Who Are You? How to Protect Against Identity Theft

Identity theft has become one of the most lucrative criminal endeavors, with over half a million cases reported in the United States resulting in annual losses in the billions of dollars. Facilitated by the voluminous information available on the Internet to those who know where to look, the reported incidents of identity theft have grown at an unprecedented rate. Unfortunately, while the victims of identity theft may spend years attempting to clear their credit histories and criminal records, this crime is rarely prosecuted. While numerous laws have been enacted in an attempt by the United States government to address the issue of identity theft, the best protection available to consumers is constant vigilance.

With more than 100 million Americans connected to the Internet [1], information security has become a top priority. Many applications – electronic mail, electronic banking, medical databases, and electronic commerce – require the exchange of private information. As an example, when engaging in electronic commerce, customers provide credit card numbers when purchasing products. Identity theft, the fastest growing type of fraud, affected 500 000 Americans in 2001, resulting in over $2 billion in losses at an average cost of $17 000 per victim of which roughly $1500 is required just to repair the damage to a victim's credit report. From January through September of 2003, nearly ten million Americans were identified as victims of identity fraud, resulting in over $5 billion in victim out-of-pocket losses and $48 billion in losses to businesses and financial institutions according to a Federal Trade Commission report [2]-[8], [15], [18], [20]. Through the use of email address hiding, the Internet has enabled identity thieves to flourish, increasing the scale of this type of fraud by a factor of up to 50 when compared to more traditional types of fraud [2], [4], [5], [8], [9]. Moreover, identity fraud is a criminal activity that typically goes un-prosecuted and under-punished. According to a Gartner study, identity thieves have only a 1 in 700 chance of being either exposed or arrested [3].

Identity theft is the assumption of another person's financial identity through the use of the victim's identifying information. This information includes a person's name, address, date of birth, social security number, credit card numbers, and checking account information. With this information, a thief is capable of charging merchandise to the victim's account and changing the billing address for the account so that the unauthorized purchases remain undetected.

Identity theft opens the door to other crimes, such as gaining access to welfare and social security benefits, ordering new checks to a new address, obtaining new credit cards, obtaining the victim's paycheck, taking out loans in the victim's name, and using the victim's name upon arrest [2], [3], [5]-[7], [9], [10], [15], [17]-[20]. The most common forms of identity theft involve credit card usage and social security numbers. According to Garner, 70% of credit card related cases of identity theft involve insiders [3], [6], [8]. Social security numbers also pose a significant problem in that they are overused as customer account numbers and employee numbers, giving a thief a “master key” into an individual's digital identity [2]-[4], [6], [9].

Adam J. Elbirt is an Assistant Professor and the Director of the Information Security Laboratory in the Electrical and Computer Engineering Department at the University of Massachusetts Lowell, Lowell, MA. He is also the Associate Director of the Center for Network and Information Security (CNIS); email: Adam_Elbirt@uml.edu.

Tactics

Identity thieves are extremely resourceful in their efforts to obtain personal information about their victims. Dumpster diving, i.e., searching someone's garbage, and mail theft are commonly used to obtain credit card numbers and bank account numbers from discarded statements. Pre-approved credit card offers are also frequent targets of thieves intent upon establishing a line of credit based on false credentials [2]-[6]. Basic theft of electronic equipment such as laptops and personal digital assistants may yield significant amounts of personal information. Moreover, thieves often pose as legitimate account managers for credit card companies and financial institutions and ask for personal information under the guise of account verification or maintenance [2], [3]. Even worse, an identity thief may legally obtain much of the necessary personal information for perpetrating identity fraud by using public information sources. Examples of these types of sources include on-line data resellers and information brokers that provide background information on an individual for a small fee [2], [3], [10].

Additional options abound for computer savvy identity thieves. Much like Trojan horse programs and Internet worms, it is possible for an attacker to place a file on a user's computer to track their actions, intercept electronic communications, and snoop through files to gain the desired information. Even more aggressive strategies include [2]:

- Creating fake e-commerce sites with desirable products at cheap prices to lure customers into providing detailed personal information.
- Gaining unauthorized access to on-line systems and placing programs on servers to allow unauthorized persons to access the system.
- Publicly posting fake product sales information to Usenet forums with links to web pages asking for more detailed personal information.

