**August 8, 2013 Release # 227**

-- Begin Transmission --

# What You Need to Know to Avoid Identity Theft - Part 2

## Types of Identity Theft

When it comes to identity theft, the first step in protecting yourself is learning what thieves are doing to steal your personal information. This article explores the evolution of techniques from old-school to next-generation.

**Dumpster Diving:** This method of identity theft is one of the most traditional—and most effective. Thieves search your trash for documents that contain your personal information and gain access to important numbers that can help them commit identity theft.

**Online Shopping:** Thieves are experts, before you know it, you've completed your transaction online and inadvertently handed over the personal information they need to commit fraud.

**Shoulder Surfing:** The prevalence of cameras and recorders in today's mobile phones make this form of identity theft a real threat. Thieves position themselves within sight or earshot of your latest credit application, and record your information to commit future fraud.

**ATM Skimmers/Handheld Skimmers:** Today's thieves are innovating the way they steal your personal information, by swiping your cards—literally—when you are in the midst of a legitimate transaction such as paying for dinner bill at a restaurant, gas pumping stations, grocery, departments stores and other outlets.


**Overlays:** Hidden devices can be installed almost imperceptibly on any ATM, enabling thieves to swipe your account information when you insert your card, and then transmit your account information to a nearby computer for future fraudulent use.

**Data Breaches:** By the time financial institutions detect that a data breach has occurred, a fraud attempt has already been made without you even knowing that your personal information has been compromised.

**Phishing:** These days, that email from your bank in your inbox could be real—or a phish attempt. Today's thieves are busy impersonating legitimate businesses via email and websites in order to acquire your personal information like PINs, credit card or bank account numbers, and other vital information.

## Next Generation Identity Theft

**Malware, Malicious Software, Viruses, Worms, Trojan Horses, Spyware, and Root kits:** Cyber thieves can install malicious software to exploit weaknesses in features of many popular software titles. Once installed, malware can run executable programs in your computer without your consent, including transmitting personal information via the Internet to remote computers, where it is stored and sold to counterfeiters at a later date.

**Keystroke Logging:** Keystroke logging is one of the most advanced forms of malware criminals use to register your passwords, login IDs, and account information—without you even knowing.

***To be continued…***

-- End of Transmission --

**Information Security:** It's a Shared Responsibility

REFERENCE(S): http://www.lifelock.com