



You're Not Paranoid, They Really Are Watching You!

By: GIDEON J. LENKEY, CISSP

Over the past five years, Identity theft has become a serious problem. The growth of the Internet and its expansion into almost every facet of daily life has resulted in an explosive growth in identity theft. With 214,905 cases filed with the FTC in 2003, and an estimated 500,000 to 700,000 victims a year, identity theft may be the fastest growing white collar crime. By 2006 Meridian Research predicts annual losses of 8 billion dollars in the Financial sector alone.

The number and sophistication of identity theft schemes is increasing. Whether it's a local petty thief or an international organized crime group, they're after your personal information. Because the theft often takes place over an extended period of time before it is noticed, the individual losses can be staggering. These losses go far beyond the direct financial theft. It can take a victim years in some cases to 'clean up' financial reporting data after certain types of identity theft. Even more frightening than the statistics is the fact that so much of your personal private data is stored and handled by computer systems outside of your control, that you may not be able to prevent identity theft from happening to you. At any time, it could just be your turn.

The purpose of this article is not to instruct you how to detect identity theft or recover from it. We'll touch on those subjects, but they're very well documented in other articles and website resources. The focus will be on awareness of the types of identity theft that are preventable and what you can do to protect yourself. I hope that after reading this, you'll be just a bit more cautious and perhaps take some basic precautions. Remember, you're not paranoid, they really are watching you!

The term "Identity Theft" covers a broad range of crimes. In its simplest form identity theft can mean someone stealing your credit card and using it to purchase goods or services. More complicated forms include using your social security number to open credit accounts, obtain loans and purchase expensive items such as automobiles in your name. In cases like this, the thief often has the

correspondence sent to a mailing address they control. Sometimes a thief will have the billing address changed on an existing stolen credit card or bank account so the statements do not reach the victim. This will give them more time to exploit the asset before it is discovered and the account deactivated.

In some cases, a stolen social security number is used to gain employment. If an individual is under a court order garnishing wages, providing a stolen social security number can offer a way to avoid paying it. Additionally, some criminals will use an alternate stolen identity in the event they are arrested. They are often released on bail based on the victims good credit and clean criminal record. When they do not show up for their court date, the judge issues a warrant and the police arrest the victim. Identity information for these purposes can be purchased or traded for in a sort of underground black market.

Stealing someones wallet or purse is an age old way to separate them from their money. Typically a thief will quickly try to reach the credit limit on a card before the theft is noticed and reported. Unfortunately, many people carry far more information with them than they need to. In addition to a driver's license and credit cards, it's not uncommon for people to carry their social security card, various ID cards with their home address printed on them and a spare 'emergency' check. Putting it all together you get, name, address, social security number, bank account number and driver's license number. The worst part of this is that none of it has to actually be stolen to effectively steal your identity. Simply copying the information is enough. If the thief is practiced, you won't know you've been victimized for some time.

This information can also be collected in bits and pieces from your home trash, recyclables or mail. Tax returns provide everything an identity thief needs in one package. By copying the information and re-mailing the return, the victim is unaware of the crime until much later when the credit damage becomes noticeable. Discarded credit card receipts sometimes have the entire card number printed on them. A thief who finds a receipt in someone's trash is likely to find the person's full name and address as well. Bank account numbers can be collected by stealing outgoing mail right from the mailbox. By stealing a payment from the mail the thief gets the full name and address, the checking account information and a sample signature. This information can be used to forge checks from the bank account. Although banks won't give an account balance over the phone without some sort of authentication, if the thief claims to be the recipient of a check, they will indicate if the account has enough funds to cover the (stated) amount on the check. This gives the thief an idea of how much money is in the account. Some thieves simply remove the ink from the check using a chemical process and make the check payable to whoever they want and whatever amount they want.

Corporations and institutions that store large quantities of personal private information are prime targets for identity thieves. This data can be stolen in the simplest of ways such as manually recording the information from a computer terminal screen on paper or with a camera phone. One case in recent memory involved a bank teller who, between transactions at the drive-up window, would pull up personal and account

