Identity Theft and Social Networks

Jordana N. Navarro, Ph.D.
Tennessee Technological University
Department of Sociology and Political Science

Jana L. Jasinski, Ph.D.
University of Central Florida
Department of Sociology

Identity Theft and Social Networks

Overview

Identity theft is frequently referred to as one of the fastest growing crimes in the United States (Aïmeur & Schonfeld, 2011; Brody, Mulig, & Kimball, 2007; Hoofnagle, 2007; Lynch, 2005; Slosarik, 2002). In 2012, the United States Federal Trade Commission (FTC) received more than two million complaints, and approximately one in five of those complaints related to identity theft (Small, 2013). In addition, as of September 30, 2012, the United States Internal Revenue Service (IRS) had already identified more than 600,000 incidents of identity theft relating to tax administration alone (White, 2012). Prohibited by the Identity Theft and Assumption Deterrence Act, identity theft is defined as:

> Knowingly transferring or using, without lawful authority, a means of identification of another person with the intent to commit, or aid or abet, any unlawful activity that constitutes a violation of Federal law or that constitutes a felony under any applicable State or local law. (Federal Trade Commission, 1998).

Despite widespread recognition of identity theft as a serious social problem affecting consumers, businesses, and governments; there is a death of information on the actual scope of the problem (Allison, Schuck, & Lersch, 2005; Hoofnagle, 2007; May & Headley, 2004; Newman & McNally, 2005; Slosarik, 2002). Determining the prevalence of identity theft is difficult for the following reasons: victims may not learn of thefts until months later; victims may decline to report identity thefts to law enforcement; victims may report thefts to other agencies instead of law enforcement (i.e. banks, credit card companies); thefts may span multiple jurisdictions resulting in confusion regarding investigation responsibility; and due to the

complexity of these crimes, an identity theft may only be part of the possible countless other offenses a perpetrator engaged in (Hoofnagle, 2007; May & Headley, 2004; Newman & McNally, 2005; Stana, 2002).

Accounting for these barriers, the Bureau of Justice Statistics (BJS) reported that approximately 8.6 million households experienced an identity theft in 2010: representing an increase of 5.5% from 2005 data (Langton, 2011). Victim characteristics derived from 2005 and 2010 data indicate that individuals 65 years old or older were less likely to suffer identity theft compared to households headed by younger individuals (Langton, 2011). However, risk of identity theft to non-Hispanic Caucasian and Asian head of households increased between the two years (Langton, 2011). Finally, risk of identity theft increased among households with an income of $75,000 or more and among households that did not disclose income (Langton, 2011). These data indicate victims of identity theft suffered a total financial loss of approximately $13.3 billion in 2010 (Langton, 2011). Monetary cost is only part of the damage though; evidence suggests victims experience extensive non-monetary damages as well (Hoofnagle, 2007; May & Headley, 2004; Newman & McNally, 2005; Lynch, 2005; Sharp, Shreve-Neiger, Fremouw, Kane, & Hutton, 2004; Slosarik, 2002).

According to May and Headley (2004), an identity theft victim spends an average of 200 hours trying to repair the damage caused by the violation. These hours are spent contacting banking institutions, credit bureaus, and other vendors; copying documents; obtaining legal assistance; and spending hours on the phone to all relevant parties (May & Headley, 2004). In addition, victims of identity theft may encounter additional barriers to obtaining employment in the forms of destroyed credit (Hoofnagle, 2007) or criminal histories for offenses the perpetrator engaged in using the stolen information (Lynch, 2005; Newman & McNally, 2005). Taking into

account the extensiveness of these consequences it is not surprising that research suggests victims also experience psychological and physical ramifications of identity theft.

One study found within two weeks of learning of an identity theft; victims felt angry and irritable, fearful and anxious, and frustrated (Sharp et al., 2004). At 26 weeks following the victimization, victims were angry, desperate, and distressed. Moreover, victims also experienced physical reactions such as anxiety, appetite problems, headaches, sleep problems, and weight changes (Sharp et al., 2004). Although this chapter is primarily concerned with identity thefts of individual victims, businesses and governments also bear direct costs (i.e. resulting from the actual fraud) and indirect costs (i.e. resulting from conducting investigations) for these offenses in excess of millions of dollars annually (Hoofnagle, 2007; Lynch, 2005; May & Headley, 2004; Newman & McNally, 2005; The President's Identity Theft Task Force, 2007).

Less is known about perpetrators of identity theft and what information is known can be largely inconsistent across studies. For example, while some evidence suggests African-American females comprise a large proportion of offenders (Allison et al., 2005); other research indicates perpetrators are from a variety of backgrounds (Aïmeur & Schonfeld, 2011). Research has shown that perpetrators also vary in age, typically operate independently, and often have no prior criminal background (Aïmeur & Schonfeld, 2011; The President's Identity Theft Task Force, 2007). However, identity theft rings operated by formal organizations - such as the Hell's Angels - are also known to exist (May & Headley, 2004; Newman & McNally, 2005; The President's Identity Theft Task Force, 2007). Finally, although some research has found that victims may not know perpetrators (Allison et al., 2005); other evidence indicates that it is not uncommon for the victim and perpetrator to indeed be familiar with each other (Finn & Banach, 2000; Newman & McNally, 2005; The President's Identity Theft Task Force, 2007). According

to Neman and McNally (2005), if the victim and perpetrator are known to each other, the most frequently reported relationship is through a familial association.

Far from a novel crime, some suggest the rapid advancement of technology, particularly the rise in popularity of social networks, has exacerbated the identity theft problem by providing a rich setting for criminals (Weir, Toolan, & Smeed, 2011). This chapter will explore the aforementioned topic in detail by first providing an overview of social network characteristics that make these cyberspace "hang-outs" attractive targets for identity thieves. Discussion will then focus on different forms of identity theft, and how identity thieves exploit social networks to steal personal information. Finally, concluding discussion will provide information on emerging methods of identity theft within social networks.

