- Cybersecurity

COVER STORY

# DELETE YOUR INTERNET FOOTPRINT

*With spies lurking everywhere, how can you keep yourself safe? Try these 25 smart steps.*

BY *Chris Hoffman*

WITH ADDITIONAL REPORTING BY *Lucy Wildman*

PHOTO ILLUSTRATIONS BY *Justin Metz*

# As the

saying goes: The internet is forever. Once you've put something online—a credit card number, a silly photo, a heat-of-the-moment comment on social media—it can come back to haunt you.

But what are the risks, really? "There are two worst-case scenarios," says Thorin Klosowski, a security and privacy activist at the Electronic Frontier Foundation. "The most obvious one is a security issue. Everyone's email address and basic details are leaked somewhere online, and if you reuse passwords, that means a nefarious person will have an easier time getting into your accounts."

The problem is enormous: According to the Global Anti-Scam Alliance, scams cost more than $1.03 trillion worldwide in 2023, and most of that money was lost online.

"The second worst-case scenario is more primal: embarrassment," says Klosowski. And sometimes the blows to our pride are far more personal than blushing over an unflattering photo. "Many of us store our most intimate thoughts in a digital notes app and draft emails we never send, or pour out our private feelings into a direct message to a friend. This is the type of thing that can get leaked online, either through a provider being negligent or through your own misunderstanding of the often-confusing privacy settings in the software and services."

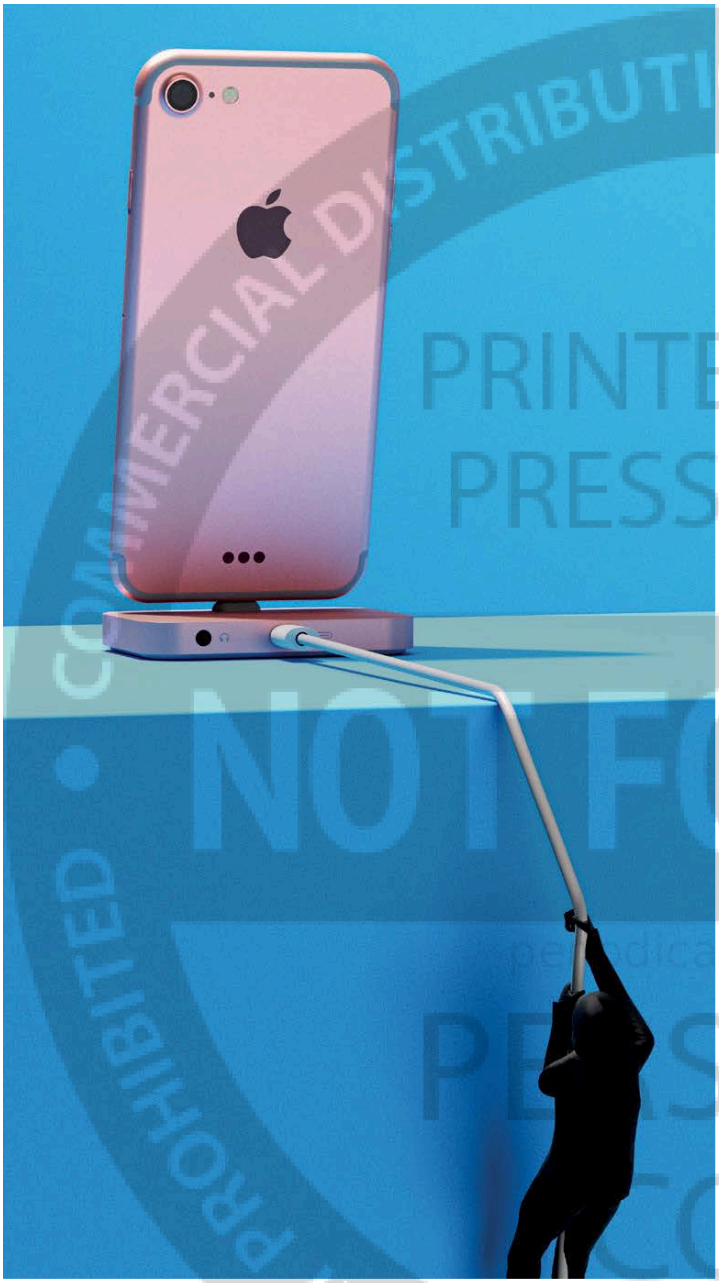
With these sorts of slip-ups, the stakes can be high. But you're not powerless. You can stand up for your privacy and begin to take control, starting right now. Here's how:

## 1 Mix Up Your Passwords

If you always use the same password, no matter how carefully crafted it may be, it's probably already out there.

The 2024 breach of the U.S.-based background-check company National Public Data, which resulted in the loss of 2.9 billion records including email addresses and phone numbers, was big news, but we don't always hear about the smaller-scale breaches, which are frequent. They occur when criminals purchase leaked databases of usernames (usually email addresses) and passwords on dark web marketplaces. Then the crooks try these combinations, hoping to access people's other accounts. So use a strong, unique password for every account.

VECTOR CIRCUIT BOARD: MICROVONE/GETTY IMAGES



## 2
## Use a Password Manager

How can you possibly remember all your passwords? You can't. But if you enlist the help of a password manager, you need to remember just one password—for it. The manager will do the rest, creating strong passwords and automatically filling them in for you.

The service 1Password offers an excellent manager for a few euros a month. Bitwarden is a good free option. Or use the free manager built into your browser. The latest operating system on Apple devices comes with Passwords, which generates and manages passwords at no extra cost.

## 3
## Find Out Whether Criminals Have Your Information

Visit *haveibeenpwned.com* to see whether your email address or passwords are included in any leaked databases available to criminals. Spoiler: Your information has probably been involved in multiple leaks. (The leaks on HaveIBeenPwned are just the tip of the iceberg of what criminals have access to.)

## 4
## Delete Old Accounts

You probably have a lot of online accounts you no longer use, and they might contain personal information. Delete them. Don't leave whatever details you may have shared sitting around so they can be discovered by criminals—or misused if an unscrupulous company one day buys and abuses your data.

To learn how to delete an account, perform a web search such as "delete old email account." Or go right to the

company; check its online support pages or contact customer support and ask for account deletion.

## 5 Download Your Data

Deleting an account doesn't mean you lose everything you had on that particular site. For example, you can easily download all the data associated with a Facebook or Google account and do whatever you want with it. Just be sure to keep backup copies of everything you consider important.

## 6 Find Old Accounts to Delete

You probably don't remember every online account you've ever created. To find old accounts you might want to delete, search your emails for terms like "welcome," "verify," "your account," and "free trial." The emails that pop up will remind you of accounts you've signed up for so you can then choose which ones to get rid of.

It's even easier if you already track your passwords in a password manager. Just scroll through the list to find accounts you no longer use.

## 7 Delete Old Emails Too

Do you really need to keep old emails forever? They contain personal details that could be useful to identity thieves. Consider deleting old emails, possibly after downloading a copy. This protects your correspondence from hackers.

## 8 Search Your Usernames Online

Head to a search engine and search for your name, as well as any usernames

you've gone by online. The results show you where your name appears on the public web. In all likelihood, your social media profiles will pop up in the results. That means they will also show up for other people who search for you.

## 9 Hide Social Media Profiles from Search Engines

Want to wipe these personal details from the internet? You can make your social media accounts vanish from search results by visiting each site that came up in your initial search and changing the privacy settings. Each site works a bit differently; for guidance, search for "privacy settings" and the name of each site. While you're cleaning things up, you can also remove comments you've posted, delete accounts, or ask websites to take down your personal information.

## 10 Control Social Media Privacy Settings

You may also want to restrict who can see what you post on social media sites. For example, on Facebook you can limit who can find you, who can see what you post, and what Facebook shares about you with other companies. To get started, go to your profile page in Facebook and click the Account button in the top right-hand corner, then select Settings & Privacy.