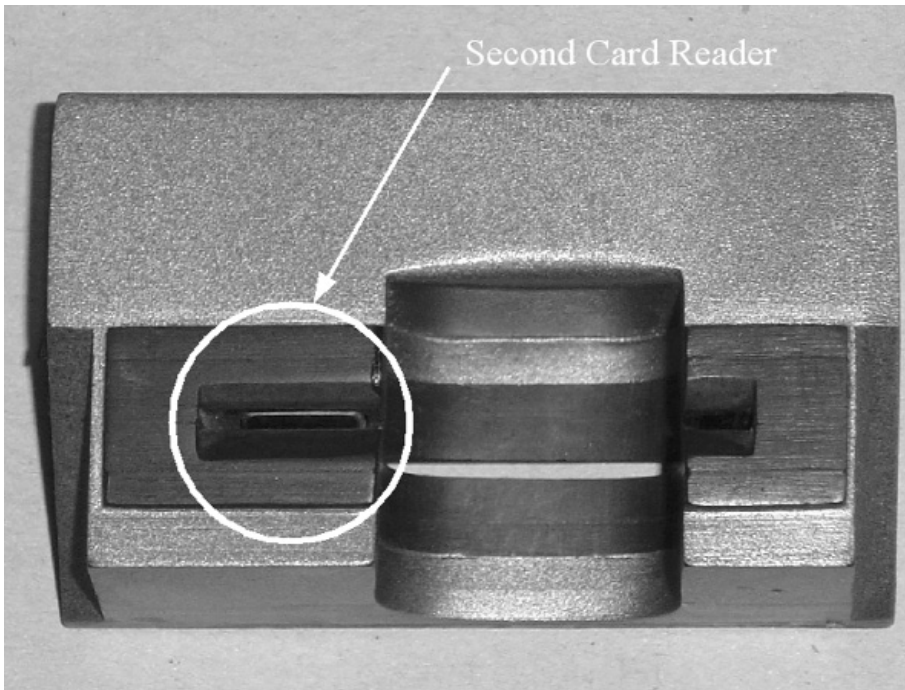


information on her computer terminal, write it down and then pass it to her accomplice through the drive-up widow. The bank was unaware of this activity until federal agents arrived to 'enlighten' them. In this instance it's a perfect intersection of a relatively low paying job with a high value and portable asset (identity). On the other end of the spectrum is a case involving two Russian programmers who had collected over ten thousand credit cards by breaking into banks and Internet ISPs and stealing the data. They then wrote a program that put up phony auctions on ebay, bid on and won the auctions and then paid for the merchandise through Paypal fifteen and twenty dollars at a time. Automated money laundering in essence. The cash amounts were so small that often the card holder wasn't suspicious. The number of cards meant that even with small individual transaction amounts they were capable of generating more than \$150,000 per iteration through the card database. Not bad considering that at the time, the average annual income of a college educated Russian in St. Petersburg was \$600 (USD) per month. They were offered 'hacking' jobs in the US by a security company that turned out to be the FBI. Both were successfully prosecuted.

Internet websites and email offer a tempting "numbers" game for identity thieves. Who hasn't received an email that said "your credit card has been denied, please follow this link" or "we're updating our records....". Of course it only looks like the legitimate site and really just steals your information, but some people will fall for it. It costs the thieves as much to send out a million emails as it does to send out one, so they only need a small percentage of responses to be successful. In other cases, vulnerable browser software allows websites to perform operations directly on your computers data. I recall a demonstration by a German 'hacker' group called the Chaos Computer Club. When you visited their website using the Microsoft IE browser and had Quicken installed on your system, their site would display your account information back to you. This worked whether your quicken file had a password on it or not. A personal computer can be a treasure trove of personal private financial information.

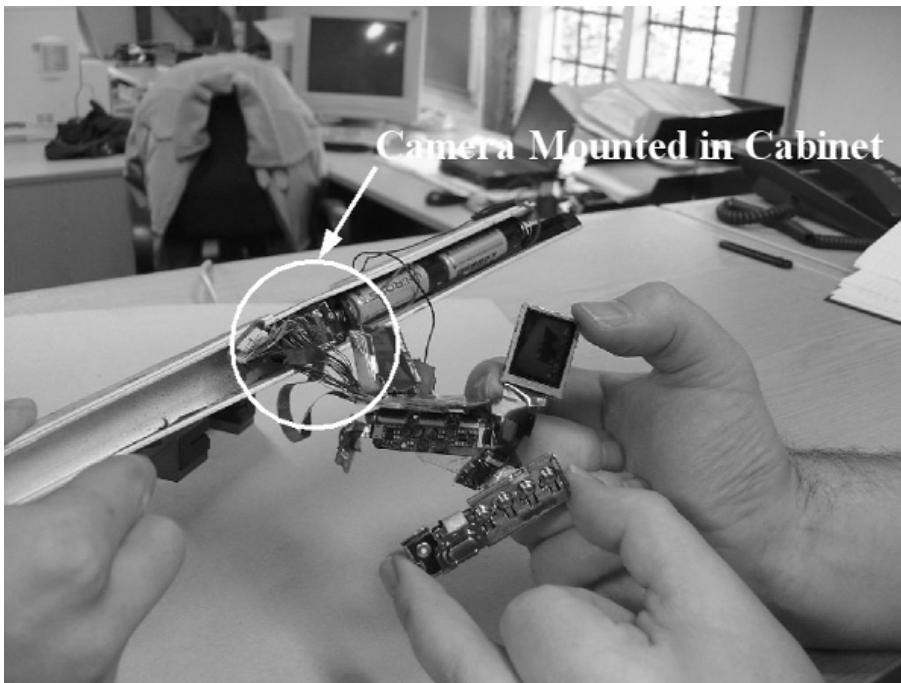
Another popular identity theft activity involves card skimming. This is where the thief takes your card information at the point of use. This can be as simple as a waiter copying the information off the card while the transaction processes or more complex such as a card reader that records the information into a database. There was one incident several years ago where a department store clerk had a card reader attached to a Palm Pilot PDA. Every time she would process a credit card transaction, she would swipe the card twice. Once through the cash register and once through her card reader. This double swipe was noticed by an alert customer and reported. Because it was the holiday shopping season, she had a considerable number of cards .

