

Identity Theft: The New Technology Crime

Robert Ing, DSc, DLit, FAPSc

Full Article Available at www.drroberting.com
Copyright 2004, 2005 Dr. Robert Ing, Toronto, Canada. All rights reserved.

Identity Theft in the Western World has increased dramatically since the beginning of the millennium and has replaced credit card fraud as the new number one technology crime.

What It Is.

Identity Theft is when someone steals (uses) someone else's identity for the purpose of personal or financial gain, or in order to support the commission of a criminal act.

Specific Examples.

Specific examples of identity theft involve the perpetrator posing as someone else to obtain credit, to hide from the authorities or others, to conceal a criminal past, to obtain access under an assumed identity to an otherwise "off limits" facility, or to cross a border. The ideal identity for most seeking a new one, is that of an average working citizen; one with a fairly ordinary life that will enable the perpetrator to blend in easily.

In the past, before the prevalence of computer databases and the Internet, most identity thieves would use the identities of the deceased by taking names and dates of birth from grave markers. The next step would be to obtain family information, such as the names of parents and family members under the guise of doing family history research. Once this information was acquired, a request for copies of the birth certificate and other personal identification documents would be made and used to impersonate the deceased. However, with the computer cross-referencing of birth, death and other personal identification records by government agencies this method is seldom used.

The current methods employed by identity thieves is to obtain personal information from stolen or "cracked" government and corporate computer databases and from publicly available or low level restricted access sources such as credit bureaus, public records services, online resume databases, genealogical databases and personal web pages. Depending on the purpose for the stolen identity, the depth of information required on the target individual will vary. For instance, someone interested in obtaining credit in the name of the target may only require a credit report or social insurance number, date of birth and resume. A terrorist interested in crossing a border or gaining access to a high security facility would require more of the target's personal information in order to obtain copies of the official documents required. An individual interested in assuming the identity of another for a year or more would no doubt obtain as much personal information as possible such as the high school attended, names of relatives and pets, and even take up the sports and hobbies of their target.

Regardless of the motive, an identity theft usually centers around the use of either copies and newly issued personal identification documents or altered and forged documents made to appear like officially issued original documents. While the Western world possesses the technology to cross-reference and validate most legitimately issued government documents, other countries are not as advanced or vigilant. The result is that people with altered, forged and duplicate copies of official documents have a 3 out of 10 chance of passing these questionable documents and themselves as the genuine article.

Once a person's identity is stolen, it takes an average of 18 months after the fact before the crime is discovered. This is largely due to the fact that the identity thief while using another's identity will attempt to maintain a low profile. Also, the public is generally unaware of the discrete signs of

identity theft and despite the role of technology in society the ability to positively identify individuals is not cost efficient, practical or socially acceptable. As a matter of fact, in 8 out of 10 identity theft cases worldwide, the perpetrator is first arrested on a different criminal charge where upon further investigation it is discovered that the individual is not who they claim to be. In essence, the stolen identity was used as an aid in order to perpetrate a more profitable crime.

Tell Tale Signs That Your Identity Has Been Stolen

1. You apply for a loan or other form of credit and are turned down, yet you know your credit is good.
2. You receive telephone calls or mail personally addressed to you from financial, retail or collection agencies that you have never done business with at your home or office.
3. Balances on credit card statements or bank accounts are inaccurate.
4. Expected items containing personal information that are to be mailed to you become lost or unreasonably delayed in the mail.

Reduce The Risk of Someone Stealing Your Identity

1. Report any lost or stolen identification immediately to the issuer and the authorities.
2. Make photocopies of the back and front of all identification, keep it a safe place and use it as a reference when you have to report lost or stolen items. If going on vacation, leave this record with a relative at home, so that if your identification is stolen, you have someone who can report all the details on your behalf.
3. Never give out key identification information to people or companies you do not know, or post them on your personal web site. Key information in obtaining identification includes date of birth, mother's maiden name, names of both parents, your high school, current employer, social insurance or social security number, city of birth, your bank, credit card numbers, driver's license number, or license plate number. If a professional identity thief has any two of these items it is a relatively easy task to obtain further information on you, obtain or forge identification documents and steal your identity.
4. Check your credit report on an annual basis or before you apply for financing for a major item such as a new home or car. If you see loans and credit cards on your report that you have never applied for, this is a tip off that your identity has been stolen, report these immediately to the authorities, credit grantors and credit bureau.
5. When throwing out any documents that have personal information on them, shred them first. This includes old credit card and bank statements, resumes and similar documents. Some identity thieves will stop at nothing to obtain an identity and going through garbage, also known as dumpster diving, is how many criminals get your personal information.
6. Always check credit card and bank statements for unauthorized transactions. Report these immediately to your financial institution.

About the Author

Dr. Robert Ing is a forensic intelligence and technology crime specialist. He may be reached at 416-563-6958, or via e-mail at Ring549@aol.com, www.drroberting.com