Hackers know your social security number. Here's how to stay safe

Alaina Yee Senior Editor, PCWorld Sep 23, 2024 3:30 am PDT

Summary

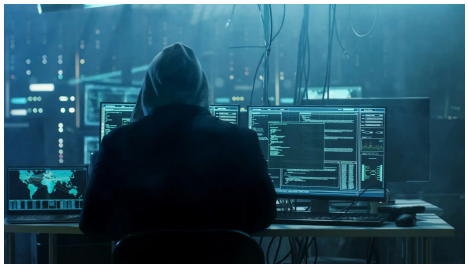


Image: Shutterstock / Gorodenkoff

The article discusses the alarming reality that hackers now possess your social security number due to numerous data leaks. To protect yourself from identity theft and fraud, the article suggests several crucial steps. Firstly, you can check if your personal details have been leaked through reputable websites like NPD Breach Check and National Public Data Breach Check & Search.

Table of Contents

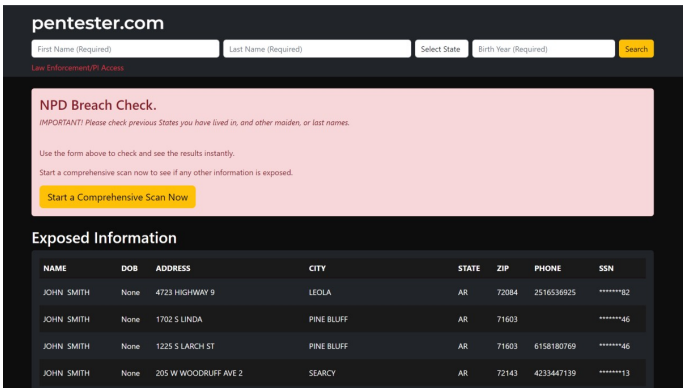
Thanks to a multitude of data leaks, your most sensitive information is now easily accessible to the world.

For anyone trying to keep their personal information secure, recent headlines have been a grim kick in the pants. The harshest came last month when the National Public Data breach was disclosed—the source of a purported 2.9 billion records spilling onto the dark web. But it wasn't the only prominent data leak. In early September, Medicare contacted almost one million beneficiaries about a loss of personal identifiable information related to a vulnerability in third-party software.

In other words, your social security number—central to filing taxes, applying and maintaining credit, and receiving certain US government benefits—is very likely available to hackers and would-be criminals for exploit. And if it isn't yet, the unfortunate reality is that another data breach will inevitably change that.

You don't have to wait for trouble to find you, however. You can take several steps to minimize the possibility of identity theft or fraud in your name, since other details like your full name, birthdate, and residence are also likely loose in the wild. Here's what to do.

1. Check to see what details have leaked



This step isn't strictly necessary since you can take precautionary measures whether or not you've been caught in a major data breach. But confirming if your info was leaked can be helpful—like when convincing yourself or loved ones to take action.

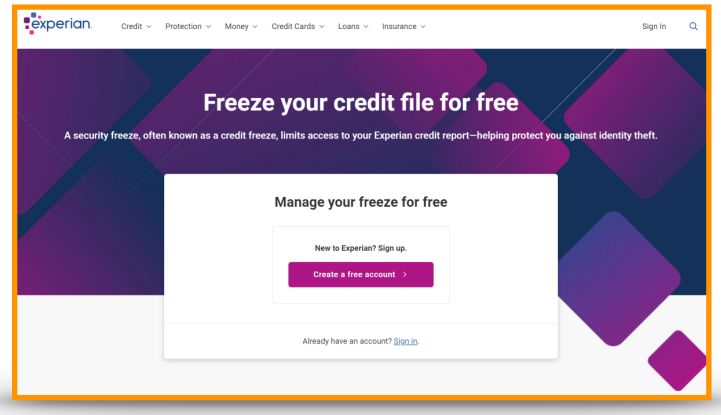
Generally you shouldn't volunteer your personal details to websites claiming to check if you were caught in a data breach, especially if you don't know who runs them. But several have been vetted, with a couple dedicated specifically to the National Public Data breach—and don't require sensitive info for verification.

- NPD Breach Check (npd.pentester.com)
- National Public Data Breach Check & Search (npdbreach.com)

For more details on these two NPD-specific sites, my former colleague Michael Kan dives into who runs them (one a cybersecurity firm, the other a data removal company). The NPD Breach Check site returns multiple listings linked to full name, state, and birth year you input, while the National Public Data Breach Check & Search site returns more granular results based on full name + zip code, social security number, or phone number.

If you're still wary of these sites or want broader, more long-term monitoring, you can also get notifications through Google's Dark Web Report service and some paid antivirus subscriptions. Have I Been Pwned is also an excellent resource for data breach notifications, though your email address must be part of the lost data for it to work.

2. Freeze your credit reports



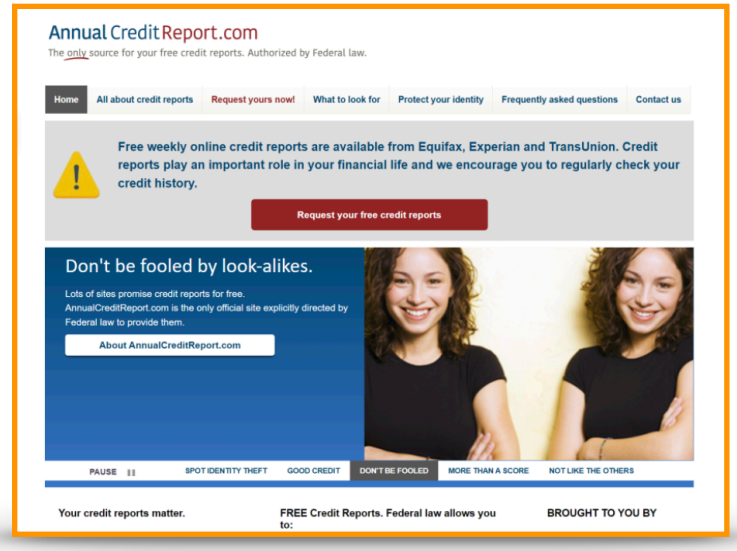
Freezing your credit costs nothing and keeps fraudsters from opening credit cards and loans in your name—a smart move when your full name, date of birth, and social security number are floating around on the internet.

