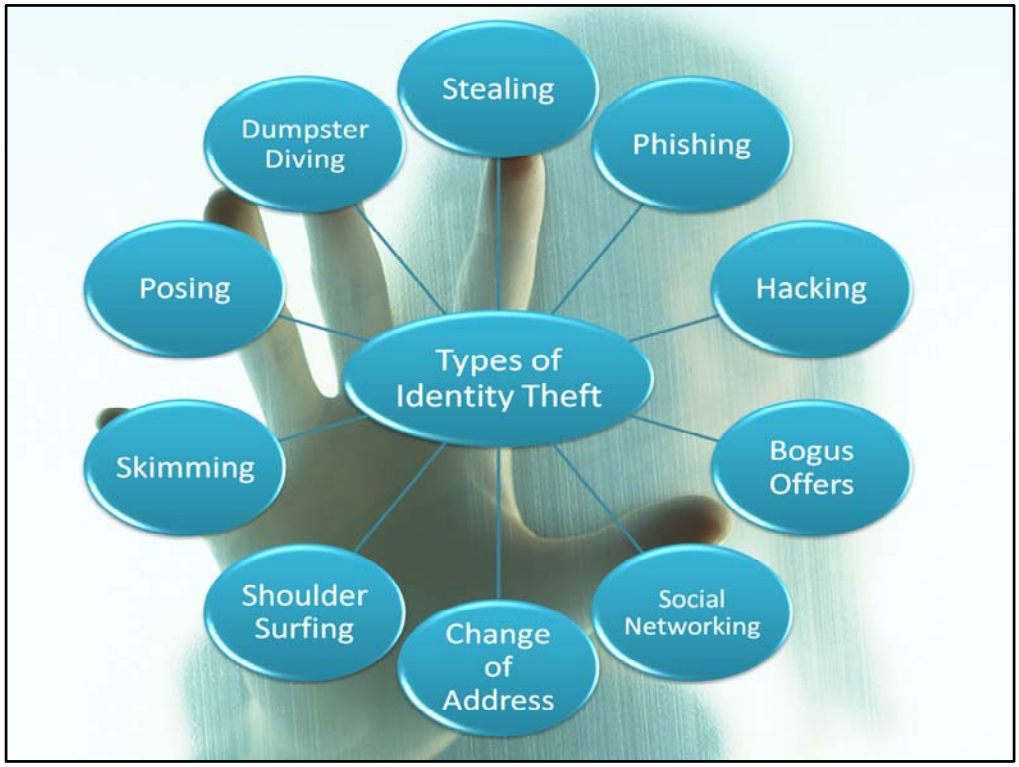
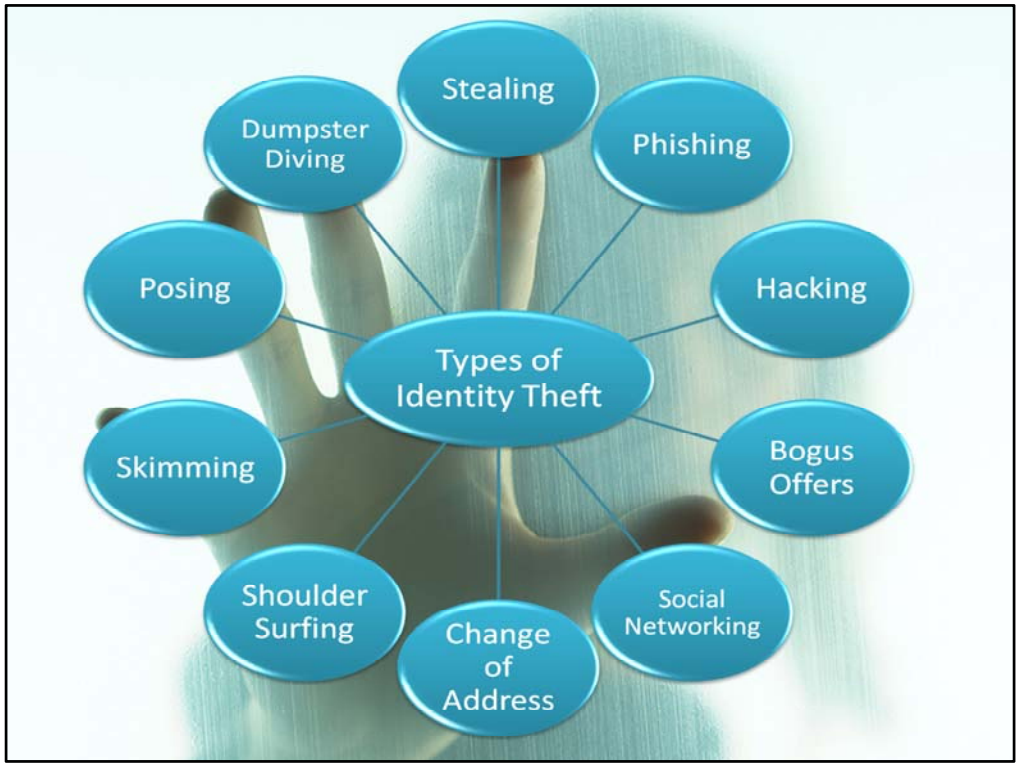
Identity theft is a growing crime in which an impostor steals personal information, such as your name, account numbers, Social Security number, or driver's license number and uses them to assume your identity. Once they have your information, they can then open bank accounts, make purchases, obtain cash, get an apartment, or commit crimes in your name!

