What To Do If You're a Victim

If you're a victim of identity theft, the Federal Trade Commission (FTC) recommends that you do the following:

- Contact the fraud department of the three major credit bureaus to place a fraud alert on your credit file. The fraud alert requires creditors to contact you before opening any new accounts or making any changes to your existing accounts.

- Close the accounts that you know or believe have been tampered with or opened fraudulently. Use the ID Theft Affidavit (available on the FTC website and accepted by the three major credit bureaus) when disputing new unauthorized accounts.

- File a police report. Get a copy of the report to submit to your creditors and others who may require proof of the crime.

- File your complaint with the FTC at www.consumer.gov/idtheft. The FTC maintains a database of identity theft cases used by law enforcement agencies for investigations. Filing a complaint also helps the agency learn more about identity theft and the problems victims are having so that it can better assist you.
Follow up with and it doesn’t arrive. And Trans Union at least twice a year from the three major credit bureaus: Equifax (www.equifax.com) and Experian (www.experian.com). The Fair Credit Reporting Act allows you to get one free credit report from each of the three major credit bureaus once per year. Visit www.equifax.com or www.experian.com to order your credit report, and send the letter return receipt requested. You have not used in the last six months.

Make a list of all your credit card account numbers and get your PIN numbers. Be careful when using ATM machines and long-distance telephone calls. Only use secured sites. Look at the bottom of the screen for a padlock symbol. Do not give out personal information. Pay attention to your billing cycles. Cancel all credit cards initiated the contact or know with whom you’re dealing.

How to Prevent Identity Theft

• Make a list of all your credit card account numbers and get your PIN numbers.
• Order your credit report and correct all mistakes on your credit report in writing.
• Pay attention to your billing cycles.
• Cancel all credit cards unless it is encrypted on a secured site. Look at the bottom of the screen for a padlock symbol. Do not give out personal information.

Identity Theft is the fastest growing crime in America, affecting half a million new victims each year. In the course of the day you may write a check at the drugstore, charge tickets to a concert, rent a car, call someone at work, or visit a bank. You purchase something advertised for sale on the Internet or through the phone book. Scams and schemes are a criminal’s “bread and butter.” If you have a computer, a telephone, or a credit card account, you are potentially somebody’s target.

How Identity Theft Occurs

How Identity Theft Occurs

• Someone else uses (steals) your identity to obtain money from a victim’s existing accounts, apply for credit and credit cards from banks and retailers, steal Social Security or account numbers and credit card information. They may send you an email message that says your account must be updated immediately.
• You get an email or pop-up message that says your account must be updated immediately.
• You are promised a credit card regardless of your credit history, for a fee. Or you are promised credit card protection or credit repair services, also for a fee. You pay, but the card or service is never delivered.
• You get an email that contains a link to a bogus website so they can steal your Social Security or account numbers and credit card information. They may send you an email message that says your account must be updated immediately.
• Telephone Slamming: You miss seeing them because your phone bill is complicated with authorized charges such as voice mail and Internet service.
• Unauthorized charges for goods or services appear on your phone bill, but you did not authorize them. You are offered a magazine subscription at a very low price by someone who claims to work for the magazine company. The price is misrepresented and is actually much higher, or the magazine is never delivered.
• Magazines are not delivered at all. You pay for the magazine or materials and you receive a kit with cheap craft materials and there are no clients to pay for your work. A company guarantees scholarship money for an upfront fee, but it only recruiting new members. Plans that promise profits for recruitment of members rather than for selling goods and services are illegal and usually collapse.

• Bogus Merchandise Sales: A company guarantees you an insurance policy for a fee, or it will be closed. You click on a link to a website that looks like it belongs to your bank or other institution and “update” your account by entering personal identifying information. Soon you discovered you are a victim of identity theft.
• Telephone Cramming: You get an email or pop-up message that says your account must be updated immediately.
• Pharming: Pharmers “poison” the Domain Name Service in order to “fool” a user’s browser into linking to a bogus website.
• Phishing: You are offered tickets to enter a foreign lottery and send money, but you did not authorize them.
• Nigerian Money Scam: You are invited to participate in an investment opportunity and promised spectacular profits with no risk. Instead of making money, you lose it.
• Charity Scams: A company guarantees scholarship money for an upfront fee, but it only recruiting new members. Plans that promise profits for recruitment of members rather than for selling goods and services are illegal and usually collapse.
• A company guarantees you an insurance policy for a fee, or it will be closed. You click on a link to a website that looks like it belongs to your bank or other institution and “update” your account by entering personal identifying information. Soon you discovered you are a victim of identity theft.
• Bogus Merchandise Sales:
• Telephone Cramming:
• Pharming:
• Phishing:
• Nigerian Money Scam:
• Charity Scams:

How to Prevent Identity Theft

• Make a list of all your credit card account numbers and get your PIN numbers.
• Order your credit report and correct all mistakes on your credit report in writing.
• Pay attention to your billing cycles.
• Cancel all credit cards unless it is encrypted on a secured site. Look at the bottom of the screen for a padlock symbol. Do not give out personal information.

Charity Scams:

■ A company guarantees scholarship money for an upfront fee, but it only recruiting new members. Plans that promise profits for recruitment of members rather than for selling goods and services are illegal and usually collapse.

• Bogus Merchandise Sales: A company guarantees you an insurance policy for a fee, or it will be closed. You click on a link to a website that looks like it belongs to your bank or other institution and “update” your account by entering personal identifying information. Soon you discovered you are a victim of identity theft.
• Telephone Cramming: You get an email or pop-up message that says your account must be updated immediately.
• Pharming: Pharmers “poison” the Domain Name Service in order to “fool” a user’s browser into linking to a bogus website.
• Phishing: You are offered tickets to enter a foreign lottery and send money, but you did not authorize them.
• Nigerian Money Scam: You are invited to participate in an investment opportunity and promised spectacular profits with no risk. Instead of making money, you lose it.
• Charity Scams: A company guarantees scholarship money for an upfront fee, but it only recruiting new members. Plans that promise profits for recruitment of members rather than for selling goods and services are illegal and usually collapse.