Illustration 1



The latest and most interesting front on the identity theft war is the privately owned ATM machine. In some cases the ATM machine you use may actually be owned by an organized criminal group. The machines can be modified to record your information while you're using it. These modifications can be remarkable low tech. Illustration 1 one shows the plastic fascia plate of an ATM card slot modified to hold a second battery powered card reader that simply stores a list of card numbers. The pin numbers for the cards are gathered by a digital camera (Illustration 2) that has been disassembled and installed into the plastic cabinet above the keypad (NOTE: Photos courtesy of <http://atm.ev6.net>. The author has not confirmed the authenticity of the photos but has no reason to doubt them). The card numbers from the reader and the pin numbers from the camera are manually correlated using timestamps. This is a simple but effective identity theft.

Illustration 2



Although not all Identity theft is preventable, there are things you can do to limit your risks:

- Remove yourself from unsolicited credit offers by exercising your opt out rights with credit reporting agencies.
- Minimize the information you carry with you.
- Don't carry your social security card.
- Carry only the credit cards you need not all of them.
- Do not routinely carry checks.
- Do not write your PIN or social security number on anything you carry.
- Purchase a cross cut shredder and shred materials containing personal information before you put it in the trash.
- Don't use an unfamiliar ATM machine. If you must, use one in a bank lobby.
- If you keep financial information on your personal computer, learn to use encryption software such as PGP to protect your information.
- Consider keeping your financial information on a separate computer that you don't connect to the Internet.
- Get a lock for your mailbox.
- Don't mail your bills from your home mailbox.
- Never mail your tax return from your home mailbox, use a post office mailbox.
- Never use a debit card for on-line purchases. Use a credit card instead. Your liability with a credit card is \$50. It can be much higher with a debit card if you don't notice the theft right away.
- Do not use a phone to access your financial information in public, especially from a payphone. Wait until you have privacy.
- Keep track of when you receive bills and watch for missing bills and statements.
- Always reconcile your checking and credit accounts.
- Check your credit report at least once per year.
- Many banks will email you a daily balance, you might notice a large drop this way.
- When traveling, carry a decoy wallet or purse while keeping your actual wallet or purse hidden. The thieves are smart too, so carry some cash in it so you don't have to reveal your real wallet or purse before you arrive at your destination.
- Keep all personal private information on removable media such as a biometric thumb drive. This storage device requires a finger print to access the information stored on it and it fits in your pocket or on your key chain.
(www.thumbdrive.com/prd_info.htm)

It is important to report identity theft as soon as you discover or even suspect it. In a very recent case, the victim felt uneasy about the checkout process while buying computer equipment on the Internet with a debit card. He checked his bank balance several times a day and within a week a large unauthorized purchase was made. Because he noticed and reported it quickly, he had no liability. The bank immediately reversed the transaction.

Although some circumstances are beyond your control, you are ultimately responsible for your own personal information security posture. It may seem overwhelming at first but through awareness you can develop good personal information security practices and habits. Over time these habits can significantly reduce the risk of preventable identity theft.

Gideon J. Lenkey is president and co-founder of Ra Security Systems Inc., a New Jersey based information security consulting and managed services company. He holds a CISSP certification from the ISC2 and has over 12 years of experience in the field. Gideon is a member of the High Technology Crimes Investigation Association (HTCIA), the Computer Security Institute and the New Jersey chapter of the FBI's InfraGard program where he is currently the President. Gideon can be reached at glenkey@rasecurity.com.