Chapter 3

Identity Theft: Tools and Techniques of 21st Century Bandits

Chapter Outline

I. Introduction
- A. Identity has been generally defined as the theft of someone's identity through the use of some form of personal identifying information, with the information being used for some fraudulent activity.
- B. A variety of different methods are employed in the classification of identity theft.
- C. Two primary classifications of identity theft
  1. Situations in which an individual's identity is stolen and the thief assumes the physical identity of the victim.
     a. This title of identity theft is rarely encountered.
  2. Situations involving credit fraud/financial fraud.
- D. Assuming the life of a potential victim
  1. Difficult to accomplish
  2. It is possible for a terrorist organization or an extremist group to assume another's identity in an attempt to remain hiding during the planning stages of an attack.
  3. Person may find themselves seeking a lifestyle that is beyond their means and may find that living someone else's life allows them an escape.
- E. The theft of a victim's credit identity
  1. A financially devastating criminal act.
  2. This is the fastest-growing high-technology crime in the world .
  3. A person becomes the victim of this form of identity theft when the thief is able to obtain a small amount of personal identifying information (normally a social security number, address, employer, spouse's name, etc.) and then uses that information to being modifying the victim's credit accounts.
     i. There are a variety of ways this information can be obtained.
- F. Online identity or virtual identity
  1. This is a third form of identity theft that is rarely discussed.
  2. Person can gain control of the screen name of another person, they can log into their social networking sites and change settings and posts comments about others who are in the victim's social circle.
  3. The theft of someone's virtual identity can be committed as a means of harassment or as a means of sending advertisements and solicitations to larger groups of people to whom the identity thief would not normally have access.

II. How Serious is the Identity Theft Problem?
- A. Identity theft is an extremely damaging crime, costing victims untold amounts of money in terms of lost credit, financial harm, and time invested in straightening out the matter.
- B. Victims can feel embarrassed when their credit applications are denied on the basis of an act for which they had no knowledge.
- C. Victims do not often suffer physical harm as a result of identity theft, and it might not be taken as seriously as other criminal activities, such as robbery or burglary.

D. Many victims might not even realize they have been victimized until they either apply for credit somewhere, or in extreme cases, the individual may discover that they are a victim when they are contacted by a court of law concerning outstanding warrants or fines.
E. According to information released by the Federal Trade Commission, identity theft accounts for more than 40 percent of all consumer fraud complaints, with approximately 9 million Americans having their identity stolen each year.
F. Why would someone not report being a victim of identity crime?
    1. Individual's perception that they could have done more to prevent the crime.
    2. Victim's belief that their victimization will not be taken seriously.
    3. Some victims think it is easier to not report the victimization than to report the crime and have law enforcement never make an arrest in the case.
    4. Law enforcement responses to this crime have gotten better over the last few years.
G. Misinformation in regard to how identity theft operates is a serious problem and is one that must be addressed in the near future.

III. How Identity Thieves Operation

A. Identity theft can be committed through a variety of techniques consisting of those that employ the use of computers, those that employ other high-technology device, or those that employ old-fashioned physical con artistry and thievery.
B. One of the earliest forms of identity theft involved a financial fraud scheme termed "check fraud."
    1. Blank checks were either stolen or manufactured.
    2. It is much easier to manufacture checks today with the use of computer hardware and printers.
    3. Operations that involved manufactured checks often utilized a technique known as "kiting" where an individual would take advantage of the lag time for communications between banks and cash checks on nonexistent accounts.
        a. Computers today allow banks to communicate much faster, and such activities as kiting are more difficult to engage in.
C. Beginning in the early 1990s, there were thousands of documents traded via computer networks and the Internet that discussed the crime of identity theft.
    1. Many contained detailed descriptions of how to commit identity theft, which at the time was reformed to as "carding."
        a. The term "carding" described all forms of identity theft related to the theft of a victim's credit card.
        b. Discussed methods of creating credit card numbers from using mathematical formulas to software programs that can general numbers.
        c. Individuals who advocated carding were always careful to stress that while obtaining the credit care information was fun, it was only half the process.
            i. An individual would have to utilize the stole credit card information to purchase some form of goods or services.
            ii. Early methods of shopping involved ordering items over the telephone and then scheduling the items to be delivered to the victim's residence when the victim was not at home.

iii. Carders then moved their deliveries to official delivery locations where anyone could open a fake account with only a minimum amount of identification.

d. Carding has been enveloped by the more encompassing term "identity theft."

