Dark Web Monitoring: What You Should Know

You may see ads for identity theft services claiming that they will look for your Social Security number, credit card numbers, or other personal information for sale on the "dark web." Do you know what these services do if they find it? In a survey commissioned by Consumer Federation of America, 36 percent of people who have seen these "dark web monitoring" ads believed that these services could remove their personal information from the dark web, and 37 percent thought they could prevent the information that's sold on the dark web from being used. In reality, neither is true!

Here is what you need to know about the dark web, how identity theft services work, and what you can do if your personal information is in danger.

What is the dark web?

Picture the internet as an iceberg. The part above the water is the "surface web," where you can find webpages using search engines such as Google or Bing.

The part of the iceberg under the water is the "deep web." Search engines won't bring you to the pages here. This is where you are when you sign into your bank account online with your username and password. It's where the content is beyond paywalls. It's where you communicate with other people through social media, chat services and messaging platforms. The deep web also houses large databases and many other things. It is a significantly bigger chunk of the internet than the surface web.

The "dark web" is a small part of the deep web. Mozilla Firefox, Internet Explorer, Google Chrome and other commonly-used web browsers won't get you there; you need a special browser such as Tor. One of the features of Tor is that it disguises the computer that is being used to reach the internet, providing a high degree of privacy. While Tor can be used to go anywhere on the internet, if a website address ends in ".onion" it's in the dark web and only accessible via Tor.

The dark web sounds like scary place, but not everyone there is up to no good. It's used by whistle-blowers, investigative journalists, people organizing against repressive governments, law enforcement agencies, and others who need to shield their identities and locations. There are legitimate discussion groups, news sites, and publications there. But there are also people selling child pornography, illegal drugs, stolen personal information and other illicit goods and services. They commonly take payment in the form of Bitcoins or other "cryptocurrency" that can't be traced. The anonymity of the dark web makes it challenging for law enforcement to find and prosecute these people.

What can identity theft services do if my personal information is for sale on the dark web?

Identity theft services look for signs that that your personal information may have been used fraudulently. They usually check your credit reports, and some will monitor your financial accounts as well. They may also look at public records, commercial databases, and the internet. They have tools that the average person doesn't for accessing places that are hard to reach, such as sites that sell stolen personal information on the dark web. If they find something suspicious, they'll let you know.

Identity theft services also provide advice about what to do to remedy the problems they find. Some offer one-on-one counseling to guide you through the steps you need to take, and some go further, actually getting your permission to remedy the problems for you.

You can correct, and in some cases remove, information about you in commercial and public records that has resulted from identity theft. That's because you're dealing with legitimate companies, agencies or organizations that will cooperate with fraud victims. The dark web, however, is another matter. The people who trade in stolen personal information there won't cooperate with an identity theft service or anyone else, so it's impossible to get the information removed, stop its sale, or prevent someone who buys it from using it. What dark web and other types of monitoring can do is alert you so that you can take action to avoid or limit the damage that the fraudulent use of your personal information could cause and remedy any problems that have already occurred.

If you have reason to believe that your personal information has been stolen, you don't need dark web monitoring to know that it could end up for sale there.

What should you do if your personal information is in danger of fraudulent use?

This will depend on the types of personal information involved.

- **Financial and other account numbers.** Notify the places where you have those accounts. You may need new account numbers and to make other changes to stop those accounts from being misused from that point on. If fraud has already occurred, ask what you need to do to clear up the problems. You have the right to challenge credit card charges and debits you did not make.
- **Passwords.** Change them. And if you've used the same passwords for multiple accounts (a common but dangerous practice, since crooks often try them in several different places to see if they work), be sure to change them everywhere.
- **Driver's license and passport.** Contact the agencies that issued them.
- **Email address and phone number.** It's probably not worth the hassle to change them, but be on guard for your email address being used to send spam or your phone number being "spoofed" to make calls look like they're coming from you. Contact your service provider if that happens.
- **Social Security number.** This is the most dangerous type of personal information in the hands of identity thieves because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refunds, employment – even using your identity in bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your life in so many ways. There are a number of things you can do, including alerting the Social Security Administration, Internal Revenue Service and by placing fraud alerts or a security freeze on your credit files.

Medical records, diplomas and other personal information may also be found for sale on the dark web. At the Federal Trade Commission's www.identitytheft.gov website you can get step-by-step instructions for what to do, tailored to your specific situation. The nonprofit Identity Theft Resource Center also provides free help for identity theft victims. Go to www.idtheftcenter.org or call 888-400-5530.

If you are a data breach victim, take advantage of free identity theft services if they're offered. Thinking about buying identity theft services? Shop around and make sure you understand how they work, what they cost, and what help they provide if you become a victim before deciding whether to sign up and which one to choose. Do not be swayed by scare tactics, claims that an identity theft service can prevent you from becoming a victim, or million dollar guarantees. You can do many things you can do to monitor your personal information and reduce your risks. To learn more read CFA's tips, *Nine Things to Consider When Shopping for Identity Theft Services*, and go to our www.IDTheftInfo.org website, where you'll find additional information about identity theft from trusted sources.