Attractive Targets: Why Identity Thieves Like Social Networks

Social networks are online social structures comprised of nodes representing people and organizations that are interconnected through business relationships, familial background, friendships, general interests, and shared values or visions (Bilge, Strufe, Balzarotti, & Kirda, 2009). Since bursting onto the technological scene, social networks have grown in popularity at an exceedingly rapid pace and now constitute some of the largest databases in the world (Aïmeur & Schonfeld, 2011; Bilge et al., 2009; Debatin, Lovejoy, Horn, & Hughes, 2009). For example, although social network giant Facebook was established in 2004, as of 2013 the site boasts more than a billion monthly active users (Facebook, 2013). This growth in popularity is likely due to the substantial benefits of social networks that are free to users: the ability to facilitate instantaneous access to long-lost friends, loved ones, and professional acquaintances regardless of geographic boundary (Bilge et al., 2009).

Private individuals are not the only individuals increasingly utilizing social networks; companies also heavily utilize social networks for advertising purposes (Timm & Perez, 2010). For example, MySpace and Facebook generated more than $300 million dollars in advertising revenue in 2006 alone (Timm & Perez, 2010). The popularity of social networks sites among individuals and companies is one of the primary reasons why they are prone to security threats (Sood & Enbody, 2011). According to Timm and Perez (2010), social network sites provide access to millions of potential victims and plenty of tactics to evade detection. Moreover, because security and privacy controls are generally not a top priority for developers, safeguards against attacks are relatively weak (Aïmeur & Schonfeld, 2011; Al Hasib, 2009; Bilge et al., 2009).

While more attention has been placed on social network privacy controls as of late (see for example Arthur, 2012), ownership to protect oneself is still largely the responsibility of individual users. This burden of responsibility may be unduly placed as research suggests that social network users are not fully aware of how their profile information is accessed or shared by others, including search engines, or knowledgeable about general security awareness (Al Hasib, 2009; Aïmeur & Schonfeld, 2011; Bilge et al., 2009). As a result, the convergence of these three factors - motivated offenders, suitable targets, and a general lack of safeguards – produces online environments where identity theft is relatively inexpensive to commit and the chances of arrest are significantly lower than other types of crimes (Lynch, 2005).

Types of Identity Theft

Although identity theft victims primarily suffer financial loss (Lynch, 2005), victims may be targeted in order to damage reputations and/or destroy brands (Aïmeur & Schonfeld, 2011; Al Hasib, 2009). Victims may also be targeted as a means to acquire access to health services,

employment, or to evade detection by law enforcement (May & Headley, 2004; Sterritt, 2011; The President's Identity Theft Task Force, 2007). Arguably, in some cases, motivations may be complex and multifaceted. For example, a perpetrator may target a particular victim to not only cause financial ruin, but also to destroy the victim personally as well.

Financially Motivated Identity Theft.

Two of the most common types of financially driven identity theft are the creation of new accounts and account takeovers (Hoofnagle, 2007; The President's Identity Theft Task Force, 2007; Vacca, 2003). The former type entails perpetrators utilizing stolen personal information to obtain access to a plethora of services, including but not limited to: credit cards, mortgages, phone accounts, and utility accounts (Acquisti & Gross, 2009a; Hoofnagle, 2007; The President's Identity Theft Task Force, 2007; Vacca, 2003). In contrast, an "account takeover" entails perpetrators acquiring security credentials in order to assume control over their victims' financial accounts for the purposes of stealing funds and making illegal transactions (Hoofnagle, 2007; Sharp et al., 2004). Upon obtaining access, perpetrators also acquire the ability to change credentials in order to prevent victims from accessing their own accounts (Timm & Perez, 2010).

According to May and Headley (2004), financially-driven identity theft has become a booming business coordinated by organized international networks of thieves targeting large numbers of victims in order to steal as much capital as possible. Some of these organizations identified include the Hell's Angels, Mara Salvatrucha (MS-13), and foreign groups based overseas (Newman & McNally, 2005; The President's Identity Theft Task Force, 2007). Particularly unsetting is the fact that most victims do not learn of the theft until potentially years later (Slosarik, 2002) or after they are denied credit (The President's Identity Theft Task Force,

2007). This lag in awareness is likely due to the common practice of changing victims' mailing addresses to prolong detection among others (May & Headley, 2004).

Other Types of Identity Theft.

Perpetrators may engage in identity theft for several other nefarious purposes (Aïmeur & Schonfeld, 2011). For example, one such purpose is to acquire access to services in order to assimilate into society (Acquisti & Gross, 2009a; Aïmeur & Schonfeld, 2011; The President's Identity Theft Task Force, 2007). Access to services could entail using stolen information to obtain medical services (or make false claims for medical care) and to obtain passports in order to secure employment (Aïmeur & Schonfeld, 2011; The President's Identity Theft Task Force, 2007). Perpetrators may also engage in identity theft in order to participate in crimes under the guise of another individual or to evade detection by law enforcement altogether by masquerading as someone else (Aïmeur & Schonfeld, 2011; Lynch, 2005; Newman & McNally, 2005). Finally, perpetrators may engage in identity theft in order to personally harm victims by destroying reputations (Timm & Perez, 2010). After providing a brief overview of the various types of identity theft, the following discussion focuses on how these crimes are conducted online and within social network sites – often with unsettling ease (Slosarik, 2002).

Tactics Utilized by Identity Thieves Online

The advancement of technology - particularly the creation of online social networks - has created environments where identity theft is substantially easier to commit with significantly less risk (Lynch, 2005; Slosarik, 2005). In the following sections, several of the most common methods utilized today are discussed. These methods include relatively simple techniques (i.e. aggregation of publically available data, Evil Twin attacks) and more complex "high-tech" procedures (i.e. malware, phishing attacks). Because perpetrators are increasingly using social

networks to engage in identity theft, the following discussion will also include examples of how the aforementioned methods occur within these online communities.

