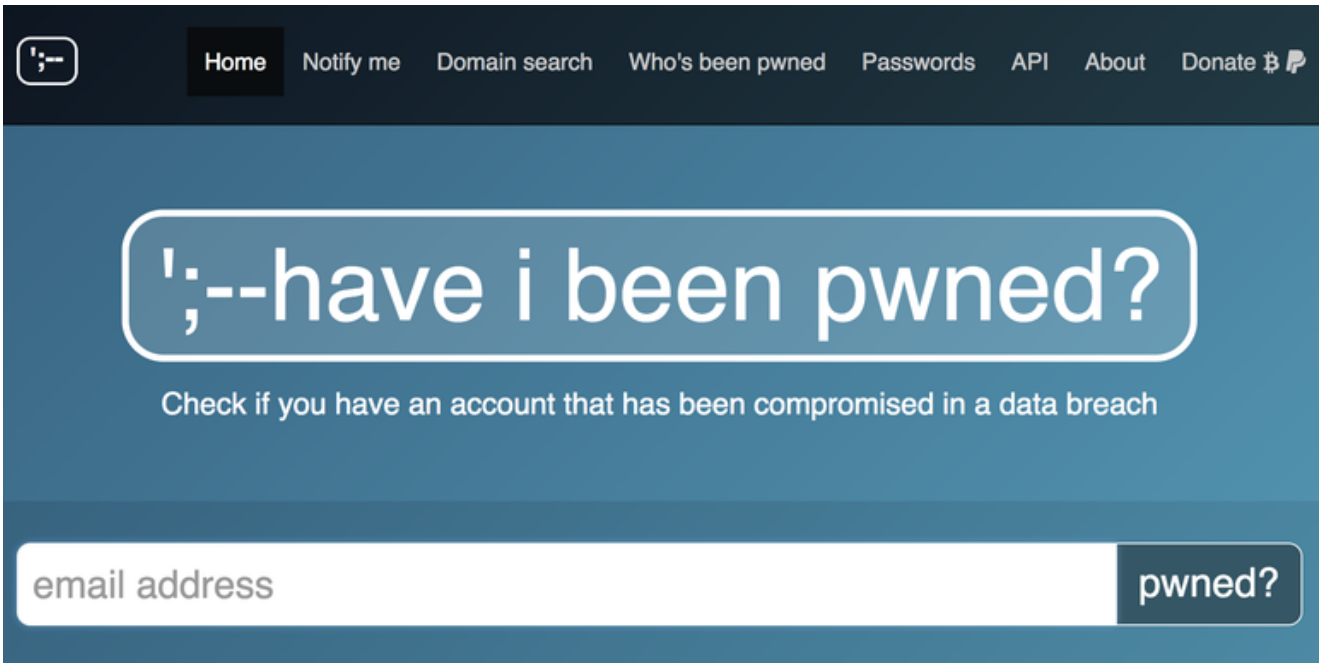
To submit a request related to other products, such as Blogger, Google Ads, or Image search, you can use the form here.

Also: GDPR: Two-thirds of organizations aren't prepared for the 'right to be forgotten'

Have I been pwned?