## 11 Delete Old Social Media Posts

Facebook was created back in 2004. By now, most of the university students who shared their party photos on the social media service in its infancy are 40 or older. Fortunately, Facebook has a Manage Activity tool that lets you delete or archive posts older than a certain date. Instagram allows you to delete or archive individual posts. Only you can see the things you've archived on either platform.

On the social platform X, formerly Twitter, individual tweets can be easily deleted, and several third-party tools can help you delete multiple tweets either automatically or based on specific criteria. TweetDeleter can even remove your likes on other people's tweets.

## 12 Know How Privacy Laws Affect You

Data protection rules vary from country to country. The United States, for instance, does not have a comprehensive national privacy law, though individual states have legislated protections.

The European Union's General Data Protection Regulation, introduced in

2018, is one of the strictest privacy and data security laws in the world, giving citizens the right to obtain and review personal data that has been collected about them, to object to the use of their data for direct marketing, and to insist that companies delete it.

## 13 Use a More Private Search Engine

To limit the data gathered on you in the future, use a more private search engine, such as DuckDuckGo. Make it your default search engine on all your devices by going to *duckduckgo.com* and clicking Set as Default Search.or downloading the app on a smartphone. Unlike Google and other big-name search engines, DuckDuckGo doesn't track your searches and link them to you, so it won't show you targeted ads or personalized search results either.

Other search engines that are highly rated for privacy include Qwant, Mojeek and Brave Search.

## 14 Tell Google to Stop Tracking You

Even if you want to keep using Google, you can activate more privacy settings to keep the internet giant from tracking all your web searches—which it does automatically if you're logged in to Google (while using Gmail, for example). Even YouTube, which is owned by Google, tracks a history of the videos you watch.