Aggregating Publically Available Data.

While researchers have identified several well-known high-tech and low-tech methods utilized by identity thieves, one "mid-tech" method also utilized simply involves the aggregation of publically available online data using a computer and widely-available search engines or social network databases (Aïmeur & Schonfeld, 2011; Allison et al., 2005; Lynch, 2005; The President's Identity Theft Task Force, 2007; Timm & Perez, 2010). According to Aïmeur and Schonfeld (2011), Internet users are largely unaware of the amount of personal information they disclose online; which is then accessed by search engines, social network sites, and other online services. Even fewer users are aware that these data can easily be aggregated and linked together in order to steal identities (Aïmeur & Schonfeld, 2011; Marshall & Tompsett, 2005).

One particularly infamous case of identity theft through aggregation of publically available data occurred less than five years ago. In 2010, a 20-year-old college student successfully hacked into Sarah Palin's Yahoo email account by resetting her password using only publically available online information (Aïmeur & Schonfeld, 2011; Lehrman, 2010). In another widely discussed case, Herbert Thompson (a professor and software developer) was able to successfully obtain access to an acquaintance's bank account in less than an hour by utilizing only publically available online information (Aïmeur & Schonfeld, 2011; Thompson, 2008). Adding to this alarm, relatively recent research has uncovered that social security numbers can be successfully predicted from information frequently posted online and on social network profiles.

The importance of safeguarding social security numbers cannot be understated as identity

thieves can completely decimate victims' personal and financial lives by merely knowing these authentication numbers (Acquisti & Gross; 2009a, 2009b; Slosarik, 2002). Therefore, given this importance, Acquisti and Gross (2009b) recently evaluated whether social security numbers could be predicted from publically available information regarding date of birth and hometown – two pieces of information also included on social network profiles (Gross & Acquisti, 2005). After taking into account the standard formatting of social security numbers[1], the scholars were able to successfully predict – on first attempt – the partial social security numbers for 7% of the individuals born nationwide from 1973 to 1988 whose information resided within the Death Master File (DMF) database maintained by the Social Security Administration. Moreover, the success rate increased to 44% for individuals born after 1988 (Acquisti & Gross, 2009b). Given the potential risks of "over-exposing" one's personal information, Thompson (2008) cautions Internet users to "think first, post later." Thompson's advice is particularly important for social network users as these sites are becoming frequent conduits to infect users with "malicious software," otherwise referred to as malware (Hunter, 2008).

Malicious Software.

The advancement of the Internet has led to identity thieves utilizing increasingly sophisticated methods to steal personal information, such as the creation and dissemination of malware (Aïmeur & Schonfeld, 2011; Bilge et al, 2009; Emigh, 2006; Jaishankar, 2008; Newman, 2006; Sood & Enbody, 2011). The term malware defines a malicious type of software

[1] According to Acquisti and Gross (2009b), the construction of social security numbers follows a relatively standard format. The first three numbers, referred to as the "area number," correspond to the zip code of the mailing address included on the original application for the identifier (Acquisti & Gross, 2009b). The two next digits are referred to as the "group number" and follow a precise and nonconsecutive order between 01 and 99 (Acquisti & Gross, 2009b). Finally, the "serial number" is the last set of four digits that are assigned consecutively from 0001 to 9999 (Acquisti & Gross, 2009b).

that performs an undesirable function to the user (Emigh, 2006; Timm & Perez, 2010). Several of the most common categories of malware include crimeware, spyware, adware, browser hijackers, downloaders, toolbars, and dialers (Emigh, 2006; Timm & Perez, 2010). Although all types of malware are undesirable, crimeware and spyware are particularly important for the problem of identity theft (Emigh, 2006).

Crimeware broadly defines any type of malware designed to facilitate an illegal activity – such as stealing personal information (Emigh, 2006; Timm & Perez, 2010). Relatedly, spyware broadly defines any type of malware designed to secretly collect information about users, which then may also be used to engage in identity theft (Timm & Perez, 2010). Specific types of malware include the following: Trojan horses, backdoors, keyloggers, screen loggers, and worms (Aïmeur & Schonfeld, 2011; Emigh, 2006; Newman, 2006; The President's Identity Task Force, 2007; Timm & Perez, 2010). Although the umbrella term "malware" is used to describe any type of malicious software, each particular program functions slightly differently.

A widely recognized form of malware is a Trojan horse. A Trojan horse conceals itself by appearing to be legitimate software, but actually provides unauthorized access to a computer (Newman, 2006; Timm & Perez, 2010). Similarly, backdoor malware facilitates access to a computer system by specifically bypassing normal authentication procedures (Timm & Perez, 2010). Keyloggers and screen loggers are types of malware designed to either record keystrokes or screen shots of confidential information – such as user names and passwords – and send this information back to a storage location (Aïmeur & Schonfeld, 2011; Timm & Perez, 2010). Finally, worms are an infectious type of malware that can rapidly propagate - without assistance from users - to compromise the security of many other machines (Emigh, 2006; Lehrman, 2010; Newman, 2006; Sood & Enbody, 2011; Timm & Perez, 2010).

According to Emigh (2006), not only can malware be used to collect sensitive information about victims, but can also be utilized to gather information about each victims' colleagues and acquaintances. Moreover, because malware software often appears to perform legitimate functions (e.g. appear as an update to Adobe Flash); victims may not realize their information has been stolen for some time. While all forms of malware pose dangers to users, worms are particularly vicious within social networks and are becoming a frequently utilized method by identity thieves to steal personal information (Bilge et al., 2009; Emigh, 2006; Jaishankar, 2008; Lehrman, 2010; Newman, 2006; The President's Identity Theft Task Force, 2007; Thomas & Nicol, 2010).