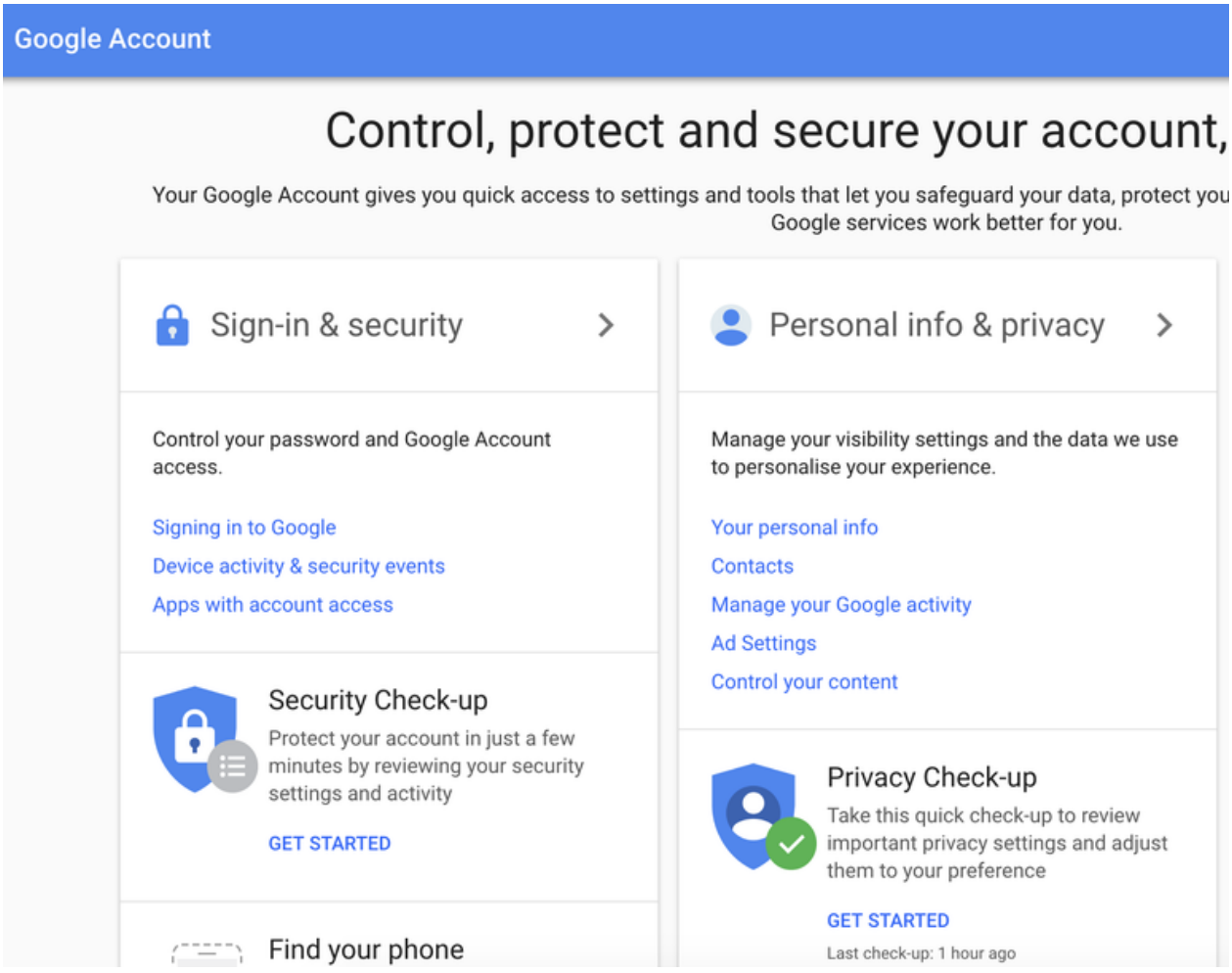
You cannot take control of your digital footprint without knowing where and what information is stored -- and potentially leaked.

The HaveIBeenPwned service is run by cybersecurity expert Troy Hunt and can be a useful tool to discover if any account information belonging to you has been compromised or included in a data breach. If you find an email address connected to you has been pwned, check to see what data breaches you have become embroiled in -- and make sure you change your passwords as quickly as possible.



Google accounts

Make sure you visit the Google Account page, where there are a number of settings that can boost your privacy, reduce data collection, or remove you altogether from the ecosystem.



Privacy checkup: The Google Privacy checkup allows users to prevent Google from saving your searches and other Google activity to your Google Account, as well as turn off your location history.

You can also choose to disallow Google from saving YouTube search & watch history and a record of videos you have watched, your contacts, device information, voice and audio activity including recordings harvested from interaction with Google Assistant, and other data.

In this section, you can also choose whether or not to allow Google to use your information to tailor advertising during your browsing sessions.

Also: Broadcaster ABS-CBN customer data stolen, sent to Russian servers

Security checkup: The Google Security checkup can be used to show you which devices have access to your account, including laptops, PCs, and handsets. You can also find a list of any third-party applications which have been granted permission to access your account. Revoke permissions as necessary.

Delete me: Found under Account Preferences, Google's deletion service can be used to delete select products, or remove your account entirely.

For a quick fix, use a service

There are a number of services available out there in which you can pay to keep your information away from data brokers.

One such example is DeleteMe, a paid subscription service which maintains tabs on data collection and release, as well as removes data including names, current and past addresses, dates of birth, and aliases on your behalf.

In turn, this can keep your private information off search results and away from platforms such as open people search databases.

Also: GovPayNow payment portal may have exposed over 14 million customer records

When it comes to **mailing lists**, services such as unroll.me can list everything you are subscribed to, making the job of unsubscribing from newsletters, company updates, and more far easier.

However, this service is not currently available to those in the EU due to GDPR regulations.

Lock down your social media accounts or delete primary accounts entirely

Facebook: In the Settings tab, you can download all of the information that Facebook holds on you.

