Mitigation of Identity Theft in the Information Age

Reggie Becker
Emerson Electric, USA

Mark B. Schmidt
St. Cloud State University, USA

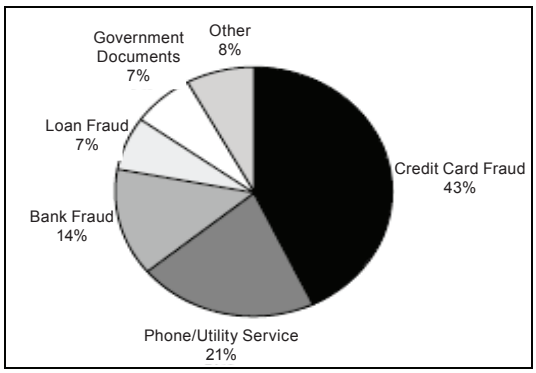
Allen C. Johnston
University of Louisana Monroe, USA

INTRODUCTION

The information age is characterized by unprecedented levels of information sharing, connectivity, and convenience. Along with the expediency afforded us by electronic commerce (e-commerce), online banking, e-mail reminders, and electronic government (e-government) services comes a degree of dependence on the information technology that drives these processes. Moreover, these processes are inherently insecure, thereby generating an unparalleled level of concern for computer security and identity theft, in particular. This article will discuss identity theft techniques and describe how readers can avoid it.

A familiar problem faced by numerous Americans each year, identity theft can be defined as "a situation where someone assumes the identity of another and makes telephone calls or obtains merchandise, credit, or other valuable things in their name" (Swartz, 2003, p. 17). The Federal Trade Commission estimates that each year 3.2 million American citizens have their identities stolen; equating to roughly one theft every ten seconds (IMJ Staff, 2005a). Prior to the emergence of today's highly interconnected world, identity thieves would employ a variety of techniques to obtain the personal information of their potential victims. These methods included such acts as dumpster diving, phone inquisitions, and social engineering.[1] While simplistic, these techniques were nonetheless effective. Today, however, we face a new type of criminal. This new criminal is more sophisticated than previous identity thieves and leverages the Internet to facilitate theft. For instance, today's criminals may design Web pages that compel users to offer personal information without thinking twice about it. Figure 1 depicts the common types of identity theft.

Figure 1. Sources of identity theft (adopted from Bidwell, 2002)



BACKGROUND

During the 1990s, the phenomenal growth of the Internet spurred a flurry of online consumer and business activity, and indirectly produced an influx of online identity theft and other forgeries. In fact, between 1990 and 2003, 33.4 million Americans reported themselves as victims of identity theft or fraud, with more than 13 million having fallen victim after January 2001 (Swartz, 2003). Additionally, based on information obtained in a 2003 Federal Trade Commission (FTC) survey, more than 10 million people had experienced identity theft in one from or another over the course of one year (Moye, 2006). These surveys give some indication of the reach of identity theft and the prolific nature of the problem.

Indeed, identity theft is not an isolated phenomenon. Figure 2 presents a list of the top ten states in terms of identity theft. As is evident by this figure, identity theft does not discriminate on the basis of geography, race, sex, or social standing. It is likely that if someone

Figure 2. Top ten states for ID theft (adapted from U.S. Ways and Means Committee, 2004)

Top Ten States for ID Theft Occurrences		
State	**Victims per 100,000 People**	**Number of Victims**
Arizona	122.4	6,832
Nevada	113.4	2,541
California	111.2	39,452
Texas	93.3	20,634
Florida	83.0	14,119
New York	82.4	15,821
Oregon	81.7	2,909
Colorado	81.3	3,698
Illinois	77.4	9,792
Washington	77.3	4,741

has not been victimized, they know someone that has. Moreover, the problem is likely to only worsen as more and more Americans become reliant on the Internet and technology to function effectively and efficiently within our information-based society.

Identity theft awareness and protection are clearly needed in the United States. The dissemination of information to various organizations and individuals is far too relaxed, with few controls regulating the manner in which information is collected, stored, transferred, and shared by people in many different fields. As American society becomes more and more dependent on the Internet and its complimentary technology, the need for the adequate and appropriate protection of these processes becomes even greater. Certainly, thieves will continue to evolve in terms of resourcefulness and they will increase their risk propensity in effort to obtain personal information. However, if protection is addressed on an individual level, business level, and government level, the thieves' road to success becomes more difficult. In the open market of the information age and the Internet, it is difficult to prevent identity thieves from contacting and soliciting potential victims. Awareness is a logical method by which to prevent thieves from stealing people's identities and financials, and in many cases is the first step in defense (GAO, 1998; Goodhue & Straub, 1989; Im & Baskerville, 2005; Rhee, Ryu, & Kim, 2005; Siponen, 2000; Straub & Welke, 1998).

ACTIONS FOR PROTECTION

Individual

An individual can play a major role in his or her identity defense. While there is no fool-proof defense, there are a few things he or she can do to reduce the odds of becoming a victim. Typical advice includes checking URLs for the correct spelling and ensuring the padlock icon is displayed in the corner of the Internet browser (Knight, 2005). Unfortunately, most people who use the Internet on a regular basis do not follow this advice. Another action for protection is the obtainment of a free credit report. Everyone is entitled to one free credit report per year. An individual should, therefore, obtain a credit report at least this often to monitor accounts for any suspicious activity. Most people do not know that they are entitled to a free credit report, and even less use the service (Swartz, 2005). Therefore the free credit check is not being used to its full potential.

Security or credit freezes are another identity protection option. When an identity is threatened through security breaches, credit reports should be locked. If someone tries to open an account, additional identity checks will be needed to ensure the loan is going to the actual person identified on the credit report. A credit freeze is a valuable tool to allow consumers to control their degree of risk (IMJ Staff, 2005b). If a freeze is affected, credit files cannot be accessed and instant credit, such as retail credit cards or on-the-spot car loans, cannot be issued (IMJ Staff, 2005b).