A. The more commonly encountered methods of identity theft:

1. Dumpster diving

a. Dumpster diving involves a focus on a search for any documents with credit card information and a user's account information.

b. There is still a lot of information that can be found concerning a potential victim by engaging in a dumpster diving session.

c. One approach useful to identity thieves involves the collection of information from university settings.

i. Observe students throwing away unwanted solicitations and papers including preapproval forms for credit cards.

ii. Potential identity thief could come along and collect several of these applications at the end of the day.

2. Skimming

a. Skimming refers to the use of a small, often handheld, device that can store several hundred credit card numbers, cardholder names, and card expiration dates.

b. Skimmer devices work in much the same manner as the electronic card readers that are used in commercial venues when one uses their credit card or debit card.

c. Earlier text documents concerning skimming individuals encouraged obtaining jobs in the retail industry.

i. Information could be stolen from the electronic card reader

ii. Individuals could buy their own credit card skimmers and run cards through them before running them though the actual credit card reader.

d. Information stored on a skimmer could be connected to a computer and used to create a fake credit card that would bill all transactions to the original cared owner's account.

3. Shoulder Surfing

a. Similar to shoulder surfing used by hackers and phone phreaks.

b. When a user takes out his or her credit card to pay for their merchandise, either in preparation for the payment or after payment has been made and the user is waiting to sign the credit card slip, the identity theft will peer over the user's shoulder.

c. Because many credit card companies utilize the first four to eight numbers on all their credit cards, the identity theft does not have to remember many numbers.

d. Some identity thieves will use accomplices where one will wait until the person pulled out his or her credit or debit card and while the victim was signing the slip or talking to the cashier, the individual would call out the numbers over a cellular telephone to the accomplice.

4. Retail Scams
    a. There are a number of scams designed to work in large-scale retail outlets.
    b. Types of retail scams:
        i. One involves the use of an unwitting store clerk.
            1. When a potential victim comes along, the identity thief makes a telephone call to the cashier pretending to be a member of the company's lost prevention or security team.
            2. The clerk will be asked to read the check or credit card numbers over the phone.
        ii. Another scam involves the use of credit cards that are only used at the store issuing the credit card.
            1. Some stores allow customers to fill out credit card applications using miniature computers located around the store.
            2. These computers often only verify the existence of the social security number and may not verify the actual identity of the owner of the social security number.
            3. An identity thief can shoulder surf and get the credit card number and open an account.
5. Packet Sniffing
    a. A packet sniffing program is a software program that allows users to intercept data while it is en route to a website.
    b. This could allow an individual to intercept credit card information while the data is being transferred to a commercial website.
    c. Will read the headers of packets containing credit card information and then make a copy of the information and forward it to the packet sniffing software's administrator.
    d. All the information is then collected and the individual may begin to make purchases on the credit card numbers as they were received.
    e. It is believed that this type of software is infrequently used because it takes a great deal of effort to come away with a relatively few credit card numbers.
6. Phishing
    a. Phishing refers to a process whereby an identity thief will attempt to get a potential identity theft victim to provide them with the personal information needed to engage in identity theft.
    b. The victim might not realize that they information is being requested by a non-trusted source.
    c. Often times the victim of one of these scams will receive an e-mail or other communication that appears official and requests that the person submit this information in order to maintain their accounts.
    d. The term "phishing" is a play on the world "fishing," substituting the "ph" in hone of the hacker/phreaker subculture.

e. Credit card companies and banks have both spent a significant amount of time and resources on developing awareness campaigns, even going as far as to inform customers that they will never request personal information via e-mail.

IV. Anti-Identity Theft Legislation

A. Over the last 12 years there have been an increasing number of legislative acts drafted by Congress.

B. Identity Theft and Assumption Deterrence Act of 1998

1. Made identity theft/fraud a crime against a person.
2. Made it a federal crime to steal an individual's identification information, to include their name, social security number, date of birth, driver's license number, or any other individual identifying piece of information.
3. Established a reporting clearinghouse to assist victims.
    a. The Federal Trade Commission (FTC) is responsible for housing this information.