So, how do criminals get your personal information in order to assume your identity?



Click on each of the types of identity theft shown here to learn more about the methods that criminals use to obtain your personal information.



Continue to explore each type of identity theft shown. Once you have learned about each type, click the next button to learn more about preventing identity theft.

In order to get your information, criminals may simply steal it. They may have access to your information through their own place of employment so they may steal your information while they are at work. Others may bribe another employee who has access to the information at their job. They may even con or trick another employee into getting your information for them. They may even steal your mail, including your bank statements, credit card statements, credit card offers, new checks, and tax information. Some may just steal your wallet or purse or rob your home in order to steal your personal information.

Click on the “Next” button to return to the menu.

Dumpster diving is when criminals go through your trash to get your personal information. Also, they can go through a business's trash or the public trash dumps to get your information.

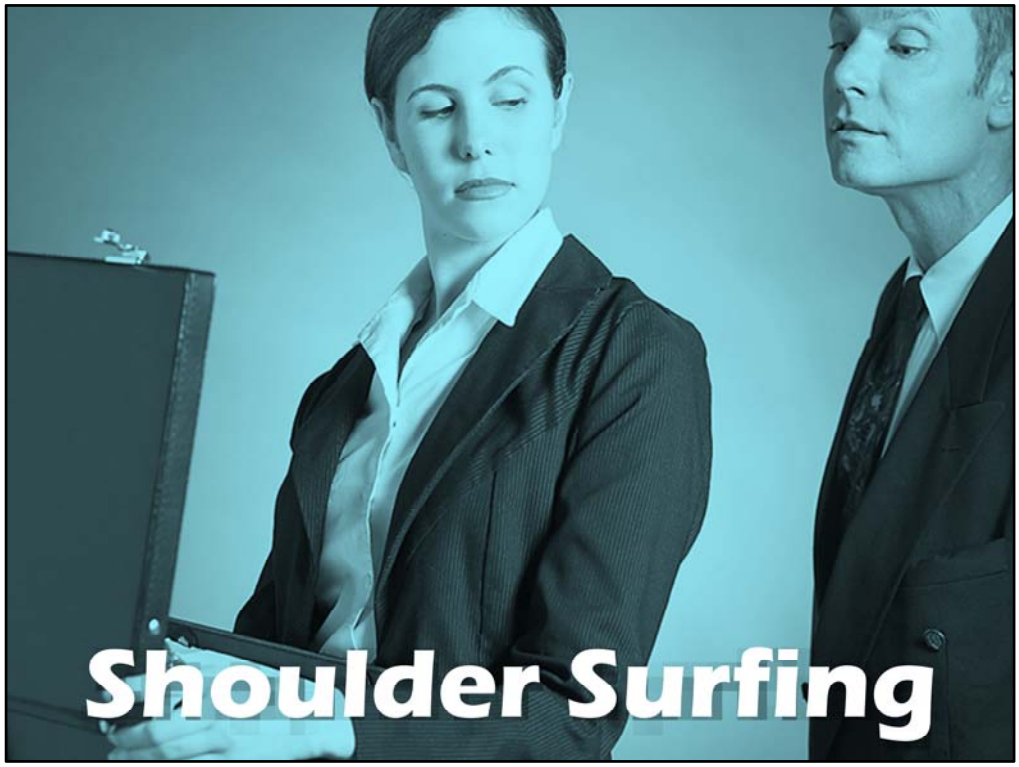
Click on the "Next" button to return to the menu.