From January through September of 2003, nearly ten million Americans were identified as victims of identity fraud

Laws Designed to Protect Consumers

A number of laws have been enacted in an effort to protect consumer information privacy and deter identity theft. The Health Insurance Portability and Accountability Act (HIPPA) was passed in 1996 and attempted to address the confidentiality of patient information by forbidding the divulgence of individually identifiable health-care information without patient authorization or prior consent. HIPPA covered health-care information obtained both electronically and orally, requiring health-care providers to protect both the confidentiality and integrity of patient information. HIPPA also requires health-care providers to supply patients with a notice of their privacy rights and the privacy practices of the provider. Finally, HIPPA states that health-care providers must safeguard against unauthorized use and disclosure of patient information and these providers must obtain a patient's written authorization in advance if the provider is to use protected health-care information for most purposes not related to treatment or payment. Note that exceptions to this requirement exist for certain public health purposes, law enforcement, and other public purposes [11].

The Identity Theft and Assumption Deterrence Act, passed in 1998, addresses the use of another person's identification information without lawful authority. This law classifies identity theft as a felony violation at the state or local level (whichever is determined to be more appropriate) if the theft results in further activities that violate federal law [6], [10].

The Gramm-Leach-Blily Act of 1999 targets the protection of private consumer information by financial institutions. The law classifies the obtaining of private consumer information via fraudulent means as a federal crime. This law includes fictitious statements made to all employees, officers, or agents of the financial institution or those statements made to customers in an attempt to obtain the desired information. The law also details the obligations that financial institutions have to consumers to guarantee the security and confidentiality of customer records against unauthorized access and use in addition to other likely threats against the non-public personal information that these institutions collect from their clients. Moreover, the law specifically enables states to enact and enforce laws that are tougher than the Gramm-Leach-Blily Act [3], [4], [10], [11], [16].

Legislation enacted more recently includes the USA PATRIOT Act of 2001 and the Consumer Privacy Protection Act of 2002. Unlike previously established laws that protect an individual's private information, the USA PATRIOT Act requires financial institutions to maintain records for reporting purposes to aid in identifying money laundering activities as part of the fight against terrorism [11]. In 2002, the Consumer Privacy Protection Act was established to place requirements on data-collection organizations in regards to collection and sale of private information as well as to detail solutions for instances of identity fraud [9].

Two other proposed pieces of U.S. legislation are currently under debate. The Fair and Accurate Credit Transactions Act was proposed in 2003 to enable consumers to obtain one free copy of their credit report each year. This proposed law would also bar merchants from printing all of the numbers of a credit card on receipts in addition to requiring credit card

companies to put an automatic fraud alert on all credit files that are considered to be at risk of fraudulent activity [9]. The Social Security Misuse Prevention Act, also proposed in 2003, would require individual consent to allow organizations to sell or display social security numbers on their documentation. This proposed law would also forbid the United States government from displaying an individual's social security number on public records that are either posted to the Internet or distributed to the public via electronic means. Finally, this proposed law would put strict limits upon businesses as to when it would be permissible to require that their customers provide social security numbers [9], [14].

Guarding Against Identity Theft

When attempting to minimize the opportunities for identity theft, it is imperative to guard our personal information. This information includes but is not limited to our social security number, maiden name (yours and your mother's), date of birth, past addresses, and driver's license number [2], [4], [6]. To further protect against identity theft, we must remember to be both proactive in our defense efforts and constantly aware of how identity thieves obtain the information they need to be successful. To that end, contact your insurance agent to discuss the purchase of identity theft insurance and be sure to support legislation designed to protect your personal information. In addition, there are a number of measures that any of us can implement to impede the efforts of an identity thief [2]-[4], [6], [8], [9], [12], [13], [18], [19].

