How to Ghost the Bad Guys and Protect Your Privacy

Regularly reviewing your online presence can help protect you from various threats, including phishing scams, ransomware, and identity theft. The goal is maintaining a minimal digital footprint and securing your digital identity from cybercriminals. With careful management and a proactive approach, you can effectively protect your privacy and stay safe online. Here's how to do it.

BY JAMES PEARSON

A local radio station approached me several months ago to discuss identity protection and cleanup services. I was not familiar with these services then, but I soon realized their direct relation to data breaches and identity theft. Intrigued by this connection, I delved deeper into the subject and made some surprising discoveries.

I have personally experienced a few incidents when either someone else's identity or incorrect online information has caused adverse consequences for me in financial or other transactions. And my firm has worked with a few clients who have had their identities stolen. These experiences have motivated me to delve deeper into the issue, which is the focus of this article.

My intention with this article is not to show you how to disappear completely, become disconnected, and live off the grid. However, we can learn a lot from people who have done so. This process can help you clean up your confidential information, improve your online reputation, and reduce your chances for ransomware, data breaches, and security risks.

Why Care?

You could throw your hands up and say, "What's out there is out there, and the bad guys already have it," and you are correct. Through no fault of your own, plenty of data breaches have already exposed the most common information such as name, address, phone number, email, and date of birth. The Equifax and Yahoo! data breaches are perfect examples. Despite both happening years ago, much of your data is publicly available because of these and other similar data breaches. But there are reasons why you should care. Your personal information can be and is continually being exploited by the bad guys for targeting you better, using phishing emails, ransomware, other fraud, and identity theft.

A few years ago, on a Black Friday morning, I received a series of threatening phone calls and voice messages from a local businessperson. They thought I was a customer who owed them a significant amount of money. I was confused as to why they thought it was me. After some quick investigation, I realized that my landline phone number, which we rarely used and had for over seven years at that time, was still listed on some websites as the person this business owner was looking for. This incorrect data resulted in me having to contact the police

James Pearson owns the Computer Center, Janesville. He is a Microsoft Certified Professional and a frequent author and speaker on cybersecurity and safety topics. Access the digital article at www.wisbar.org/wl.

james.pearson@computercenter.com

www.thelawyersgeek.com

department to stop the calls and threats.

Some people want a say in what information about them is available on the internet. By learning what is already out there, they can decide how much control they want over that information and how to rein it in.

Below are tips on how to ghost the bad guys.

Conduct a Digital Audit

Before taking any action to protect your online privacy, conduct a digital audit. This involves searching the internet to find out which of your personal information is available online. It is like excavating your online footprint and is similar to the process anyone looking for you would begin with.

Start with Google, and search for your name and your current city and state. You will find that many websites have published basic information such as your name, address, and phone number.

During this process, be conscious of your actions as well. Use your web browser's private or incognito modes. Using a browser other than Google's Chrome may also be advantageous because Google is known for mining users' data. Firefox, without any extensions (which can also compromise privacy), is an excellent place to start. There are also more privacy-oriented search engines, such as DuckDuckGo, which also has a privacy-focused browser.

Another possible step is to check out data brokers. These companies collect, aggregate, and resell your data. One such data broker is www.truepeoplesearch.com. Much of the information on this site is available for free, while many of the data brokers and sites you will find will tease you with some basic information and then ask you to pay for more details.

When you conduct a digital audit, you will discover the accessible information and its location. During this process, you might be surprised, amazed, or even shocked to find an abundance of information that is freely available and accessible, without a paywall, to anyone using the internet.

Set Your Privacy Tolerance

The next step is deciding what your privacy tolerance is. List the websites and information you found during your audit. Was the data you found incorrect? If so, you might decide to correct it as part of this process. If accurate, then you must decide whether you want that information in the wild or attempt to limit where it is, in which case you should begin the data removal process, discussed below.

When setting your tolerance level for sensitive data, it is important to remember that if you decide to clean it up and remove it, you will need to change your behavior in the future to prevent the data from leaking again. If the information is mostly correct, up-to-date, and accessible to the public, you might have a high tolerance level. However, if the information is incorrect and causes issues, it might be worth the effort to remove it altogether.