You should also take the opportunity to lock down your account. In the Privacy tab, you should restrict your posts to 'friends only,' limit your past posts, and you can also decide to disallow lookups through your provided email address or phone number.

An important element that shouldn't be overlooked here is the option to remove your Facebook profile from **search engine results** outside of the social networking platform.

Under the Location tab, consider turning off location data collection by Facebook, too.

Twitter: Twitter also allows users to request their archive, which is all the information collected from you. This option can be found under the Settings and privacy tab.

In the settings area, you can also choose to lock down your account entirely and make tweets private and only viewable by those with your approval; you can turn off tweets containing location data; you can decide whether or not to allow email and phone number searches to connect others to your profile, and you can choose whether or not to allow others to tag you in photos.

Under the Safety portion of the tab, you also have the option to prevent your tweets appearing in the search results of those you have blocked on the micro-blogging platform.

Instagram: Facebook-owned Instagram has a number of privacy settings you can also change to maintain an acceptable level of privacy.

By default, anyone can view your photos and videos on your Instagram account. However, by going to your profile, clicking Settings, Account Privacy, and switching 'Private account' on, you can make sure your content is only viewed by those you approve.

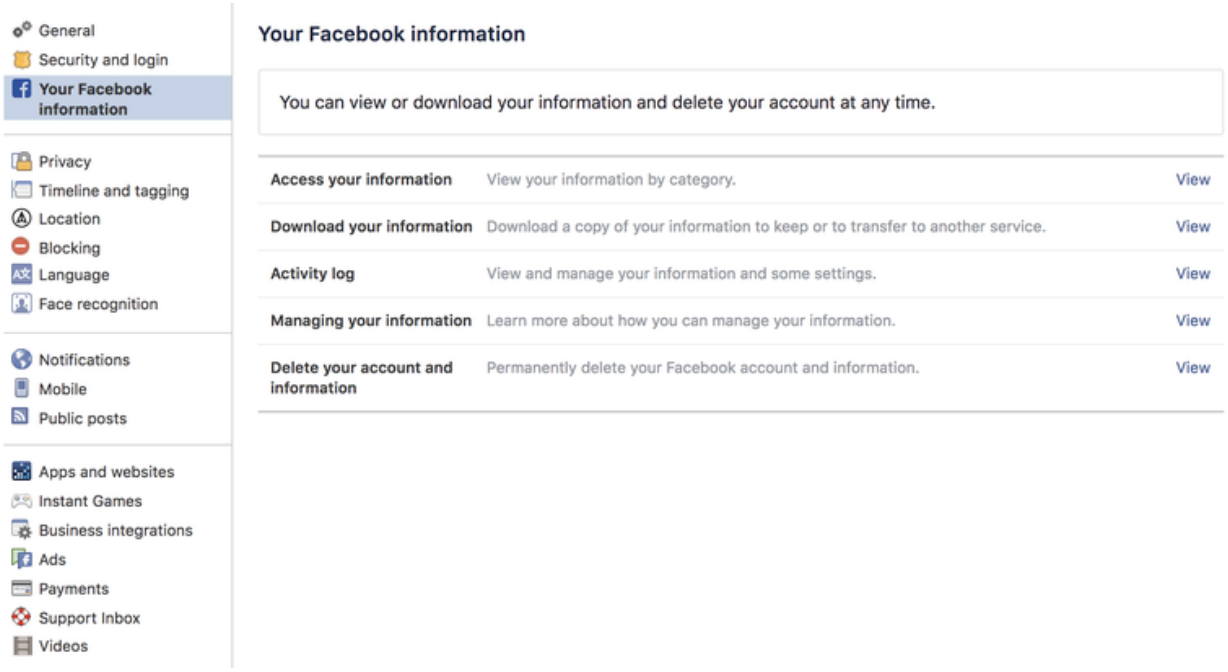
Remove everything: A more extreme option is to delete all of your primary social media accounts completely.

In order to do so on Facebook, you need to go to Settings, General, and Manage your account to deactivate it. This gives you the option to return at a later time and does not delete your data. Your settings, photos, and other content are saved, but you will not appear beyond unclickable text.

Deactivating your account gives you the option to take a break and return later, and will take you off searchable results.

Also: Medical records of high school students leaked in 'appalling' data breach

However, you can also permanently delete your account by clicking Settings, going to Your Facebook Information, and clicking Delete Your Account and Information, followed by Delete My Account. If you have trouble finding this setting, you can also type "delete Facebook" in the Help Center tab.



You are given a grace period of 14 days to change your mind and log back in. It can take up to 90 days before the deletion of content on your wall and in your account will begin.

