How criminals commit ID theft

ID THIEVES ARE ALWAYS LOOKING FOR WAYS TO STEAL YOUR PERSONAL INFORMATION. HERE ARE SOME OF THEIR TACTICS.

MAIL THEFT

Thieves will steal mail directly from unlocked and low visibility mailboxes, enabling them to access your personal information from bills, statements, etc.

DUMPSTER DIVING

Thieves will sort through garbage to find old bills, recent receipts and other discarded personal information.

DATA BREACHES

If the companies you do business with store your personal information – even a huge insurance or medical corporation – your identity could be compromised in a large-scale data breach.

ATM OVERLAYS

Thieves could install these devices at ATM machines and gas pumps to steal your account information when you insert your card.

CHANGE OF ADDRESS

Thieves will change your address and divert your mail into the wrong hands.

MALWARE & VIRUSES

With the number of new viruses, your computer and your information can be hacked through websites, Internet programs or file-sharing networks allowing thieves to access your private personal information.

STOLEN WALLET

While some thieves might be after your wallet or purse for money, others are more interested in your personal identification, which they could use to steal much more than just your cash.

SHOULDER SURFING

Thieves stand behind you with a camera – or even their own eyes—and watch as you enter passwords, personal identification numbers or private information.

KEYSTROKE LOGGING

On public computers, gas pump displays and ATM keypads, criminals can install technologies to record the buttons you press as you enter card numbers or passwords.

VISHING

Phone scams that request personal information either by a direct caller or through voice messages can be used to steal your identity.

Questions? Please visit LifeLock.com or call 1-800-LifeLock (543-3562).
A U.S.-based agent is available to help.

No one can prevent all identity theft.

LifeLock

PROTECT YOURSELF WITH THE BEST

800-543-3562 | lifelock.com

How criminals commit ID theft

ONLINE SHOPPING

If you mistakenly shop at a fictitious retail website or through unsecured payment systems, your credit and debit cards could be at risk.

THE DARK WEB

This is an underground, online community where criminals can go to buy and sell your personal information.

PHISHING

These are fake emails that can look surprisingly legitimate. If you get tricked into clicking a link or providing information, thieves can get your passwords and account numbers.

SMISHING

Phishing through a Short Message Service (SMS) or text message. The message will direct you to visit a website or call a phone number.

How thieves can use your stolen information

ONCE A CRIMINAL HAS WHAT THEY NEED TO PRETEND THEY'RE YOU, THEY CAN START DOING VERY BAD THINGS FOR THEIR GAIN AND YOUR LOSS. HERE ARE FOUR EXAMPLES.

TAX-RELATED ID THEFT

By only using a stolen Social Security number and birthdate, identity thieves can file a fake tax return in your name.

DRAIN ACCOUNTS

Under your name, thieves can withdraw money or make major purchases like a house or car while you're stuck with the bill.

MEDICAL ID THEFT

You may not notice this type of theft until it's time for medical treatment or an insurance claim. Thieves can use your name or insurance information to receive medical care.

OPEN NEW ACCOUNTS

Thieves can open accounts for credit cards, loans, utility accounts and more in order to make purchases or steal funds. These accounts may not be detected for a year or more.

Questions? Please visit LifeLock.com or call 1-800-LifeLock (543-3562).
A U.S.-based agent is available to help.

No one can prevent all identity theft.