C. The Fair and Accurate Credit Transaction Act of 2003

1. Provided a variety of means to protect potential identity theft victims, as well as provided a means of assisting victims with repairing their credit.
2. Notable features of the act:
    a. Required merchants to remove a consumer's credit card information from their receipts (allowing only the last few numbers).
    b. Provided consumers with the ability to obtain a free credit report each year so that they can monitor their credit activity to ensure they have not been victimized.
    c. Provided victims with the ability to work with creditors and credit reporting agencies to remove any entries on their credit report that are the result of identity theft.
    d. Allowed consumers to place a variety of alerts on their credit file.

D. Identity Theft Penalty Enhancement Act of 2004

1. Maintains increased penalties for individuals who engage in identity theft–related activities as a means of furtherance of another crime.
2. Individuals who use their position within a company as a means of obtaining information to be used in an act of identity theft can face increased punishment under this legislation.

E. The above statutes are federal statutes but all states have also passed their own identity theft–related statutes.

F. The federal and state governments have made prosecuting individuals for identity theft much easier.

G. Many states have begun limiting the amounts of personal information that individuals can obtain without a thorough verification process.

V. Responses to Identity Theft

A. Historically, when an individual complained that he or she was a victim of identity theft, the department would merely mail out a victim's statement packet.

1. Two problems with these packets:
    a. It took too much time to receive packet, complete it, and return the

material to the police.
i. Identity thief would be long gone.
b. Victims could not begin repairing their credit until they had received an official copy of their complaint filed with the police.

B. Many law enforcement agencies today require officers to take timely reports of incidents related to identity theft and make these reports available as soon as possible so that the victim can start repairing his or her credit.
C. Many departments now maintain divisions to investigate fraud and identity theft.
D. Things that can make it difficult to investigate identity theft:
1. Law enforcement agencies can run into some difficulty when dealing with credit card companies and banks when trying to solve identity theft cases that can result in an inability to close the case.
2. Investigating identity theft can also be complicated by the fact that the crime may involve a combination of physical-world techniques and Internet-based techniques.
3. Some law enforcement departments cannot maintain trained personnel to handle these investigations because they cannot afford proper equipment and training.
E. Many feel that the key to controlling identity theft is by focusing more on a proactive approach through education and awareness.
1. Involves speaking to civilian groups.
2. Allowing citizens to gain a better understanding of the dynamics of identity theft.
3. It is recommended that an individual do the following to prevent falling victim to identity theft:
a. Do not give out personal information like a social security or bank account numbers over the phone.
b. Delete e-mails asking for banking information to help someone who is in need of assistance.
c. Shred all papers containing social security numbers, names, addresses, and similar information before throwing them into the trash.
d. Be careful with credit card receipts and carbons. Destroy the receipts and trash them at another location.
F. Corporations are now beginning to provide their own protections against identity theft.
VI. Conclusion

Key Terms

Carding: All forms of identity theft related to the theft of a victim's credit card.

Fair and Accurate Credit Transactions Act of 2003: Act that provided a variety of means to protect potential identity theft victims, as well as a means of assisting victims to with repairing their credit.

Identity Theft: Generally defined as the theft of someone's identity through the use of some form of personal identifying information, with the information being used for some fraudulent activity.

Identity Theft and Assumption Deterrence Act of 1998: Act that made identity theft/fraud a crime against a person and established a reporting clearing house to assist victims.

Identity Theft Penalty Enhancement Act of 2004: Act that maintains increased penalties for individuals who engage in identity theft-related activities as a means to further another crime and for those individuals who use their position within a company as a mean of obtaining information to be used in an act of identity theft.

Packet Sniffing: Program that allows users to intercept data while it is en route to a website.

Phishing: A process whereby an identity thief will attempt to get a potential victim to provide him or her with the personal information needed to engage in identity theft.

Skimming: The use of a small, often handheld, device that can store several hundred credit card numbers.

Virtual Identity Theft: the theft of someone's online identity.