In order to deactivate **Twitter**, you need to click on Settings and privacy from the drop-down menu under your profile icon. From the Account tab, you can then click deactivate.

To delete your **Instagram** account, log in and go to the request deletion page. Once you have submitted an answer as to why you are deleting your account, you will be prompted to re-enter your password, and then a delete account option will appear.

Delete and deactivate old accounts

Do you have a MySpace account? Do you have old, unused customer accounts with e-commerce platforms that you only remember you opened when they send emails which detail recent discounts and deals?

When information such as your name, physical address, telephone number, and credit card details are spread across multiple businesses, should these companies experience a data breach, your data is up for grabs.

Also: Peeled onions and a Minus Touch: Verizon data breach digest lifts the lid on theft tactics

Unless the account is one you use frequently, consider deleting it permanently. It is a pain to find, remember credentials, and recover passwords associated with old accounts, but this is an important step in locking down your data.

Remove old social media, blog posts

Is it really necessary to preserve what you had for breakfast one morning in 2013 or your review on a now-defunct retail shop near you? Probably not.

We are all responsible for the information we post online, but once it is posted, it does not have to stay there. Effort and time are required to comb through old posts, but the result is worth it, and this may also train you to be more selective about the information you share in the future.

... and if I can't delete embarrassing content?

If you have come across embarrassing forum posts or messages that you do not have the privileges required to delete, the only other option is to contact organizations and webmasters directly.

When you contact them, make sure you include a link to the content you are concerned about, give your reasons, and hope they agree to delete it. However, do not expect an immediate response.

Deseat.me

Deseat.me is an automated option for requesting account removal and subscription deletion from online services.

It is incredible just how many accounts you may have tied to your account, which -- as it was in my case -- could be in the hundreds.

You will need to temporarily give the service access to the email account that is used to sign up for services and allow it to send emails on your behalf. However, this can be quickly removed afterward, and even if you do not use the tool for its intended purpose, Deseat.me can still give you valuable insight into what is connected to your email account.

Another alternative is Account Killer, which also gives users a rating system that describes the complexity of account deletion processes provided by online services.

Hide yourself

If you cannot delete online accounts outright and only deactivate them instead, before you do, wipe as much content from them as possible. If the account is no longer relevant to you, consider changing the **name** and **personal details** connected to it, as well as remove or change photos to generic alternatives.

When it comes to active accounts such as on anonymity or aliases can help keep your digital and physical presence separate.

It is against terms of service to not use your full, correct name, but it is still common practice for many to change their surname at the least to prevent work and personal accounts -- and lives -- from colliding.

On Twitter, users will often choose aliases, and there is no reason why you cannot, too. Using profile pictures which do not show your face and names which do not directly correlate to you may help.

Set up a second email account for junk

Another way to keep your digital footprint clean of debris is to separate online services between email accounts. If you need to provide an email address for a one-off purchase, for example, consider using a junk email address -- which will quickly become full to the brim with promotional material but will keep marketing databases separate from your primary email address.

Use a Virtual Private Network (VPN)

A VPN is able to mask your IP address and creates a private tunnel between yourself and the Internet. This tunnel ensures that data and communication packets sent between a browser and server are encrypted, which in turn can prevent eavesdroppers from harvesting your information or tracking your online activity.

There are services out there that are both subscription-based and free. it is generally better to sign up for a paid service if you can -- no VPN service is truly 'free' given the cost to create and maintain the infrastructure required to route traffic, and therefore your data may be used or sold to third parties in return for VPN services.

See also: The best VPN services: Our 10 favorite vendors for protecting your privacy | VPN services: The ultimate guide to protecting your data on the internet | How to choose the VPN that's right for you

What about Tor?

If you are inclined to further anonymize your footprint, consider using the Tor onion router network. Tor is used by the privacy-conscious, activists, and those seeking a means to circumvent censorship barriers such as the Great Firewall of China. If you use the network to browse the Internet, anyone attempting to monitor you would be met with a series of nodes used to divert your encrypted traffic, making it very difficult to trace you back to an original IP address.

The most permanent measure

Starting from scratch may seem extreme, but in some cases, could be worth considering. The outright deletion of email accounts, social media, and e-commerce services won't immediately destroy all data or search results connected to them, but it will, over time, make them less likely to appear.

Just make sure that before you take this irrevocable step you have backed up any data that you want to keep, such as irreplaceable photos you have uploaded to social media or stashed away in your email inbox.

By Charlie Osborne for Zero Day | December 7, 2020 -- 03:16 GMT (19:16 PST) | Topic: Security