Evidence suggests that social network users place too much implicit trust in their online interactions, thereby exposing themselves to cybercriminals seeking to exploit that confidence (Bilge et al., 2009; Thomas & Nicol, 2010; Timm & Perez, 2010). One method of exploitation increasing in frequency is the utilization of social network sites to distribute destructive worms, such as the infamous Koobface program. First appearing in 2008, Koobface (an anagram for Facebook) used social network users' contact lists to replicate itself at a rapid pace; ultimately compromising victims' information (Lehrman, 2010; Thomas & Nicol, 2010; Timm & Perez, 2010).

The start of Koobface's infection began when unsuspecting social network users were sent a communication from seemingly trusted sources that contained a hyperlink to a third-party site (Thomas & Nicol, 2010). Although appearing as legitimate contacts, these communications may have come from other compromised accounts or forged accounts automatically created by Koobface (Thomas & Nicol, 2010). However, because the messages appeared to be from legitimate sources, naive users followed the provided navigations, received a prompt to update a

legitimate piece of software (Adobe Flash in this case), and were duped into installing the Koobface worm on their own machines (Lehrman, 2010; Thomas & Nicol, 2010). As a result of installing the malicious software, victims unknowingly compromised their personal information as well as granted perpetrators unauthorized access to their social network accounts to further spread the Koobface worm (Lehrman, 2010; Thomas & Nicol, 2010).

In their relatively recent investigation of Koobface, Thomas and Nicol (2010) discovered the worm was sent to over 213,000 social network users: netting over 157,000 clicks (i.e. number of times malicious link was accessed) for perpetrators. Moreover, while the Koobface worm targeted Facebook users, similarly constructed and equally destructive worms have also surfaced on other social network sites like MySpace and Twitter (Sanzgiri, Joyce, & Upadhyaya, 2011; Sood & Enbody, 2011). Despite the infamy of these worms and risks of malware in general, evidence indicates that the average social network user still does not have a holistic understanding of how to protect themselves from attacks.

Relatively recent studies support the notion that social network users may be continuing to place themselves in vulnerable positions. For example, research conducted by Debatin et al. (2009) found that while half of the respondents noted they increased their social network account privacy settings, a relative majority also had over 300 friends with varying degrees of connection to the user. In addition, over 90% of respondents included their full real name, gender, date of birth, and hometown on their profiles; a comparable percentage also included information relating to friends, family members, and pets as well (Debatin et al., 2009). Taking into account that security questions may reference the aforementioned information (i.e. a pet's name), the availability of this information in an online forum can easily be used to compromise users'

identities. Related to the problem of malware, another method that identity thieves utilize to acquire victims' personal information is through conducting phishing frauds (Brody et al., 2007).

Phishing and Spear-Phishing.

The term "phishing" stems from the word "fishing," because it involves a process of "casting" many emails – or messages within a social network site – in an attempt to "lure" and "hook" unwary victims (Brody et al., 2007; Jagatic, Johnson, Jakobsson, Menczer, 2007; Jaishankar, 2008; Lynch, 2005; Newman & McNally, 2005). In contrast to the previous section, phishing scams are essentially online cons meant to dupe victims into *voluntarily disclosing* personal information (Aïmeur & Schonfeld, 2011; Brody et al., 2007; Hoofnagle, 2007; Hunter, 2008; Jagatic et al., 2007; Jaishankar, 2008; Lynch, 2005; Timm & Perez, 2010). In addition to indiscriminate phishing scams, a more lethal form of this con – referred to as spear-phishing – is gaining increasing attention from cybersecurity guardians (Brody et al., 2007). Considered a hybrid form of phishing, spear-phishing targets specific victims instead of a broad audience (Brody et al., 2007). As a result, spear-phishing is more difficult to detect, because the communication appears to legitimate (Brody et al., 2007).

Although phishing scams continue to evolve with technology, research has established a fairly predictable pattern associated with these assaults. The process begins with phishers sending a message to victims luring them to a seemingly legitimate website; however, the website provided is actually "spoofed" or malicious (Aïmeur & Schonfeld, 2011; Brody et al., 2007; Hoofnagle, 2007; Hunter, 2008; Jagatic et al., 2007; Lynch, 2005; Timm & Perez, 2010). In order to encourage users to navigate to the spoofed site, phishing messages typically employ a scare tactic and stress an immediate action is necessary from the target (Lynch, 2005; Timm & Perez, 2010). For example, a phisher may send an email notifying targets that their PayPal

accounts have been compromised and requesting they reset their security credentials immediately (Newman, 2006). However, instead of linking to the legitimate PayPal site, a malicious website address is noted instead (Newman, 2006). An example of this trick is the difference between the legitimate website address for PayPal (www.paypal.com) and potential spoofed website address (www.paypa1.com) that has the number one noted in place of the lowercase "l" (Newman, 2006). Targets that fall for the deception and click the malicious link are then navigated to the bogus website created by the phisher, which is usually indistinguishable from its legitimate counterpart (Brody et al., 2007; Lynch, 2005). Although targets may believe they are logging into the legitimate site, they are actually disclosing their login credentials to the phisher to enact further damage (Lynch, 2005; Timm & Perez, 2010).

Given the enormity and general lack of safeguards on social network sites, phishing attacks have become more sophisticated and can now easily exploit contacts in these online databases (Jagatic et al., 2007; Timm & Perez, 2010). Indeed, according to Timm and Perez (2010) phishing attacks on social network sites have increased by 240%; including Facebook, MySpace, and Twitter. In order to illustrate how phishing scams occur within these online communities, information regarding several actual attacks targeting three major social networks is discussed in the following section.