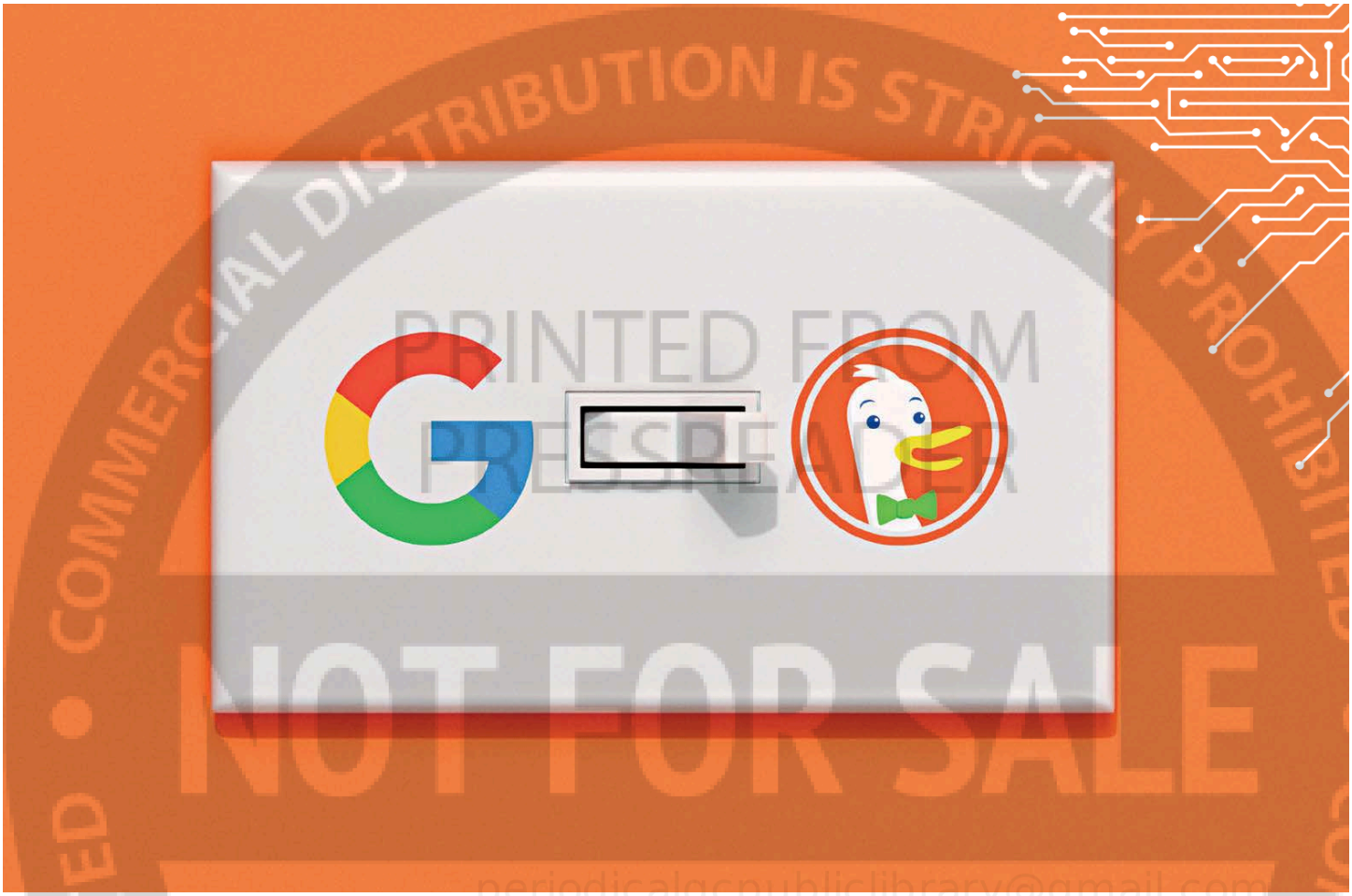
But this tracking is optional. You can tell Google to stop collecting your data in the future and to delete whatever it has already collected. To do so, click on your Google profile photo, go to Manage Your Google Account, and, in the left navigation panel, click Data & Privacy. Then, under History Settings, click My Activity and turn off any activity you don't want to save.

## 15 Configure Your Browser for Privacy

Browser cookies are small pieces of information that websites can store in your browser to track you. Chrome is moving away from cookies and toward a technology called Topics API, which tracks your activities online and determines your interests in broad terms. Advertisers then use these interests to place online ads that might appeal to you.

In 2022, Google launched My Ad Center, which allows you to limit or switch off ad personalization. In your Google account, go to Data & Privacy, then click on My Ad Center. You can switch off the "Personalized ads" button at the top of the page, or you can customize how your data is tracked.

There are other ways to limit this





tracking, with ad blockers and browser extensions that protect privacy. But you can be tracked in other ways, including by your internet protocol (IP) address, a number that identifies your internet connection online. (Every device on your home network likely shares the same IP address.) One way to conceal your IP address is with a VPN.

## 16
## Use a VPN

A VPN, or virtual private network, creates a secure tunnel to the internet, acting as a middleman between you and your internet service provider by encrypting your connection. With a VPN, your internet service provider can't see what websites you're accessing, and the websites you're accessing can see only the VPN's IP address, not your IP address.

If you've ever worked remotely, you have likely used your company's VPN. The privacy that VPNs provide is attractive not just to businesses but also to dissidents in repressive countries such as China, where VPNs can get around internet censorship and shield users' online activity (which is why China has outlawed the use of VPNs for private citizens).

When choosing a VPN, do some research, look up independent reviews, and be sure to pick a trustworthy one. Wirecutter, a product-recommendation service owned by the *New York Times*, recommends Mullvad, and also sug-

gests TunnelBear for those who use multiple devices at once. Operating a VPN costs money, so many free VPNs are untrustworthy and may even sell your data to make a profit. A good VPN generally charges a subscription fee, often just a few euros per month.