Other criminals may get your credit reports by posing as a potential landlord, employer, or anyone else who has the right to see your credit report, like a loan officer. When dealing with any individual or company, be sure to ask them for references and check their rating at a consumer protection site like the Better Business Bureau.

Click on the “Next” button to return to the menu.

Skimming is when someone steals your credit or debit card number with a storage device that captures data from the magnetic strip on your cards. The device could be attached to the machine where you swipe your card to make a purchase or to an ATM when you withdraw money. This is especially true if the machine is outside like a gas station pump. Be sure to check a machine before you insert you card and be wary if the card swiping area is loose or a different color from the rest of the machine. If you suspect anything, leave and go to a different ATM or gas station.

Click on the "Next" button to return to the menu.



Shoulder surfing is when a thief eavesdrops on transactions conducted in public areas in order to obtain your personal data. When the clerk asks for your zip code or phone number, thieves can overhear and you may become a target. Be sure to speak at an appropriate volume when providing personal information and cover any key pads from the view of other people.

Click on the “Next” button to return to the menu.

Phishing is when someone sends an email posing as a trusted company in order to get you to reveal personal information. For example, a criminal may send you an email pretending to be your bank saying that your account may have been compromised and they need you to provide some personal information like your PIN or social security number in order to ensure that your account has not been tampered with. Never send this information via email; instead, visit the bank in person to confirm any issues.

Click on the "Next" button to return to the menu.

Hacking is the unauthorized use of computer and network resources to steal personal information from computer databases. Sometimes databases are leaked to the public because of improper handling or malicious actions. These databases may contain personal information. Computer savvy criminals can hack into a company's database and get information on their clients and employees.

Criminals can also use the Internet to find out all kinds of information about you. They can research potential victims using government registers, search engines, or public records search services.

Click on the "Next" button to return to the menu.

Some criminals may advertise bogus, or fake, offers such as home-based work, private insurance, fixing bad credit, etc. When people reply to the advertisement, they are asked to provide their full name, address, phone numbers, banking details, etc. They may even be asked to submit a resume which lists all of their work history.

Click on the "Next" button to return to the menu.

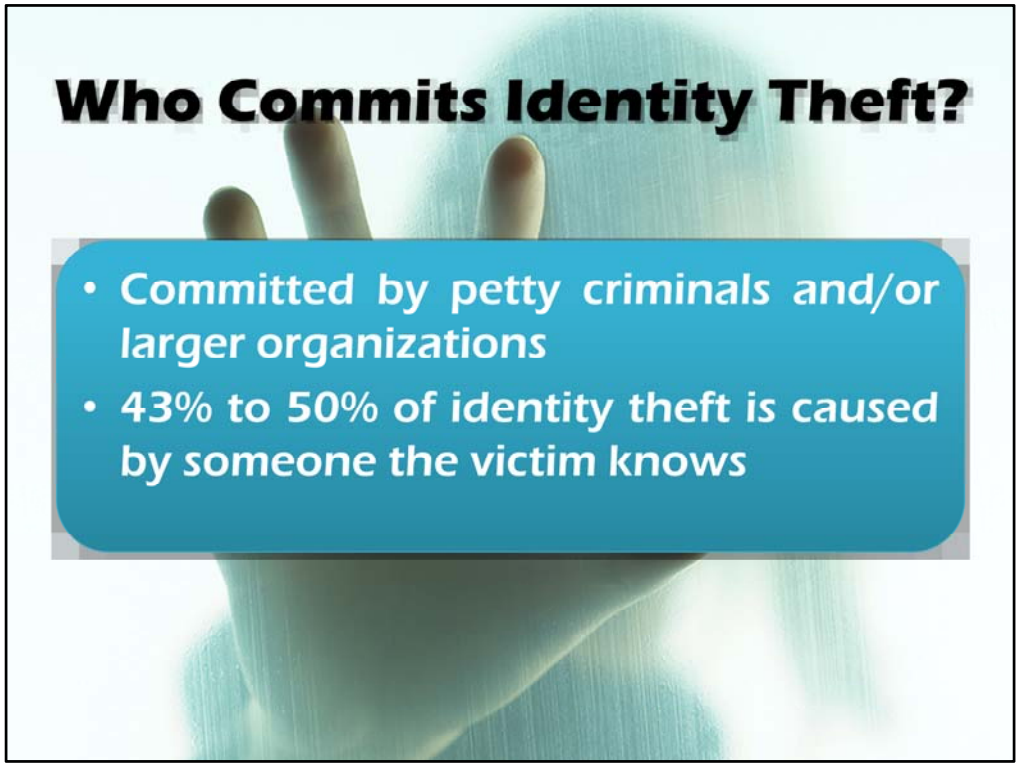
Many people post personal information online through their social networking sites like Facebook or MySpace. When you post your location or your vacation plans, criminals can obtain that information by browsing these sites. Make sure to set your privacy options in such a manner that only your trusted friends can view your information and never post information about your whereabouts.