In early 2009, Twitter users received phishing messages from followers enticing them to click a malicious link (Timm & Perez, 2010). Targets that clicked the link were directed to a spoofed site that appeared to be Twitter's main page and prompted to log back in (Timm & Perez, 2010). The Twitter accounts of the users that fell for the scam and entered their credentials were then compromised and used as conduits to send additional phishing messages (Timm & Perez, 2010). Similar attacks also occurred on Facebook and MySpace. In these attacks, phishing

messages were sent to users advertising opportunities to earn quick money (Timm & Perez, 2010). Users that followed the provided navigations were then prompted to re-enter their security credentials; however, instead of accessing the social network, users only succeeded in compromising their own accounts (Timm & Perez, 2010). While some scams may only involve attempts to dupe targets into disclosing security credentials, other more sophisticated deceptions include tricking targets into downloading malware to further compromise their information.

In an example provided by Timm and Perez (2010), the phisher sent the target a message through a social network enticing the "phish" to watch a funny video. After clicking on the link, the target was taken out of the social network to a seemingly legitimate video-hosting site (Timm & Perez, 2010). As noted by Timm and Perez (2010), the target then received a notice to update their software in order to view the video. However, the supposed update was actually malware that assumed control of the target's browser upon installation (Timm & Perez, 2010).

Although the example provided by Timm and Perez (2010) illustrates how phishing and malware were used to ultimately conduct a browser hijack, the same method of attack is increasingly being utilized to disseminate all types of malicious software (i.e. keyloggers, screen loggers, worms, etc.). Indeed, according to Jaishankar (2008), malware is the main method utilized by phishers to engage in cybercrime, such as identity theft. Although malware and phishing pose serious threats of identity theft, evidence repeatedly suggests that the weakest link to safeguarding information is the social network user and the implicit trust placed into online interactions (Thomas & Nicol, 2010). The aforementioned is exactly why relatively simple forms of social engineering can be as dangerous to users as the high-tech methods previously discussed.

Social Engineering, Evil Twin Attacks, and Profile Squatting.

In contrast to the high-tech methods (i.e. malware and phishing) previously discussed, conducting identity theft through relatively simple forms of social engineering – such as in "Evil Twin" attacks or profile squatting – requires minimal technological knowledge. Social engineering broadly defines attempts to manipulate victims in order to extract some information from them or to encourage them to engage in malicious activities on behalf of the attacker (Aïmeur & Schonfeld, 2011; Huber et al., 2009; Lehrman, 2010; Newman, 2006; The President's Identity Theft Task Force, 2007; Timm & Perez, 2010). For example, the process of spreading malware is considered a form of social engineering, because perpetrators manipulate victims into installing the malicious software that then potentially facilitates illegal activities (Emigh, 2006; The President's Identity Theft Task Force, 2007). Similarly, phishing is also a form of social engineering, because it involves manipulating victims into disclosing confidential information under false pretenses (The President's Identity Task Force, 2007). Likewise, conducting an "Evil Twin Attack" or "profile squatting" is a form of social engineering, because the actions are ultimately deceptions by the perpetrator in order to achieve an overall objective.

An Evil Twin Attack simply involves perpetrators pretending to be legitimate users in order to gain something they are not entitled too (Timm & Perez, 2010). Similarly, "profile squatting" involves perpetrators creating bogus profiles of renowned individuals or brands for the same purposes (Al Hasib, 2009). Evil Twin Attacks and profile squatting may occur on social networks for any of the following reasons: to trick friends into giving money to the perpetrator, to post inflammatory comments in the victim's name in order to damage that individual's reputation, and to post inaccurate comments regarding a company's performance under the guise of a high-level executive in order to influence stock prices (Timm & Perez, 2010). Accounting

for the largely unrestricted registration process utilized among social networks and the lack of identity verification conducted by administrators, establishing false profiles entails minimal effort from identity thieves (Aïmeur & Schonfeld, 2011; Timm & Perez, 2010). Indeed, according to Timm and Perez (2010), the only information actually required in order to engage in an Evil Twin attack is the name of the person to impersonate. Any additional information to ensure the profile is *believable* can often easily be found online, although is not necessary (Timm & Perez, 2010). Again, while motivations may vary, the two primary reasons perpetrators engage in these forms of identity theft are to harm victims financially or to harm victims personally (Al Hasib, 2009; Marshall & Tompsett, 2005; Timm & Perez, 2010).

A common method of stealing funds from victims via an Evil Twin Attack is by impersonating friends who are in detrimental situations (Timm & Perez, 2010; Weir et al., 2011). For example, in a scenario provided by Weir et al. (2011), a social network user (the actual victim) receives a frantic message from a friend supposedly traveling abroad (actually the message is from the identity thief who has assumed control of their friend's account). According to the message, the victim's friend was mugged and lost all their resources (i.e. money, passport, etc.; Weir et al., 2011). As a result, the victim's friend is in desperate need of money and pleas for funds to be sent to a specified account (Weir et al., 2011). However, in reality, the identity thief is the actual owner of the account and subsequently defrauds the victim (Weir et al., 2011). Although victims in this case suffer financial repercussions, damage caused by these types of attacks may also be personally shattering.

The motivation of an Evil Twin Attack may be non-monetary and purely driven to enact personal damage on a victim as the case of James Lasdun illustrates. According to Lasdun (2013), after rejecting the advances of a former student, the student began engaging in a variety

of behaviors online meant to destroy his professional and personal reputation. One method of attack entailed masquerading either as the victim himself or as his professional associates (i.e. a program director) and posting defamatory comments (Lasdun, 2013). For example, due to the lack of restrictions and identity verification conducted online, the former student was able to post comments masquerading as Lasdun that openly claimed he plagiarized others (Lasdun 2013). Although Lasdun's case is not specific to a social network, similar methods of identity theft occur in these venues as well.

