NAVIGATING A WORLD OF ACCELERATING CHANGE CNET

We May Use Your Chat? Advertiser disclosure

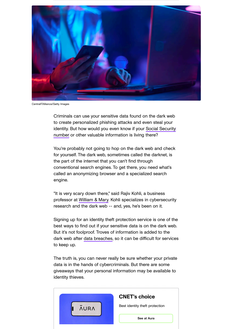
Our research panel among staff selects the products we cover and rigorously reviews them. If you buy through our links, we may get a commission. Reviews policy Advertiser disclosure

Your Personal Data Is Probably on the Dark Web. Here's What You Can Do to Fend Off Identity Thieves

Your private information is splattered all over the worst parts of the internet. This is your action plan.

Geoff Williams
Nov. 3, 2021 5:01 a.m. PT

1 min read



Cornered/Moxumbury Images

Criminals can use your sensitive data found on the dark web to create personalized phishing attacks and even steal your identity. But how would you even know if your Social Security number or other valuable information is being there?

You're probably not going to hop on the dark web and check for yourself. The dark web, sometimes called the darknet, is the part of the internet that you can't find through conventional search engines. To get there, you need what's called an anonymizing browser and a specialized search engine.

"It is very scary down there," said Rajib Kohli, a business marketing at William & Mary. Kohli specializes in cybersecurity research and the dark web -- and, yes, he's been in it.

Signing up for an identity theft protection service is one of the best ways to find out if your sensitive data is on the dark web. But it's not foolproof. Some of information is available on the dark web after data breaches, so it can be difficult for services to keep up.

The truth is, you can never really be sure whether your private data is in the hands of cybercriminals. But there are some giveaways that your personal information may be available to identity thieves.

CNET's choice
Best identity theft protection
See at Aura
Aura can let you know if your data's on the dark web.

Advertisement

NAVIGATING A WORLD OF ACCELERATING CHANGE CNET

Is my personal information on the dark web?

So how can you tell if your personal data is on the dark web? There are several signs you'll want to look for.

Advertisement

NAVIGATING A WORLD OF ACCELERATING CHANGE CNET

Random emails, texts and phone calls

Everyone gets these, and they're not automatically a sign that your information is on the dark web. Still, it's a possibility. Kohli says that if you're getting a lot of unwanted junk emails, calls and texts, "it's probably because someone purchased a list to run some sort of financial scam, and your information was on it."

Unfamiliar purchases on your credit card

Your Spidey senses should start tingling if this happens to you. Kohli says that it's a sign that it's possible someone has purchased your credit card number from a list of hundreds of credit card accounts which are sold for as low as just five cents apiece on the dark web." Kohli says. Your bank will normally send you a new card after suspicious purchases are identified or reported.

You're locked out of your bank account

It's one thing if you forgot your password and guessed too many times for your bank's comfort. But if that isn't the case, and you find yourself locked out, it's possible that someone else has tried to log in to your account too many times.

Odd health insurance claims

If you're getting medical bills for procedures you never underwent, get you on the phone with the healthcare provider or your insurer immediately. If medical claims that should have been accepted are rejected due to benefits being used, that, too, is a sign that you have been hacked. Identity theft is a real problem. How real is it? Nearly 2% of Americans were victims of medical, according to the most recent Bureau of Justice Statistics.

Advertisement

NAVIGATING A WORLD OF ACCELERATING CHANGE CNET

Unauthorized login or password changes

If you just changed your bank password, you'll get an alert. But if you get an alert that your bank password has been changed, and you know you didn't do it, that's a major red flag. The same goes for any emails you receive about unrecognized login activity with your account.

How this can lead to identity theft

If your personal data, like your name, phone number or email address, is on the dark web, you'll be more vulnerable to identity theft and online scams. If a cybercriminal has some of your personal information, they're going to be able to craft a believable con more easily than if they are approaching a complete stranger.

Most commonly, identity thieves will put information and log in credentials on the dark web. There are many dark web sites with lists of usernames, emails and matching passwords for sale, according to Experian's guide to dark web monitoring, where they try your password from one site on a bunch of other sites, according to Andrew Wolfe, director of the cybersecurity program at Loyola University Maryland.

