Identity Theft and the Dark Web

Cybercriminals can potentially use your personal information in many illegal ways. By now, most people know of someone who has been victimized by identity theft, computer hacking or computer fraud. With activity increasing on the web, it is a priority to be aware of the risks and know what to do if you become the target of an attack.

The "dark web" is a term to describe parts of the internet where illegal activity is taking place. It is a hidden network of websites that requires special browser software and procedures to access. Computer hackers and schemers find ways to collect an individual's private information, such social security numbers, birthdates, addresses, credit card numbers, usernames, passwords, and more. Often, this private data is sold on the dark web to other criminals who use the information for their own financial gain - at your expense. Once cybercriminals buy your information, it can potentially be used to open new credit cards in your name, make fraudulent purchases, change your billing address, or even obtain a new driver's license.

Monitoring your personal information is important, especially if you feel you might be the victim of a data breach. Credit monitoring services can help by scanning the internet and dark web for your name and information and alert you to possible suspicious activity.

In 2021, cybercriminals have their eye on a new prize – stimulus checks. Reports show that a significant portion of the stimulus package money has been sent to cybercriminals.

P.O. Box 33698
San Antonio, TX 78265

Pho: 866.344.4477
Fax: 210-344-2777

A Better Way

These threats are not slowing down, and cybercriminals are getting smarter as they search for ways to trap even the most warry of internet users. One important step to help protect yourself from cybercriminals is credit report and identity theft monitoring. Working with a credit report and identity theft monitoring service helps bring you alerts for suspicious activity. You can also receive identity theft insurance and identity restoration assistance, giving you peace of mind if you're target by a cybercriminal. Make sure your finances and your identity are protected.

If your Social Security card is stolen, it can be a major cause for concern. With just your Social Security number, identity thieves can wreak havoc in your name, negatively impacting your credit, finances and even commit crimes in your name. As soon as you discover that your card is missing, or someone is using your number, you should do the following:

1. Contact local law enforcement.

File a crime report right away. You need to show copies of the report to let other agencies know that your personal information is at risk.

2. Let the three major credit bureaus know.

Add a fraud alert to your credit report at the three major credit bureaus – TransUnion, Experian, and Equifax – if you are a victim of fraud or you may be. This alert can help creditors take extra steps to confirm your identity before issuing new credit under your name. Signaling one agency alerts the other two automatically.

3. Check your credit report.

One of the first places you may see indicators of identity theft is on your credit report. Thieves can use your information to take out a new credit card or loan in your name. That can show up on your credit report. Take advantage of regular checks of your credit report to help quickly catch suspicious activity.

4. Completely freeze your credit.

Freeze your credit so no one can access your credit information. You can turn the freeze on and off with each credit bureau individually.

5. Get a new Social Security card.

It can be helpful to have a copy of your Social Security card to prove your identity, so replace it and keep it in a secure location.