Category: Concepts, Trends, and Challenges

Cyber-Identity Theft

Angeline Grace Close
University of Georgia, USA, North Georgia College and State University, USA, and University of Nevada, Las Vegas, USA

George M. Zinkhan
University of Georgia, USA

R. Zachary Finney
University of South Alabama, USA

INTRODUCTION

Internet technology facilitates "faceless" transactions. At the same time, a new set of risks arises. In this article, we focus on the Internet-related risks associated with identity theft. Specifically, our objectives are to explain electronic-based identity theft (i.e., cyber-identity theft) and to explore the impact of cyber-identity theft on consumers, businesses, organizations and public policies. Our article makes two specific contributions to the identity theft literature: (a) it explains identity theft as it relates to the Internet and (b) it defines key methods of cyber-identity theft.

BACKGROUND

We first present a brief background on this emerging issue. Identity theft is broadly defined as the practice of using the identity of another to obtain credit (Sovern, 2004). Specific to U.S. federal law[1], identity theft is the "unauthorized use of another person's identification with the intent to commit another crime" (U.S. Code, Chapter 47, Title 18). Any individual who violates federal identify law and obtains money or property valued at or over $1,000 over a one year period may be sentenced to up to 15 years in prison.

In extant studies, attention primarily focuses on legal aspects and avenues for future legislation and policy. Linnhoff and Langenderfer (2004) review the Fair and Accurate Credit Transactions Act (FACTA). As the 2003 Act currently stands, most of the financial risk is borne by the victim (Sovern, 2004). Simply stated, identity theft victims bear most of the costs of reestablishing their "good names" after an identity theft. Notably, some purchases made by identity thieves show up on the victim's credit report and may be difficult to remove. Critics claim that, at present, the law provides insufficient incentives for financial institutions to take preventative measures against identity theft (Lee, 2001; Sovern, 2004). Sovern (2004) argues that consumers should stand up to credit bureaus and creditors who fail to delete fraudulent transactions from victims' credit reports.

Identity theft has the potential to wreak havoc on consumers' social and financial lives. At present, U.S. consumers have rather extensive access to public records (e.g., birth certificates, marriage certificates, tax documents), and consumers may be reluctant to sacrifice these rights. For instance, a survey conducted at Washington State University finds that a majority of individuals in the state of Washington support continued individual access to public records (Cuillier, Passey, & Hinz, 2003), despite the presence of identity theft. Similarly, business organizations do not welcome laws concerning their security policies (Knowledge at Wharton, 2005; Lacey & Cuganesan, 2004).

Next, we explore how identity theft relates to the Internet. *Cyber*-identity theft involves the use of electronic (e.g., via the Internet) means to carry out any form of identity theft. Close et al. (2004, p. 48) define cyber-identity theft as "the online or electronic acquisition of personal information with the purpose of utilizing such information for deceitful activity either on the Internet or offline."

Currently, cyber-identity theft is the most common Internet-related crime reported to the U.S. Federal Trade Commission (FTC). Victims of cyber-identity theft often suffer socially, psychologically and financially. Businesses and organizations are also victimized by this type of Internet crime.

Academic research is beginning to emerge on the topic of identity theft; however, to date scholars have published relatively few studies specific to Internet-related identity theft. Close et al. (2004) present an overview of cyber-identity theft with an emphasis on the implications for public policy. Policy and online behavior must change to combat cyber-identity theft. Internet-related identity theft is, in part, a function of an individual's risky

online transactions (Milne, Rohm, & Bahl, 2004). Consumers' online behaviors may increase or even decrease the risk of becoming a victim of identity theft (Milne et al., 2004). Each consumer differs in the extent to which he or she protects his or her online identity and privacy. This difference may be attributed to the Internet user's demographics, attitude, and online behaviors (Milne et al., 2004).

CYBER-IDENTITY THEFT: KEY METHODS

Common methods of cyber-identity theft include: (a) phishing, (b) employee abuse, (c) mass rebellion, (d) disposal, (e) pranking/posing, (f) spyware, and (g) a scam within a scam. In Table 1, we define and provide examples of these methods. In the table, we use the term *broad scope* to refer to methods that have a negative, simultaneous effect on *multiple* consumers. Broad scope methods often make use of automated tools to facilitate identity theft (McCarty, 2003). In the table, we also describe "narrow scope" methods, which refer to methods that affect *individual* consumers (see Table 1).

Table 1 reveals a number of implications for policymakers; in order to protect consumers it is necessary: (a) to inform consumers about related dangers, (b) to provide safe environments for conducting electronic exchanges, (c) to assist victims, and (d) to implement public policy remedies and legal action. Unfortunately,

Table 1. Key methods of cyber-identity theft (Reprinted with permission from Enhancing knowledge development in marketing*, published by the American Marketing Association, edited by Bernhardt, Boles, and Close, written by Zinkhan, and Finney, 2004, pp. 48-55)*

Method	Definition	Example
Broad Scope*		
Hacking	Breaking into a computer database personal or business/organization/government	Wiring another's funds
Employee Theft	Employees utilizing or selling their company database for fraudulent means or without permission	Pilfering office files
Dictionary Programs	Automatically search all dictionary words for a possible password	Checking all works A to Z
Spyware	Software, often disguised, that may install itself with other legitimate or free downloads, to collect personal information	Weather-bug, Gator
Skimming	Copying information from a magnetic strip, and subsequently using the information to create a duplicate	Credit cards
Tapping	Monitoring computer systems to extract key information	Restaurant computers for credit card numbers
Pre-approved	Taking another's per-approved credit and SSN to open an unauthorized account	Mailed credit card offers
Mass Rebellion	Peer-to-peer networks built to exchange music or media files. At present, the future of such sites is unclear, and some users are being taken to court (e.g., by the music and film industry)	peer-to-peer sites (e.g., Kazaa, Napster)
Narrow Scope		
Carelessness	Prowling for users who use their computer or Internet access carelessly	Saved Passwords, logoff may not go through
Disposal Abuse	Obtaining information from another's disposed / sold hardware or software	Dumpster-diving, leaving personal information on old computer via junk-yard, garage sale
Autofill Abuse	Obtaining information from computer programs that "memorize" and complete typing on another's machine	Type in a few letters until cleared
Phishing	Establishing a fake Web site designed to look like a company's actual site or sending official-looking messages	"Official" request for SSN
Phony	A phony machine that copies personal information	ATM
Pre-text	Calling a prospective victim, posing in an attempt to obtain personal information	Bank. Credit card company
Posing	Unrightfully representing another individual	Bank rep., computer exams
Pranking	Posing as another online to play a joke or for fun	E-dating
Fraudulent Job Posting	Posting a job that does not exist to collect personal information	"Manager Wanted: Apply Online"
Shoulder Surfing	Peeking for information as another enters it on a computer screen; physically watching passwords	Passwords, Account numbers
Intercepting	Receiving online traffic intended for another	IM (Instant Message), E-mail