It's less common for your credit-card or government ID info to be openly published on the dark web, he said. So if your driver's license was stolen, that information probably won't be openly available on the dark web, for your run of the mill identity thief to see.

But don't exhale yet. Your stolen driver's license or Social Security number is still likely to be openly available on the dark web, and it can be worth valuable to identity thieves. Criminals will offer these for sale on dark web sales sites.

At the same time, you probably don't want to be too fearful when you think about the dark web. Not all of your information found on the dark web is too useful to bad actors.

Advertisement

NAVIGATING A WORLD OF ACCELERATING CHANGE CNET

"We typically worry that extremely sensitive information has been disclosed, and that cybercriminals are intent on using your particular information to destroy your life. This is an exaggeration," said Wolfe. "The dark web has tanker loads of data like your 2013 password for a yoga bulletin board. That is to say, most of this is trivial."

What can you do if your personal data is on the dark web

If you discover that your personal data is on the dark web, there's not much you can do. It's out there and may have already been used to steal your identity. But there are preventative measures you can take to minimize the consequences.

Sign up for ID theft monitoring

With data breaches happening more often, it's difficult to keep your information from getting into the wrong hands. But you can keep a pulse on your data with an identity theft monitoring service.

"It is extremely valuable to have some kind of dark web monitoring service," Wolfe said. "Many banks, credit unions, and other financial-service companies offer these."

For instance, Chase Credit Journey and Capital One's CreditWise offer dark web surveillance absolutely free. So too does the credit bureau Experian. However, these free services lack the digital security tools and advanced monitoring and restoration services many paid services offer.

CNET's choice
Best identity theft protection
See at Aura
Aura can let you know if your data's on the dark web.

Paid services like Aura and LifeLock provide more comprehensive coverage and typically range from $7 to $15 per month for individual accounts.

If your identity theft protection service tells you an account has been compromised, Wolfe suggests closing the account, or at least changing your password.

Freeze your credit

You can freeze your credit, so nobody can open loans, credit cards and other credit-based accounts in your name. But it also prevents you from opening a new account, unless you temporarily or permanently unfreeze your credit.

Credit freezes always sound good in theory, but they can be a time-consuming hassle to manage. But if your information is on the dark web and freezing your credit offers you peace of mind, you can do so online at each of the credit bureaus' websites.

A credit freeze is also not a complete solution for identity theft. For instance, if you put a freeze on your credit, they won't be able to take out a new loan, but if they already have your current credit card number, they could still go on an unauthorized shopping spree. And, since banks don't always run a credit check when you open a new bank account, someone could still open a checking or savings account in your name.

Change your passwords regularly

The best passwords are complicated. "Any password easy for you to remember is easy for a cybercriminal to guess," Wolfe said.

He adds that "with such hard passwords, nobody can memorize and reliably use more than a handful. But no reliable person expects you to. Basically, everyone needs a password manager."

He also warns against answering your password recovery questions correctly. Hackers likely know your former street, hometown and pet names, Wolfe said. So you'll want to answer these questions differently to prevent anyone other than you from logging in.

Review your bank statements

It may seem like a routine solution but going through your bank statements every month can help you keep an eye on potential red flags, according to Robin Chaiavat, assistant professor of cybersecurity and computer science at Quinnipiac University.

"Regular monitoring of your financial statements and credit reports can help you spot any unauthorized activity early," he says.

Look for any charges you don't recognize or even deposits that haven't come from sources you know.

How to report identity theft or a fraud case

If a data breach does lead to fraud or identity theft, contact the credit card company, bank or lender as well as the three major credit bureaus.

If you signed up for identity theft protection with white glove service orientation, the company should also assist you with these steps and help you fight any wrongful charges.You'll also want to notify the Federal Trade Commission.

"If identity theft is suspected, it's important to report it to the relevant authorities, such as the Federal Trade Commission in the US, to not only protect yourself but also help prevent further occurrences," Chaiavat said.

To report a fraud or identity theft case to the FTC, visit IdentityTheft.gov or call 1-877-438-4338.

The editorial content on this page is based solely on objective, independent assessments by our writers and is not influenced by compensation or partnerships. It has not been provided or commissioned by any third party. However, we may receive compensation when you click on links to products or services offered by our partners.

© 2024 CNET, a Ziff Davis company. All rights reserved.