Information Confidentiality

Maintaining information confidentiality is the first step in thwarting the efforts of identity thieves. To that end, exercising basic commons sense when dealing with sensitive information will serve to mitigate much of the associated risk. Secluding yourself when transmitting vital information via telephone and submitting written requests to organizations that you do business with to not share your personal information with other organizations during unrelated transactions are key steps in minimizing the opportunities for identity theft. Immediately report lost or stolen credit cards, bank cards, and telephone calling cards. Check your creditors' policies for stolen cards and fraudulently accessed accounts to determine your liability. As previously noted, social security numbers are commonly targeted by identity thieves due to their overuse as customer account numbers for organizations such as banks, credit card companies, and hospitals [2]-[4], [6], [9], [18]. As a result, it is critical that you do not carry your social security card in your wallet or purse and that you do not give out your social security number unless it is absolutely necessary and you have initiated the contact with the organization in question. You must also remove your social security number from your driver's license and your checks. Finally, contact any organization that you do business with and ask them to change your identification number to a randomly generated number in place of your social security number.

Information Tracking

Continuous monitoring of high risk targets is the next phase in guarding against identity theft. This includes regularly requests for copies of your credit report and constant attention to the billing cycles of your existing credit cards telephone, cable, Internet, and other bills for unexpected increases in charges. Call the issuer of your credit card if your bill is noticeably late, keep track of what you buy, and check your credit card bill for unusual purchases. Subscribe to your credit bureaus' regular and automatic notification of unusual credit account activity. Check your W-2 tax statements for unexpected extra earnings that would indicate that someone is working under your name. Finally, do not assume that your mail is safe. Safeguard your incoming and outgoing mail by mailing bills and other personal documents at a post office or via a post office box instead of from home. Place change of address cards in an envelope before sending them to the appropriate Postmaster.

Information Storage

How and where information is stored significantly impacts the ability of an identity thief to succeed. Store passports, birth certificates, wedding certificates, stocks, social security cards, and savings account books in locked vaults. Keep a written record of the contents of your wallet or purse in a locked vault. Protect personal information stored on your computer with firewalls and passwords. Only use encrypted web sites that have a posted privacy policy. Choose passwords that make sense to you but are not obvious choices for an identity thief to try when attempting to pose as you. Passwords such as birth dates, anniversary dates, names for pets, and maiden names are examples of bad passwords. Finally, be sure to change your passwords often to minimize the damage should one or more become compromised.

Information Disposal

To prevent dumpster diving, shred all personal documents, pre-approved credit card solicitations, old bank statements, credit card charge slips, and old credit card statements before putting them in the trash. If possible, use a cross-shredder to further obfuscate the contents of these types of documents. Cancel and cut up unused or expired credit cards, bank cards, and telephone calling cards.

Recovering From Identity Theft

Unfortunately, even the most prepared of us may still become the victim of identity theft. According to most analysts, recovering from identity theft requires an average of almost 200 hours worth of effort expended in contacting creditors, financial institutions, and law enforcement officials. Should you find yourself a victim of identity theft, a number of organizations are available to assist you in your efforts to minimize the impact of the fraudulent act [2], [3], [6], [9], [15], [16], [18], [19]:

- Privacy Rights Clearinghouse, 619-298-3396, http://www.privacyrights.org or http://www.ssa.gov.
- United States Public Interest Research Group, 202-546-9707, http://www.pirg.org.
- National Association of Consumer Advocates, http://www.naca.net/resource.htm.
- The Education Department, http://www.ed.gov/misused.
- Federal Trade Commission, 877-438-4338 or 877-IDTHEFT, http://www.ftc.gov or http://www.consumer.gov/idtheft.com.
- Federal Bureau of Investigation, http://www.fbi.gov.
- U.S. Postal Inspection service, http://www.usps.com/postalinspectors.
- U.S. Department of Justice identity theft and fraud information, http://www.usdoj.gov/criminal/fraud/idtheft.html.
- Identity Theft Prevention and Survival, http://www.identitytheft.org.
- Identity Theft Resource Center, http://www.idtheftcenter.org.
- Internet Fraud Complaint Center, http:// ifccfbi.gov.
- Contact the fraud department of your credit card companies to request that fraud alerts be placed on your accounts. The three major credit bureaus are:
  - Experian, 888-397-3742, http://www.experian.com.
  - TransUnion, 800-680-7289 or 800-888-4213, http://www.transunion.com.
  - Equifax, 800-685-1111 or 800-525-6285, http://www.equifax.com.
- Submit a written request to all of the appropriate credit bureaus to have long-term fraud alerts placed on your accounts.