## 17
## Go Incognito

A VPN isn't a magic bullet. It's just one piece of the puzzle. Let's say you connect to a VPN, visit Google's website and sign in to your Google account. Now Google knows who you are. Even if you don't sign in, websites can check your browser cookies to link your VPN activity to your previous browsing.

If you use your browser's private browsing mode while using a VPN, websites will see you as a new user each time you visit. To go incognito on Chrome, click on the File menu in the upper left corner and select New Incognito Window. On Safari, click on the File menu and choose New Private Browsing Window or New Private Window.

## 18
## Switch to Apps That Respect Your Privacy

Just like websites, the apps on our phones, tablets and computers collect data about us. Finding out how much of your data various app companies were accessing used to be difficult, but now both the Apple App Store and the Google Play Store provide plenty of privacy information.

The Apple Privacy Report allows you to see details about how often apps access data such as location, camera and microphone. In Settings on your device, tap Privacy & Security, then turn on App Privacy Report. And Google Play Store shows users how their data will be used, whether it's shared with third parties, and how it's stored. On each app's page, click on Data Safety. There are usually multiple apps for the same purposes, so choose ones that collect less data.

## 19
## Seek Out End-to-End Encryption

For improved privacy online, seek out services that use end-to-end encryption. With this type of security, your data can be seen only by you and the people you communicate with. WhatsApp uses it, for example, as does Apple's iMessage when communications are sent between two Apple users. Sites that employ end-to-end encryption often say so in order to advertise their enhanced security.

One communication app that uses end-to-end encryption is Signal. Owned by a nonprofit and popular with activists worldwide, it works on both Apple and Android products.

## 20
## Take Advantage of Apple's Privacy Features

Apple has been a leader in introducing privacy features, many of which require iCloud+, an additional paid iCloud storage plan (starting at ₹75 for 50GB per month). The included iCloud Private Relay service functions similarly to a VPN: It routes your Safari browsing traffic through an anonymous server. Websites will know the general region you're in but won't see your unique IP address as you browse.

When signing up for accounts or newsletters online, the Hide My Email feature in iCloud+ lets you create randomized unique email addresses that forward emails to your real email account. Senders can't see your real email address, and you can deactivate a randomized email address at any time—perfect for avoiding spam.

## 21
## Protect Your Mail

Even if you don't pay for iCloud+, be sure to enable the Protect Mail Activity

feature that pops up the first time you open Apple's Mail app. It will block advertisers from learning your IP address and building a profile of your behavior and location.

## 22 Remove Saved Payment Details

Don't save your payment details on online shopping sites. True, saving them makes it easier for you to buy the things you want, but it also makes it easier for criminals to gain access to your accounts and buy things as you.

As a compromise, you may want to keep a credit card stored on sites you shop often but not on sites you use only occasionally. If a shopping site offers extra security features like multi-factor authentication—which typically requires a second level of verification from your email or mobile phone—opt for it.

## 23 Be Careful About Sharing Info

Think twice before sharing any personal details anywhere online. At the time, sharing a tidbit may seem inconsequential, but remember that personal details such as your birthday or the city you were born in are just the sorts of facts you should guard carefully, as they are often the answers to your security questions.

## 24 Take Care with Smart Devices in Your Home

More and more smart devices for our homes, such as smart speakers, security cameras and even refrigerators, are connected to the internet. If not properly secured, they can provide hackers with an easy way into your network. Some devices come with an easily guessable password, like 0000, so make sure you change it to a strong password. If the device offers multi-factor authentication, turn it on.

## 25 Update Your Software Regularly

Always accept updates for the apps and programs on your devices. Over time, hackers find new ways to break through security measures built into software and can exploit these vulnerabilities to spy on your devices or implant dangerous malware.

CONCERNS ABOUT online privacy aren't just concerns about privacy on the internet, they're about privacy in every facet of our lives. All of this is a lot to fully comprehend. But knowing the scale of the problem and taking these very doable steps is a good start. R