You must perform the security freeze with each credit bureau. In the US, the three

major ones are Equifax, Experian, and TransUnion. For thoroughness, you can also freeze your report with Innovis, a smaller fourth credit bureau.

Once frozen, your credit reports become only available to you. If you need to allow a third-party credit check, like when renting a new apartment or opening a new line of credit, you can temporarily lift the freeze through the Equifax, Experian, and TransUnion websites or through their phone lines. You'll need the PIN issued to you in order to request the temporary lift.

3. Check your credit reports



While dealing with your credit reports, you should also have a look at them for any fraudulent activity. You can do so weekly through the official website (AnnualCreditReport.com) or request paper copies once per year through the phone or by mail.

If you spot inaccurate details, you can dispute them—and if you think you see signs of identity theft, you can report it and begin remediation.

4. Request an IRS Identity Protection PIN

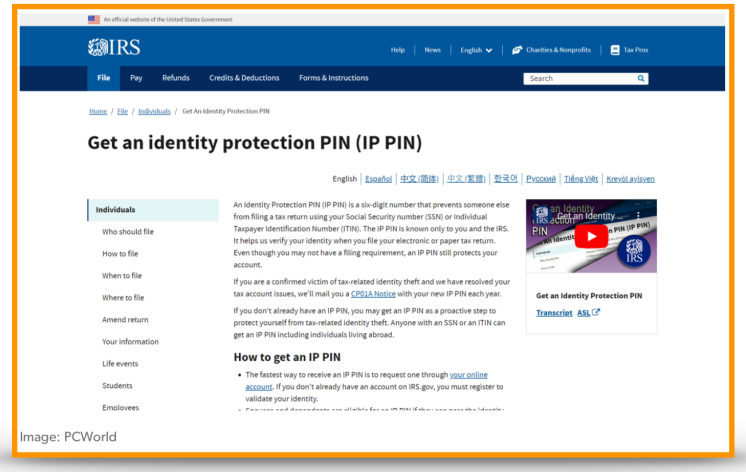


Image: PCWorld

Tax return fraud can be a serious headache. Fortunately, the Internal Revenue Service (IRS) allows you to prevent other people from fraudulently filing in your name (even if you don't need to send in a return). If you request an identity protection PIN (IP PIN), any filed return must include the six-digit PIN for it to be processed.

Most taxpayers will need to request a new PIN each year—unless you've been the victim of tax-related identity theft. If so, you should be already automatically receiving a new IP PIN each year from the IRS.

If you forget your IRS identity protection PIN, the IRS has methods to help you retrieve it. You can also store the info in a good password manager—if you're nervous about cloud-based services, you can use one that saves your data to a local hard drive or flash drive.

5. Freeze your banking report

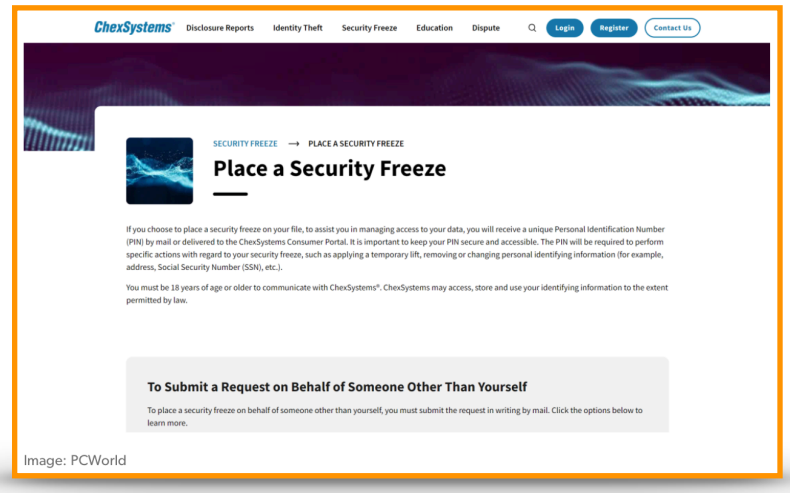


Image: PCWorld

Like with credit, a file exists on you about your banking account activity—and if someone begins opening fraudulent accounts in your name and runs them into the ground, banks may not want to do business with you in the future.

You can prevent becoming blackballed by also placing a security freeze with ChexSystems, the main company used by banks to verify if you're a worthy customer. Once in place, only you can access your report. To temporary lift the freeze (like when applying for a new bank account), you can make your request online, using the PIN issued to you when the freeze first went into effect.

Author: Alaina Yee, Senior Editor, PCWorld

A 14-year veteran of technology and video games journalism, Alaina Yee covers a variety of topics for PCWorld. Since joining the team in 2016, she's written about CPUs, Windows, PC building, Chrome, Raspberry Pi, and much more—while also serving as PCWorld's resident bargain hunter (#slickdeals). Currently her focus is on security, helping people understand how best to protect themselves online. Her work has previously appeared in PC Gamer, IGN, Maximum PC, and Official Xbox Magazine.