

The ABCs of Identity Theft

Empowering yourself against identity theft and fraud begins with knowledge. The more you know about what risks are out there, the more you can take measures to prevent yourself from becoming a victim. Let this glossary help you get better acquainted with the most common terms associated with ID theft.

Card Scanning

A device used to scan and save information from credit cards, drivers licenses, passports, medical cards and other laminated cards. Unfortunately, these devices are readily accessible to buy online.

Data Breach

The unintended disclosure of information that compromises the security of personal information, and can often lead to instances of identity theft.

Drive-by Download

Software that secretly and automatically installs on your computer when you visit certain websites. The user is usually unaware that anything was installed until after the fact.

Fraud

Any act or practice resulting in the loss of someone's rights or property. It usually involves making false and misleading representations with the intention of cheating or stealing from another person.

Hacker

Someone who exploits security holes in technology for any purpose.

Hidden Dialers

Programs that can use your computer to dial expensive phone calls that later show up on your phone bill.

Identity Fraud

Identity fraud is different from identity theft. ID fraud is using personal information that is made up rather than stolen from a real person.

Identity Theft

Identity theft occurs when a thief steals someone else's personal information as his own, creating a new identity of an existing person. Some ID theft items can include a social security number, driver's license number, usernames and passwords, employee ID number, mother's maiden name, and account information, including bank accounts and credit accounts.

Keystroke Logging

A software development tool that captures the user's keystrokes. Its intended use is to measure employee productivity on clerical tasks. Keylogging has been abused by individuals who can easily buy the tool to spy on computers and obtain passwords or encryption keys.

Mail Fraud

Thieves steal paper mail from your mailbox to obtain personal information, pre-approved credit card applications, medical insurance statements or any other information that will help them get credit in your name.

Malware

Short for “malicious software,” it refers to any harmful software. Malware includes computer viruses, worms, Trojan horses, and also spyware.

Pharming

Hackers redirect internet traffic from one website to a different, identical-looking site in order to trick you into entering your username and password into the database on their fake site. Your computer or DNS server has been hijacked into going to the fake site.

Phishing

Thieves trick someone into giving them confidential information, usually through links within emails sent to the user falsely claiming to be a legitimate business or company in order to scam the user into giving private information. In most cases, these emails appear to come from financial institutions.

Pretexting

Thieves collect individual's personal information under false pretenses such as posing to be from a charity or other legitimate organization. This is typically done over the phone or via email.

Security Alert

A statement added to one's [credit report](#) when a credit bureau is notified that the consumer may be a victim of fraud. It remains on file for 90 days and suggests that creditors should request proof of identification before granting credit in that person's name. Once a security alert is in place, the report is no longer available for online viewing.

Spam

Unsolicited commercial emails. Many of these come from legitimate companies but many also come from questionable businesses.

Spoofing

A fraudulent website or email that appears to be from a well-known company and attempts to get you to provide, update or confirm personal information. Similar to pharming.

Spyware

General term for any technology that gathers about a person or organization without their knowledge. Advertisers or other interested parties often use spyware programming to gather and relay information.

Trojan Horses

Unlike a virus, Trojan horses contain or install malicious programs that can run autonomously, masquerading as a useful program, or hack into the code of an existing program and executes itself while that program runs.

Viruses

Malicious programs with the ability to replicate and install themselves, or infect, a computer without the computer user's knowledge or authorization. Viruses are often unintentionally downloaded when the user accidentally clicks on a link to a virus.

Vishing

Using Voice over Internet Protocol (VoIP) phone numbers to steal user information.

Worms

Computer viruses which can self-replicate by resending themselves via email or a network message.

http://www.identitytheft.com/index.php/article/identity_theft_glossary