

Tips to Prevent Identity Theft

In recent years, identity theft has been on the rise. It has become synonymous with drug users and their way of getting the drugs they need. Identity theft occurs in many different ways. According to the non-profit Identity Theft Resource Center, identity theft is sub-divided into four categories:

- Financial identity theft (using another's identity to obtain goods and services)
- Criminal identity theft (posing as another when apprehended for a crime)
- Identity cloning (using another's information to assume his or her identity in daily life)
- Business/commercial identity theft (using another's business name to obtain credit)

Identity theft may be used to facilitate crimes including illegal immigration, terrorism, and espionage. Identity theft may also be a means of blackmail. There are also cases of identity cloning to attack payment systems, including online credit card processing and medical insurance.

Some of the techniques used for stealing personal information include:

- Stealing mail or rummaging through rubbish containing personal information (dumpster diving).
 - **Mail theft from the local post office has been one of the leading ways to steal checking information. Suspects are using a mail fishing technique to steal mail from the postal drop boxes located in front of the post offices. DO NOT DROP MAIL AFTER HOURS! The times that the thefts occur from the drop boxes are usually between 8PM and 8AM, before the Post Office opens. Checks are washed and cashed the very next day.**
- Retrieving information from redundant equipment, like computer servers that have been disposed of carelessly, e.g. at public dump sites, given away without proper sanitizing etc.
- Researching about the victim in government registers, internet search engines, or public records search services.
- Stealing payment or identification cards, either by pick pocketing or surreptitiously by skimming through a compromised card reader.
- Eavesdropping on public transactions to obtain personal data (shoulder surfing).
- Stealing personal information in computer databases (Trojan Horses, Hijacking).
- Sometimes databases are leaked to public due to improper handling or malicious actions. Such databases may include identity information.
- Advertising bogus job offers (either full-time or work from home based) to which the victims will reply with their full name, address, curriculum vitae, telephone numbers, and banking details.
- Infiltration of organizations that store large amounts of personal information
- Impersonating a trusted company/institution/organization in an electronic communication to promote revealing of personal information (phishing).
- Obtaining castings of fingers for falsifying fingerprint identification.
- Browsing social network sites (MySpace, Facebook, Bebo, etc), online for personal details that have been posted by users.
- Changing your address, thereby diverting billing statements to another location to either get current legitimate account info or to delay discovery of fraudulent accounts.

The best way to not become a victim of identity theft is to be vigilant of your surroundings when out in public. Constantly check your bank accounts or enroll in an identity safe program with your banking institution. Keep tabs on your credit by contacting the three credit reporting agencies.

- Calling toll-free at 1-877-IDTHEFT (1-877-438-4338).
- The FTC can also be reached at its website at <http://www.ftc.gov/bcp/edu/microsites/idtheft/>.
- Contacting SSA at 1-800-772-1213 (toll free), or
- By visiting SSA's website at <http://www.socialsecurity.gov/reach.htm>.
- Equifax — 1-800-525-6285
- Trans Union — 1-800-680-7289
- Experian — 1-888-397-3742
- ic3.gov

Detective J. Trevino #1242
Haltom City Police Department
Financial Crimes Division
817-222-7035