In a case of profile squatting, a former executive created a forged profile pretending to be Sarah Palin (Rosman, 2009). Rosman (2009) reports that almost immediately after creating the fictitious profile, the imitator acquired approximately 100 friends. Moreover, as news regarding Palin fluctuated, the imitator received additional friendship requests upwards of 500 users (Rosman, 2009). Although some followers of the fictitious profile were doubtful of its authenticity, Rosman notes the vast majority seemed unperturbed. In fact, the charade went on for some time until system administrators eventually closed the profile after the legitimate Sarah Palin (through her representatives) contacted the social network company (Rosman, 2009). While the individual behind the forged Sarah Palin account likely only represented a nuisance to the politician, Lasdun's case represents the other end of the extreme. Indeed, as noted by Lasdun (2013, p.4), "You are what the Web says you are, and if it misrepresents you, the feeling of having been violated is crushing."

Selling Victims Out: Underground Identity Theft Market

Identity theft is typically discussed in terms of three stages: acquisition or the acquiring or personal information, the use of the information or *distribution* of information to others, and the resulting fraud itself (Aïmeur & Schonfeld, 2011). In a rare investigation into the

underground economy, scholars examined the financial windfall for identity thieves that trade in stolen information. As part of their inquiry, scholars were able to harvest stolen credential information in dropzones[2] maintained by identity thieves that stemmed from more than 173,000 compromised machines (Holz, Engelberth, & Freiling, 2008). In total, Holz et al. (2008) found 10,775 unique bank account credentials comprising of the following locations (in order of highest to lowest amount of credentials stolen): PayPal, Commonwealth Bank, HSBC Holding, Bank of America, and Lloyds Bank. Credit card credentials were also recovered and represented several of the major credit grantors (in order of highest to lowest amount of credentials stolen): Visa, MasterCard, American Express, Diners Club, and other types (Holz et al., 2008). Through their analysis, Holz et al. (2008) estimated these credential data potentially netted identity thieves millions of dollars. Aside from financial information, social network accounts were also represented and commoditized.

Holz et al. (2008) found more than 78,000 social network credentials existed within identity thieves' dropzones consisting of the following providers (in order of highest to lowest amount of credentials stolen): Facebook, hi5, nasza-klasa.pl, odnoklassniki.ru, Bebo, YouTube, and other types. Moreover, slightly more than 7,000 credentials from online retailers were also recovered (Holz et al., 2008). According to Holz et al. (2008), the majority of these credentials belonged to eBay users, but a small minority belonged to Amazon and Overstock.com. As with bank account information, these data ranged in price from one to 15 dollars for credentials to social network accounts and from one to eight dollars for credentials to online retailers (Holz et al., 2008). Not only can these data be sold to engage in additional forms of identity theft, but can also be used to strengthen attacks against others (Holz et al., 2008). For example, by accessing a

[2] According to Holz et al. (2008), a dropzone is public directory on an online server that functions as an exchange site for data retrieved from keyloggers.

specific social network account, identity thieves can attempt to “spear-phish” the original victim’s friends and associates (Holz et al., 2008).

Emerging Trends in Online Identity Theft

As the technology continues to advance, undoubtedly so will the methods utilized by identity thieves. In fact, one such advancement becoming increasingly popular in attacks on social network is the distribution of malware through cross-site scripting (Timm & Perez, 2010). In contrast to identity theft largely by deception, in cross-site scripting, thieves exploit website vulnerabilities to distribute malware (Timm & Perez, 2010). In a persistent attack of this type, the only action required from the victim to become infected is to visit the compromised site (Timm & Perez, 2010). As soon as the compromised site is visited, the malware infects the victim’s machine and enacts its damage (Timm & Perez, 2010).

Another evolution in malware distribution increasing in frequency is what is commonly referred to as a “drive-by download.” According to Sood and Enbody (2011), a drive-by download occurs when perpetrators exploit vulnerabilities in web browsers. Through these tactics, perpetrators facilitate the transfer of malware to machines without the victims’ knowledge (Sood & Enbody, 2011). In a recent example of this type of attack, television network giant NBC was hacked by identity thieves who utilized a drive-by download to force malware onto potentially thousands of visitors to the NBC.com website (Infosecurity, 2013). The attack was so devastating that security experts took several hours to remove the malware from the site, which was suspected to have been in an infectious state for at least 24 hours before intervention (Infosecurity, 2013). After further investigation, the malware was determined to be the Citadel Trojan, known for engaging in banking fraud and cyber-espionage (Smith, 2013). NBC is not alone however; as of this writing, several other high-profile companies had also been subjected

to this type of attack (Apple, Facebook, the Wall Street Journal, and the Washington Post; Infosecurity, 2013). A final trend warranting concern is the increasing utilization of botnets and puppetnets to act as proxies for perpetrator activities (Bailey et al., 2009; Huber et al., 2009; Timm & Perez, 2010).

Botnets surfaced in the early 2000s and have since been utilized to engage in a variety of criminal activities, including identity theft (Timm & Perez). According to Timm and Perez (2010), "bot" is an abbreviated term for "robot," which refers to a machine compromised by malware that is under the control of the perpetrator (otherwise referred to as a "herder"). The dissemination of the malware to create the botnet (or group of compromised machines) may occur through deceptive methods previously discussed or through direct infection of operating systems (Timm & Perez, 2010). After infection, perpetrators then utilize the botnet as a proxy to engage in cybercrime, such as automated phishing attacks or identity theft scams (Bailey et al., 2009; Huber et al, 2009; Timm & Perez, 2010). Frighteningly, victims may not even be aware their systems have been compromised or that their machines are being utilized to carry out such attacks on behalf of the perpetrator (Timm & Perez, 2010). Perhaps what is more alarming is that botnets have evolved and can now be launched within social networks.