Click on the "Next" button to return to the menu.

Criminals may go to the post office and fill out a change of address form. They change your address so that your bills and statements are sent to them at another location so that they can get current account information. A change of address could also delay your discovery of their fraudulent activities, like setting up new accounts in your name.

Click on the “Next” button to return to the menu.

Unfortunately, methods to illegally obtain your personal information and money are ever-evolving. You should pay attention to the news for stories on the latest scams to educate yourself.



Identity theft can be committed by several different parties, ranging from petty criminals looking for quick money or larger organizations, like fake companies, scamming multiple individuals.

The most upsetting fact is that anywhere from forty three to fifty percent of identity theft is caused by someone the victim knows. It's not always a random crime, so be sure you always protect your personal and financial information.

It may be impossible to completely protect yourself against identity fraud, but there are some things you can do to make it far more difficult for criminals to obtain your information.

First, it is up to you to protect your information. When storing financial documents with sensitive information, be sure to keep them in a secure place that is not easily accessible to someone that would want to steal your information.

Once you no longer need them, be sure to shred any sensitive documents, especially those containing financial information, before throwing them away. When you shred documents, you make it more difficult for a criminal to access your information once it has left your possession.

Next, be sure you know who you are dealing with before you provide anyone with your personal information. Only share credit card and other personal information with a company that you know and trust and refuse to give the information to phone or email solicitors.

Also, when making internet purchases or entering your personal information on the web, be sure to use secure Internet sites. Look for the lock icon or the prefix “https” on websites, so you can confirm that a company has protected their customers from hackers.

Always be aware of your surroundings, especially when making financial transactions. Does it seem like someone is paying a little too much attention to you in a public place? Don't discuss personal information out loud, or within earshot of someone suspicious.

In case of loss or theft of your ID, checkbook, credit cards, or other financial information and data, report it immediately to all affected financial institutions or state agencies. You should keep a list of these important numbers somewhere safe in your home so that you can contact them as soon as possible if a theft or loss occurs.

Check your financial statements regularly. If you notice anything amiss on your bank or credit card statement, contact your bank immediately. If you notice mail coming to you mentioning a new account you have opened or a new line of credit, try to investigate the issue immediately in case someone has opened an account in your name.

You think you've had your identity stolen; now what? If you think you have been a victim of fraud or identity theft, there are four steps you should follow:

First, contact the fraud departments of one of the three major credit bureaus, Equifax, Experian, or TransUnion, and ask them to place a fraud alert on your account. An initial alert lasts for ninety days, and an extended alert lasts for seven years. Once you have placed a fraud alert on your account, you can obtain free reports to continue monitoring your account. As you review your report, look for loans that you didn't apply for, accounts you didn't open, and debts you didn't incur. Check your personal information like your social security number, address, name, initials, employer, birth date, etc. and have the credit bureau fix or remove any incorrect information.

Next, close any accounts that you believe have been used without your permission, tampered with, or opened fraudulently. Be sure to talk to someone in the security or fraud department of each company and be sure to send a letter to each company you talk to over the phone. In that letter, include documentation of the problem, but keep the originals for your records. You can send the letter by certified mail or return receipt through the post office. This lets you know when the letter has been received and who signed for it.

Next, you should file a police report. If you know where the theft or fraud took place, the report should be filed at the station closest to that location. Be sure to get a copy of the report for your file and make copies of it so that you can send proof to your creditors that you have filed a report.

File a complaint with the Federal Trade Commission, or FTC, for identity theft issues or other frauds. When you report the crime, you are providing important information that will help the "good guys" track down scam artists and stop them! The FTC can also give you information about scams in your area and they can give you information that can help the police in your area.