Identity Theft on the Internet

There are a lot of films out there that portray what a powerful criminal tool the internet is. Most of these show hackers stealing document files online. But did you know that identity theft can occur on the internet as well?

In today's world, the internet has become a haven for criminals and scam-artists. Most of these criminals gain access to passwords, personal data, and identifying information in order to gain access to a person's assets.

Most of this information can be acquired via various forms of spam email. Another method crooks use to get your information is by getting the victim to sign up on a website that promises him/her profits. This allows the criminal to secretly gather your information. Later on, they use it to impersonate the victim.

But criminals aren't just looking for your bank account number or social security number. They try to find out about your lifestyle as well. This enables them to do more spying.

But how does all of this happen?

Cookies play an important role. The cookie is a piece of text which the web server leaves on your computer to allow you to easily access information in the future. Cookies have information about the user's personal preferences. It can also carry information about which sites the user has visited, the email sent, and even which advertisements the user has clicked on.

Most cookies are harmless, but criminals use the cookie as a tracking device. Not only that, they use it to get precious personal data. A cookie also gives criminals an idea of in which of your areas of interest they should perpetrate the scam.

Most internet thieves use software to get access to public data records. Out of public records, the thief can get information like the victim's date of birth, their surname, maiden name, address, social security number, and more.

Aside from public record databases, most of the thieves use web-links. They just type in the Social Security number to get the info they need. The internet connects them to a search engine, which, according to recent information, has about 95 identity sites. Basically, the criminal can just click on the person's file and all their personal information will pop up.

Some criminals create fake websites. If the viewer of one of these websites subscribes, and enters his or her personal information, all of that personal information then falls into the hands of the criminal.

Beware # any machine in a public place is distributed to multiple users. When you make a purchase online, the website will leave a tracking cookie on your computer. If someone finds that information on the internet, he or she could try to acquire something from the store on your account.

There are other hackers that use encryption software. This software can be used to mix credit card numbers. This allows the criminal to figure out your number.

Keep in mind that sending your personal identification number to an online store is not completely safe. The only time encryption happens is when the viewer uses a secure shopping site. If it is encrypted, the site will show a padlock icon in the lower corner of the web browser.

Most internet identity theft criminals want to have access to someone's personal account. Most of them intend to start spending money and take the identity to make new purchases.

For instance, many of the criminals have poor credit and do not have the capacity to take out a loan. Because of this, they get someone else's account to use in an internet transaction.

With the beginning of this internet fraud, identity theft has become a profitable industry. Criminals, hackers, and scam-artists have easier and quicker access to classified data around the globe.

In order to prevent this from happening to you, you should be very careful transacting business on the web. Look for the padlock icon in the bottom corner of your browser before hitting the "checkout" button.