A "puppetnet" is arguably the next evolutionary step in the "botnet." A puppetnet is similar to a botnet in that a perpetrator has assumed remote control over victims' machines; however, in contrast to a botnet, puppets do not have to install any malware to become part of the puppetnet (Timm & Perez, 2010). Instead, victims merely have to access a malicious page - such as a social network application - to become part of the puppetnet (Timm & Perez, 2010). Subsequently, every time victims log into the malicious application, their machines come under the control of the perpetrator to engage in a variety of activities (i.e. phishing scams, identity

thefts). However, unlike their bot counterparts, puppets terminate the perpetrator's control whenever they exit the malicious site or application (Timm & Perez, 2010). Yet, in an environment where potentially millions of users could be accessing applications with malicious code throughout the day, the danger associated with puppetnets is readily apparent.

Conclusion

This chapter began by discussing the problem of identity theft and copious gaps of information that persists regarding this type of crime – particularly related to identity theft on social networks. Although identity theft is not a new type of crime, the advancement of technology has provided a plethora of new methods to steal the personal information of others (Aïmeur & Schonfeld, 2011; Allison et al., 2005; Bilge et al., 2009; Debatin et al., 2009; Ho, Maiga, & Aïmeur; 2009; Lynch, 2005; Marshall & Tompsett, 2005; Slosarik, 2002; Timm & Perez, 2010). For example, instead of monitoring the incoming mail of a few victims, perpetrators have the ability to potentially steal the personal information of thousands of victims at once (Lynch, 2005). Indeed, the widespread congregation of millions of users on social network sites appears to have exacerbated this problem, especially given the relatively weak security and authentication procedures administrators utilize to police sites (Al Hasib, 2009). In addition, research suggests users may not fully understand the risks associated with "over-disclosing" personal information (Al Hasib, 2009; Bilge et al., 2009; Gross & Acquisti, 2005; Huber, 2009; Lehrman, 2010) or the potentiality to use this disclosed information to predict highly confidential data like social security numbers (Acquisti & Gross, 2009a). Therefore, awareness campaigns empowering social network users with knowledge regarding relatively "low-tech" methods of identity theft (i.e. aggregation of publically available data; social engineering) as well as "high-tech" methods (i.e. malware attacks, phishing scams) is vital to

combat this social problem. The necessity of this information is stressed in light of increasingly sophisticated tactics used by perpetrators to engage in identity theft within these forums such as: cross-site scripting, drive-by downloads, botnets, and puppetnets (Bailey et al., 2009; Huber et al., 2009; Timm & Perez, 2010). Given the enormous consequences identity theft has on victims, businesses (including social networks), and governments, empowering victims to be especially vigilant while online will assist in combatting the efforts of these motivated offenders.

References

Acquisti, A., & Gross, R. (2009a). Social insecurity: The unintended consequences of identity fraud prevention policies. In Workshop on the Economics of Information Security (pp. 24-25). Retrieved from: http://www.heinz.cmu.edu/~acquisti/papers/acquisti-MISQ.pdf.

Acquisti, A., & Gross, R. (2009b). Predicting Social Security numbers from public data. *Proceedings of the National Academy of Sciences*, *106*(27), 10975-10980.

Aïmeur, E., & Schonfeld, D. (2011). The ultimate invasion of privacy: Identity theft. In *Privacy, Security and Trust (PST), 2011 Ninth Annual International Conference on* (pp. 24-31). Institute of Electrical and Electronics Engineers (IEEE). Retrieved from: http://www.site.uottawa.ca/~ttran/teaching/csi5389/papers/Aimeur_and_Schonfeld_PST2011.pdf

Al Hasib, A. (2009). Threats of online social networks. *IJCSNS International Journal of Computer Science and Network Security*, *9*(11), 288-93.

Allison, S. F., Schuck, A. M., & Lersch, K. M. (2005). Exploring the crime of identity theft: Prevalence, clearance rates, and victim/offender characteristics. *Journal of Criminal Justice*, *33*(1), 19-29.

Arthur, C. (2012). Facebook to improve privacy controls over public visibility. *The Guardian.* Retrieved from: http://www.guardian.co.uk/technology/2012/dec/12/facebook-improve-privacy-controls-pictures-public

Bailey, M., Cooke, E., Jahanian, F., Xu, Y., & Karir, M. (2009, March). A survey of botnet technology and defenses. In *Conference For Homeland Security, 2009. CATCH'09. Cybersecurity Applications & Technology* (pp. 299-304). Institute of Electrical and Electronics Engineers (IEEE).

Bilge, L., Strufe, T., Balzarotti, D., & Kirda, E. (2009, April). All your contacts are belong to us: Automated identity theft attacks on social networks. In *Proceedings of the 18th International Conference on World Wide Web* (pp. 551-560). Association for Computing Machinery (ACM). Retrieved from: http://dl.acm.org/citation.cfm?id=1526784.

Brody, R. G., Mulig, E., & Kimball, V. (2007). Phishing, pharming and identity theft. *Academy of Accounting and Financial Studies Journal*, *11*(3), 43-56.

Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, *15*(1), 83-108.

Emigh, A. (2006). The crimeware landscape: Malware, phishing, identity theft and beyond. *Journal of Digital Forensic Practice*, *1*(3), 245-260.

Facebook. (2013). Key Facts. Retrieved from: http://newsroom.fb.com/Key-Facts.

Federal Trade Commission. (1998). Identity Theft and Assumption Deterrence Act. Retrieved from: http://www.ftc.gov/os/statutes/itada/itadact.htm

Finn, J., & Banach, M. (2000). Victimization online: The down side of seeking human services for women on the Internet. *Cyberpsychology and Behavior*, *3*(2), 243-254.

Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society* (pp. 71-80). ACM.

Ho, A., Maiga, A., & Aïmeur, E. (2009, May). Privacy protection issues in social networking sites. In *Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS International Conference on* (pp. 271-278). Institute of Electrical and Electronics

Engineers (IEEE). Retrieved from: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5069336&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5069336

Holz, T., Engelberth, M., & Freiling, F. (2009). Learning more about the underground economy: A case-study of keyloggers and dropzones. *Computer Security–ESORICS 2009*, 1-18.

Hoofnagle, C. J. (2007). Identity theft: Making the known unknowns known. *Harvard Journal of Law and Technology*, *21*, 98-122. Retrieved from: http://scholarship.law.berkeley.edu/facpubs/470.

Huber, M., Kowalski, S., Nohlberg, M., & Tjoa, S. (2009, August). Towards automating social engineering using social networking sites. In *Computational Science and Engineering, 2009. CSE'09. International Conference on* (Vol. 3, pp. 117-124). Institute of Electrical and Electronics Engineers (IEEE).

Hunter, P. (2008). Social networking: the focus for new threats—and old ones. *Computer Fraud & Security*, *2008*(7), 17-18.

Infosecurity. (2013). NBC hack serves Citadel malware to visitors. Retrieved from: http://www.infosecurity-magazine.com/view/30905/nbc-hack-serves-citadel-malware-to-visitors/

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, *50*(10), 94-100.

Jaishankar, K. (2008). Identity related crime in the cyberspace: Examining phishing and its impact. *International Journal of Cyber Criminology*, *2*(1), 10-15.

Langton, L. (2011). *Identity Theft Reported by Households, 2005-2010*. US Department of Justice, Office of Justice Programs, Bureau of Justice Statistics.

Lasdun, J. (2013). I will ruin him. *The Chronicle of Higher Education.* Retrieved from: http://chronicle.com/article/I-Will-Ruin-Him/136693/

Lehrman, Y. (2010). The Weakest Link: The Risks Associated with Social Networking Websites. *Journal of Strategic Security*, *3*(2), 63-72.

Lynch, J. (2005). Identity theft in cyberspace: Crime control methods and their effectiveness in combating phishing attacks. *Berkeley Technology Law Journal*, *20*, 259-300.

Marshall, A. M., & Tompsett, B. C. (2005). Identity theft in an online world. *Computer Law & Security Review*, *21*(2), 128-137.

May, D. A., & Headley, J. E. (2004). *Identity theft* (p. 1). P. Lang.

Newman, R.C. (2006). Cybercrime, identity theft, and fraud: practicing safe internet-network security threats and vulnerabilities. In *Proceedings of the 3rd annual conference on Information security curriculum development* (pp. 68-78). ACM.

Newman, G. R., & McNally, M. M. (2005). Identity theft literature review. *United States Department of Justice: National Institute of Justice*.

Rosman, K. (2009). Sarah Palin's Facebook Alter-Ego Gets Found Out. *The Wall Street Journal.* Retrieved from: http://blogs.wsj.com/speakeasy/2009/08/13/sarah-palins-facebook-alter-ego-gets-found-out/

Sanzgiri, A., Joyce, J., & Upadhyaya, S. (2012). The Early (tweet-ing) Bird Spreads the Worm: An Assessment of Twitter for Malware Propagation. *Procedia Computer Science*, *10*, 705-712.

Sharp, T., Shreve-Neiger, A., Fremouw, W., Kane, J., & Hutton, S. (2004). Exploring the psychological and somatic impact of identity theft. *Journal of Forensic Sciences*, *49*(1), 131-136.

Slosarik, K. (2002). Identity theft: An overview of the problem. *The Justice Professional*, *15*(4), 329-343.

Small, B. (2013). Top complaint to the FTC? ID theft, again. United States Federal Trade Commission. Retrieved from: http://www.consumer.ftc.gov/blog/top-complaint-ftc-id-theft-again

Smith, G. (2013). NBC.com hacked, experts say website may have spread malware. *The Huffington Post.* Retrieved from: http://www.huffingtonpost.com/2013/02/21/nbccom-hacked-experts-war_n_2735545.html

Sood, A. K., & Enbody, R. (2011). Chain Exploitation—Social Networks Malware. *ISACA Journal*, *1*, 31.

Stana, R.M. (2002). Identity theft: Prevalence and cost appear to be growing. United States General Accounting Office. Retrieved from: http://www.gao.gov/assets/240/233900.pdf.

Sterritt, S. N. (2011). Applying the Common-Law Cause of Action Negligent Enablement of Imposter Fraud to Social Networking Sites. *Seton Hall Law Review*, *41*, 1695.

The President's Identity Theft Task Force. (2007). *Combatting identity theft: A strategic plan.* Retrieved from: http://www.identitytheft.gov/reports/StrategicPlan.pdf

Thomas, K., & Nicol, D. M. (2010, October). The Koobface botnet and the rise of social malware. In *Malicious and Unwanted Software (MALWARE), 2010 5th International Conference on* (pp. 63-70). Institute of Electrical and Electronics Engineers (IEEE).

Thompson, H. H. (2008). How I Stole Someone's Identity. *Scientific American*. Retrieved from: http://www.scientificamerican.com/article.cfm?id=anatomy-of-a-social-hack

Timm, C., & Perez, R. (2010). *Seven deadliest social network attacks*. Syngress.

Vacca, J. R. (2003). *Identity theft*. Prentice Hall PTR.

Weir, G. R., Toolan, F., & Smeed, D. (2011). The threats of social networking: Old wine in new bottles? *Information Security Technical Report 16*(2), 38-43.

White, J. (2012). Identity theft: Total extent of refund fraud using stolen identities is unknown. United States Government Accountability Office. Retrieved from: http://www.gao.gov/assets/660/650365.pdf.