Information Security Newsletter Series: Identity Theft

Identity theft, the fastest growing non-violent crime in America, occurs when someone steals another person's personal information—name, social security number, credit card numbers, and so on—and uses it to commit fraud. Identity thieves use this information to open credit card accounts in your name, take out loans, buy cars, establish wireless service, and more—all at no expense to the thief. A person has his or her identity stolen about once every 60 seconds. The information needed to steal a person's identity is acquired by stealing a wallet or mail, rummaging through trash to acquire old credit card or bank statements, or even posing as a landlord or employer to obtain a credit report.

Now that we understand what identity theft is and how it can occur, we can start to think about prevention. There are concrete measures you can take to greatly reduce the risk of becoming one of the 900,000 new victims of identity theft:

1. Use strong passwords for your credit card, bank and phone accounts: Avoid easily guessed passwords such as you Mother's maiden name, a birthday, your address, etc. You can view the Passwords Newsletter for more suggestions.
2. Secure personal information in your home, especially if you live with a roommate.
3. Stay up to date on information security procedures within your workplace.
4. Never give out personal information over the phone, mail, or Internet unless you have initiated contact with that person.
5. Protect information in your mail and trash by shredding credit card applications, bank statements, and anything else that could be used to steal your identity.
6. Carry your Social Security, credit, and bank cards only when necessary. Otherwise, leave them in a secured place.
7. Check your billing statements to look for purchases that you have not made.
8. Periodically check your credit report and rating to look for any malicious activity. Some signs to look for include:
   - Inquiries of your credit report: This will often include requests for credit from employers, collection agencies, or someone else with a legal right to check your credit report.
   - Incorrect address: Thieves will often change billing addresses of accounts you may have and forgotten about. All unused accounts should be closed as soon as possible in all cases.
   - Unexpected public record: This shows court judgments, liens, foreclosures, and other public records. Look for occurrences that you are unaware of or are not yours.
   - Unexpected derogatory information: Look for unexpected past-due items.

If you suspect that you have become a victim of identity theft, you should contact the fraud departments of each of the three major credit bureaus (www. Equifax.com, www.Experian.com, and www.transunion.com), file a police report both with your local police or the police in the community where the identity theft occurred, and close the accounts that you know or believe have been tampered with or opened fraudulently. Your personal information is irreplaceable. By taking the steps mentioned you will have better peace of mind about who is spending your money and using your good name.