Cleaning Up

If you decide to clean up your online presence, this is the easiest and quickest way to begin. Start by deleting old, unused accounts, particularly those you no longer need, for instance, accounts you created for a single purchase or to download a product. Even if you no longer use them, these accounts can still be hacked, exposing your information. Unused social media accounts are like open windows inviting cybercriminals into your virtual home. Delete those old profiles. Do you still have a Myspace account? Request that it be closed and deleted. Then, adjust the privacy settings on active accounts. Make it difficult for the bad guys to find you.

Next, secure your email accounts. Email addresses and passwords are valuable because they can allow identity thieves and scammers to unlock other accounts. During your digital audit, you might find email accounts that no longer exist or contain incorrect information. It is essential to delete as many old email accounts as possible. Cybercriminals can use old email accounts to access personal information. Remember, a clean online profile is the best defense against intruders.

To manage your privacy going forward, avoid giving personal information unnecessarily. Unsubscribe from unwanted emails and newsletters, and check if you have an account with that site. Unsubscribe and avoid subscribing again.

Cancel shopping loyalty programs and survey programs. If they seem too good to be true, then they are too good to be true, and if there is no cost for the service, then *you* are the product. Not signing up for these programs and removing them is a big part of the process of ghosting the bad guys.

Removing Your Data

To remove data, go back to the websites on which your personal information appears. Locate the "remove me" or "don't sell my data" forms on each website and follow the indicated procedure to have your data removed or corrected. For example, the removal forms and process for truepeoplesearch.com are at truepeoplesearch.com/removal.

But do not just fill out the form and forget about it. Although the website must comply within a specific time period (usually around 30 days), following up might be necessary to ensure your data is successfully removed.

Consider enlisting the help of a data removal and monitoring service. These experts specialize in removing and protecting personal information from cybercriminals. There are several services that will remove and clean data for you and provide monitoring in the future.

The following are some of the most frequently used services. It is important to note that this is not a direct endorsement, and it is advisable to thoroughly research each company before using their services. Once they've cleaned up your data from hundreds of sites, these services operate similarly to credit monitoring services by automatically monitoring for any modifications and notifying you so they can be addressed and resolved.

- DeleteMe: https://joindeleteme.com/
- OneRep Homepage: https://onerep.com/
- Incogni: https://incogni.com/
- Unroll.me: https://unroll.me/
- Privacy Bee: https://privacybee.com/
- Brand Yourself: https://brandyourself.com/

One noteworthy aspect is that these services offer DIY guides on their blogs or a dedicated section of their websites for removing your personal information from numerous locations.

Your Virtual Lifestyle

So, you have spent considerable time cleaning up your old accounts, correcting your data, and ensuring that it is removed to your satisfaction and privacy tolerance. You have even subscribed to a service to facilitate this process. What happens next?

Going forward, you need to do two things: monitor your data regularly, and modify your online behavior. Here are some tips to help you achieve this.

- Be conscious of cybersecurity when releasing data, filling out forms, and clicking on links.
- Be aware of everything you share and your behavior on social media.
- Use VPN software: protect your connection, especially in public places, and anonymize your information.
- Minimize or eliminate social media use.
- Check privacy settings for the social media platforms you choose to keep.
- Use private and incognito browsing modes and consider a secure web browser like DuckDuckGo.
- Remove unnecessary software applications and extensions from your computer.
- Pay with cash whenever possible.
- Avoid online purchases.

Conclusion

It is unnecessary to completely disconnect from the internet and avoid social media to protect your privacy. However, regularly reviewing your online presence can help protect you from various threats, including phishing scams, ransomware, and identity theft. You can use manual and automated methods to remove outdated or private data from unwanted platforms. It is also a good idea to limit the disclosure of personal details and seek the help of professional data removal and monitoring services when needed. Adjusting your behavior online, such as using VPNs, minimizing social media use, opting for incognito browsing, and being aware of what information you share, also help. The goal is maintaining a minimal digital footprint and securing your digital identity from cybercriminals. With careful management and a proactive approach, you can effectively protect your privacy and stay safe online. For additional information , visit the Resource Center, https://info.computer-center.com/ProtectingyourPrivacy. **WL**