10 pieces of information used to steal your identity

Stealing identity can cause incalculable consequences for victims. Let's explore 10 kinds of information that thieves use to steal identities through the following article!

According to a recent study, identity theft causes more damage than household theft, vehicle theft and property theft. Stealing identity can cause incalculable consequences for the victim, and it is best not to let anyone undergo this.

Let's explore 10 kinds of information that thieves use to steal identities through the following article!

What do scammers need to steal your identity?

1. 1. Social security number
2. 2. Your date and place of birth
3. 3. Account number
4. 4. Bank PIN
5. 5. Your card expiry date and security code
6. 6. Email address and home address
7. 7. Passport number or driver's license
8. 8. Phone number
9. 9. Your full name
10. 10. Groups you join

Scammers don't need all the details involved to steal your identity; only a few of them are enough. Thus, you need to protect every detail to make sure no future attacks occur.

1. Social security number

Social security numbers can confirm your identity in many places, from opening a PayPal account to receiving documents from law enforcement agencies. Social security numbers can be used to create a new bank account, access online accounts or fraudulent tax returns.

In short, the social security number (or something similar to it, if you live in another country) is a "lucrative prey" for identity thieves. And once they get this number, it is easier to collect other information needed to steal your identity.

2. Your date and place of birth

Surprisingly, birth dates can also be used by a fraudster to steal your identity. What can scammers do with your birthday?

Birthdays are required on most administrative documents to financial-related accounts. Your birthplace is also used as a secondary endorsement by some online providers. This can be used to reset your password or grant thieves access to your account.

Unfortunately, people tend to disclose their birth dates on the Internet. Social networking makes it easy for people to know when a special day is coming, so people want to share it with the world.

3. Account number

Financial-related accounts are always hunted by identity thieves. This includes check numbers, savings account numbers, credit card numbers, debit cards and retirement account.

With an account number, an identity and password or PIN, the thief can gain access to any of these accounts and start withdrawing money.

Thankfully, perhaps you don't often share account numbers. In fact, not many people put their credit card numbers on Twitter! Therefore, it is quite easy to protect this information. Just make sure these numbers are not where scammers can find it, such as a sticky note on a table.

With the proliferation of scams related to the health care sector, protecting your health insurance number and any other similar information you have is a good idea.

4. Bank PIN

Your personal identification number should be randomly selected, but many people still use combinations like '1234', '5280' and '1111' to secure their credit and debit cards. Thieves know this, so if you have a weak PIN, they will easily invade your card if it is stolen.

People often use personal information as PINs, such as birth dates. Unfortunately, as we mentioned above, this information is regularly posted on social networks and easily found. Hackers will try these numbers first, so don't put your PIN based on the number someone can research and find out.

Also, be sure to use different PIN codes for different accounts. If an identity thief enters an account, you probably don't want to give them access to other accounts, right?

5. Your card expiry date and security code

When you buy items online with your credit or debit card, you usually need to enter an expiration date and security code.

If a thief has your card number and this information, they can freely use your card on the Internet. High-handed scammers can get this information from a malicious device, but phishing is still a standard method that scammers use.

So, don't give this information unless you're sure you're talking to someone who really needs it. Phone phishing is aimed at this information, so be suspicious if you receive any unexpected calls from the credit card company.

6. Email address and home address

Both can be used in phishing to trick you into revealing personal information. Even past addresses may be helpful, as some organizations will require your previous address during the registration process. All this information can lead to whaling, a type of cyber attack that is worse than phishing.

Your email address is also the username for many online accounts. With appropriate pieces of information, a thief can access the account or reset the password. Like birthdays, email addresses are often quite easy to find, but you can limit the disclosure of them a bit.

7. Passport number or driver's license

Both your driver's license number and your passport can help identity thieves get more information about you. After all, these contain your full name, date of birth, nationality and address.

If a fraudster steals your driver's license or passport, these documents may be changed with the image of another person. Once completed, crooks can use it to interfere with different things in your life.

Passport is particularly dangerous, as it can lead to identity theft at the international level. Fraudsters can create accounts under your name in other countries and any existing accounts in other countries are likely to be attacked. The thief can also create a modified passport, allowing him to travel internationally under your name.

8. Phone number

Phone numbers are not used to verify identity often, but it can be used by a high-fraud scam. They can call and pretend to be a financial institution or a state agency to exploit more identity information from you.

Most people are reluctant to give out their phone number, but once an opening can make you a victim of scams. It would be good if you were always wary of making your phone number, but having a little suspicion about strange calls is also a good idea.

9. Your full name

This information appears a lot on the Internet, so you may not think it is valuable information for a thief. However, your name, middle name and last name may be quite useful for a thief. This information is especially useful if they are trying to open a new account under your name.

When buying online, some companies require full names. If a thief knows your full name, they will more accurately guess what may appear in your card.

10. Groups you join

Again, you may not think this is valuable information for an identity thief. However, such information can be used in phishing attacks, especially spear phishing.

Most people are more likely to give identification if they think they are talking to someone from a group they join. This group can be colleagues, sports clubs, fan clubs or even a group on the Internet.

Anyway, the best way is to stay alert and make sure you're talking to the right people. If someone asks for personally identifiable information, you should confirm with the organization if they need it and who called to get it.

It's amazing to know the information that a fraudster can exploit to steal your identity. Identity theft is a terrible thing, so don't let scammers get the chance to get that information from you.

If you're worried about what you reveal on the Internet, be sure to learn how hackers steal your identity on social networks.