In addition to contacting these organizations, be sure to contact local police, file a report, and obtain an affidavit of fraud and a copy of the police report so that you can give copies of these documents to creditors as proof that you have been a victim of identity theft [2], [3], [9].

Constant Vigilance

The ruthless tactics employed by identity thieves demand our constant vigilance if we are to preserve our credit histories and maintain clean criminal records. While current and pending legislation will continue to assist us in these endeavors, we must also engage in a proactive approach to managing our identities. The recommendations for guarding against identity theft must be integrated into our daily lives to further frustrate the fraudulent efforts of identity thieves. While nothing can guarantee invulnerability to identity theft, savvy consumers can put themselves in the safest possible position to avoid and, if necessary, quickly recover from the damage wrought by this type of fraudulent activity.

References

[1] "The Nielsen NetRatings Reporter." World Wide Web, June 20 1999. http://www.nielsen-netratings.com/weekly.html.

[2] S.E. Arnold, "Internet users at risk: The identity/privacy target zone," *Searcher,* vol. 9, pp. 24-39, Jan. 2001.

[3] L. Bielski, "Identity theft," *ABA Banking J.*, vol. 93, pp. 27-30, Jan. 2001.

[4] J. Bigham Bernstel, "Identity crisis," *Bank Marketing,* vol. 33, pp. 16-20, Jan. 2001.

[5] P. Fichtman, "Preventing credit card fraud and identity theft: A primer for online merchants," *Information Systems Security*, vol. 10, pp. 52-59, Nov.-Dec. 2001.

[6] S. Groves, "Protecting your identity," *Information Management J.*, vol. 36, pp. 27-31, May-June 2002.

[7] O. O'Sullivan, "Who's that knocking on my portal?," *US Banker,* vol. 109, pp. 49-52, Nov. 1999.

[8] I. Schneider, "Intruder alert," *Bank Systems & Technology,* vol. 39, pp. 24-26, 28, 46, July 2002.

[9] D.A. Riordan and M.P. Riordan, "Who has your numbers?" *Strategic Finance*, vol. 84, pp. 22-26, Apr. 2003.

[10] E.H. Freeman, "Pretexting, data mining and personal privacy: The Gramm-Leach-Bliley Act," *Information Systems Security*, vol. 11, pp. 4-8, May-June 2002.

[11] F. Scholl and J. Hollander, "The changing privacy and security landscape," *Business Communications Rev.*, vol. 33, pp. 54-57, May 2003.

[12] R. Stuhlmuller, "User identity: The key to safe authentication," *Communications News,* vol. 37, pp. 32-38, Mar. 2000.

[13] G.V. Hulme, "Slow acceptance for biometrics," *InformationWEEK,* pp. 56-62, Feb. 10, 2003.

[14] *Social Security Number Misuse Prevention Act,* Bill Summary and Status for the 107th Congress, available at http://thomas.loc.gov/cgi-bin/bdquery/z?d107:SN00848:@@@L&summ2=m&.

[15] J.R. Marbaix, "Lessons in privacy," *U.S. News & World Report,* vol. 137, no. 7, pp. 74-75, Sept. 6, 2004.

[16] "Educating students about identity theft," *Recruitment & Retention in Higher Education,* vol. 18, no. 9, pp. 5-6, Sept. 2004.

[17] D. Graham-Rowe, "Internet fuels boom in ID theft," *New Scientist,* vol. 181, no. 2438, pp. 24, Mar. 13, 2004.

[18] J. Rubenking, S. Carroll, and N.J. Rubenking, "Identity theft: What, me worry?" *PC Magazine,* vol. 23, no. 4, pp. 75-77, Mar. 2, 2004.

[19] "Identifying ways to combat identity theft," *Perspective,* vol. 19, no. 2, pp. 1-2, Feb. 2004.

[20] K. Davis and A. Stevenson, "They've Got Your Numbers," *Kiplinger's Personal Finance,* vol. 58, no. 1, pp. 72-76, Jan. 2004.