Chapter 6
Identity Theft and Online Fraud:
What Makes Us Vulnerable to Scam Artists Online?

ABSTRACT

Probably the type of online crime with which most people have direct experience involves attempts at identity theft and fraud. Most individuals have received an email involving an attempt to get them to part with their money. This chapter aims to describe some of the common types of identity theft and fraud which can occur online, as well as attempting to determine what makes us vulnerable to such attacks. To do this, the chapter will examine some aspects of human decision making, as well as identifying the social engineering tactics used by prospective fraudsters. The chapter will describe the known prevalence rates and costs of online identity theft and fraud, and will compare these types of offences to offline fraud schemes. The methods of attack will be described, including phishing, keyloggers, social engineering, advance fee frauds, and other techniques. An attempt will be made to determine what the psychology of the identity thief and fraudster is, based on comparisons to similar offline offenders. In addition to this, the effects on the victim will be considered, including the phenomenon of victim blaming, where others place partial blame on the victim for the criminal event. Possible methods of preventing identity theft and online fraud will be considered, along with potential future trends and research.

BACKGROUND

Sarah regularly uses her credit card online. When purchasing clothes from an online shop, she became distracted, and she failed to notice that the site was not secure. Her credit card details were stolen, and the thief has used her credit card to make payments of over $2,000. Sarah was not aware of her victimization until her credit card was refused after a meal at a restaurant.

DOI: 10.4018/978-1-61350-350-8.ch006

James uses profiles on several social networking websites to stay in touch with friends. The profiles include many personal details about him, including his date of birth, hometown and contact details. On applying for a loan, he discovered that he had a bad credit rating, although he has always paid his credit card, mortgage and bills on time. He runs a credit check, and discovers that a motor loan has been taken out in his name, although he never applied for it. No repayments have been made on the loan. He eventually realizes that he has been the victim of identity theft, and that the

offender used the personal information available on his social networking profile along with other online information about him to apply for the loan.

Definitions and Key Terms

The above scenarios describe how easily individuals can become victims of identity theft. There are other examples of identity theft. In some cases these can be relatively harmless, where an individual leaves their social networking profiles unprotected and a friend or relation has used the opportunity to post embarrassing comments on their profile. This 'impersonation' of the other is not normally performed with criminal intent, but rather is an attempt to play a prank on a friend or family member. That said, there have been cases where celebrities have been impersonated in online social networking websites, with the impostor sometimes portraying them in a negative light. In other identity theft cases individuals might use weak passwords for online activities, which are easy to guess with only limited knowledge of the person (such as their address or date of birth).

Smith (2010) describes identity theft as "one of the most pressing financial crime problems that has faced developed societies in recent years" (p. 273). He indicates that while it is not a new criminal activity, it is facilitated by information technology, which makes it easier to access personal information and to fabricate important identity documents. Several definitions of identity theft have been proposed. For example, McQuade (2006) defines identity theft as "acquiring and then unlawfully using personal and financial account information to acquire goods and services in someone else's name" (p. 69).

Marshall and Stephens (2008) suggest that in order to understand the concept of identity theft, the term 'identity' needs to be sufficiently defined. They suggest that identity, from the point of view of the individual, is "an awareness of one's own existence in the world" (p. 180), which is comprised of a variety of factors including membership of a family, a circle of friends, career, physical traits, behaviour and preferences. However they suggest that from the perspective of another, a person's identity is somewhat simpler, where only recognition of the individual is required in order to confirm identity. Marshall and Stephens relate how this recognition becomes less reliable if the person has never been encountered before. If this happens online, they indicate that it is necessary for the person to present some kind of 'trusted token' to either validate their identity or confirm that they have the authorization to complete the action they are attempting. This may involve a password or special documentation, which lets the system know that it is alright for the person to proceed. As such, Marshall and Stephens argue that identity theft should really be considered 'authority fraud'.

Finch (2003) distinguishes between individual identity (the person's sense of self), social identity (the external view of the person) and legal identity (a set of characteristics that are unique to the individual and provides a way in which people can be differentiated from each other). Finch (2003) indicates that neither individual nor social identity can be stolen, but that legal identity can. She indicates that the birth certificate is the foundation of legal identity, and that whenever legal and individual identity conflict, legal identity prevails. An example of this involves a nickname – it may be part of the person's social and individual identity, but it is not permissible for legal documentation. Legal identity can be verified through production of specific documents or the possession of certain knowledge, and identity theft "involves the misuse of information that is specific to an individual in order to convince others that the imposter is the individual, effectively passing oneself off as someone else" (pp. 89-90).

Finch (2003) indicates that identity theft may be short or long-term. She cites an example of a case where a man had assumed the identity of his deceased flatmate for fifteen years. In other cases, the identity theft may last for only a few