Computer Forensic
Evidence Collection and Management

Chapter 4

Computer, Internet, and Electronic Crimes

Chapter Objectives

- Understand scams and how scam artist work
- Become familiar with the crime of identity theft
- Look at the issue of Internet fraud
- See how scams and identity theft are closely related
- Identify methods and techniques to obtain evidence from Internet and Web resources
- Look at issues of child molestation and predators who are using the Web
- Recognize the resources for identifying evidence stored on business and personal computer assets
- Learn the technical and legal terms relating to scams, fraud, and identity theft

Introduction

- The computer forensic investigator must understand the environment where crimes and committed. The internet and the computer-networking environment are a complex subject. The investigators must understand the complex issues relating to personal computer-user safety and security.
- Broad spectrums of network-oriented threats are prevalent today. These include criminal groups, foreign intelligence services, terrorists, hackers, phishes, spammers, and malware authors.
- One of the most prevalent security issues today is identity theft.
- A pervasive threat to network users is the scam artist.
- Another issue concerns children and their ability to access Internet network sites that could impact the family's safety.

Scam and Scam Artists

- Scam artists use Dumpster diving, mail theft, and lost/stolen wallets to commit their crimes. These criminals are also using other techniques to defraud the general public.
- Two groups of individuals that pose serious threats to network users are:
  - Phishers: execute phishing scams in an attempt to steal identities or information for monetary gain.
  - Spammers: distribute unsolicited e-mail with hidden or false information in order to sell products, conduct phishing scams, distribute malware or attack organizations.
- The following are samples of potential scammers "tools":

Free Credit reports

Many of the "free credit report" e-mails received are scams. Either the scammer is trying to identify the Social Security number or will be billing later with a service charge.

Scam and Scam Artists (cont.)

Free Prizes

Users often receive either a phone call or e-mail offering a free gift or prize and asking to just send credit card information to take care of shipping and handling.
Free means free, which means there should be no charge. Consider this scam might be a group sending out a cheap gift in exchange for finding a 'live" phone number or e-mail address.
Responding may result in hundreds of spams or telemarketing calls.

Pyramid Schemes and Chain Letters

- There are many email chain letters/pyramid schemes. They can says:
  - Bill Gates is testing a new e-mail-tracking and wants your help. Forward the e-mail to friends and Microsoft will pay $__ for each person that receives it.
  - You will get gift or money from each person who comes after you.
  - Follow the simple instructions below and your financial dream will come true.
- *Do not respond or forward these e-mails.* Any email that asks a user to forward it to friends is a possible scam. Look for the letters "fw" at the beginning of the addressee.

Scam and Scam Artists (cont.)

Questionnaires

- Questionnaires seem to arrive daily in the mail These include questions that help the person sending it find out birth dates, passwords, and even blatantly may ask for a Social Security number.
- Do not answer these, even with false information. Answering lets the other parties know that they have reached a “live person and may eventually give away compromising information.
- *Note: providing incorrect information may actually be someone else’s real information.*

Job Advertisements

- Another opportunity to get scammed involves answering job advertisements.
- Do not place a Social Security number or date of birth on resumes sent out for jobs. Recently there have been scams involving Internet job Web sites (for instance, Monster.com) and newspaper want ads.
- *Under no circumstances should an application provide a Social Security number to a human resources person found through a newspaper add or an Internet ad prior to an actual interview or prior to authentication both the company and the person asking for the information.*

Scam and Scam Artists (cont.)

Work-at-Home

- Advertisement on television and the Web show people making millions working at home. An application would be required to start this work-at-home job. As one probably suspects by now, the application will ask for many personal details including a Social Security number, bank account number, and date of birth. This is good information to initiate an identify theft and the intent is probably fraud.

Charities

- Telephone scams can involve solicitations from various charities. Do not provide credit card information over the telephone.
- Scammers may take advantage of the new "do not call lists" being compile by state governments. No one from the state will be calling consumers asking if they want to be included on the "do not call lists," nor will theses lists require a consumer to provide a Social Security number via telephone.
- *People who do contribute to charities should determine the percentage of the funds that actually go to "legitimate" charities.*

Scam and Scam Artists (cont.)

Check cashing

- There are a number of schemes involving check cashing from ‘firms” base in foreign countries.
- Basically, checks are receive from scammers. These checks would be deposited in the personal accounts of work-at-home victims. These victims would then write checks from thee accounts. The original checks received from the scammers would be worthless.

Scam Baiting

- It is the practice of eliciting attention form the perpetrator of a scam by feigning interest in whatever bogus deal is offered. The scam baiter pretend to be duped, with the intention of making the perpetrators waste time and/or money, and exposing them to public ridicule. Scam baiters may involve the scammers in a long correspondence or encourage them to travel seeking a payoff. This activity will require someone with a high level of technical expertise and experience.

Resources

- The ScamBusters Website is an excellent resource to get information on the latest Internet scams. Most scams, by phone or e-mail, ask the user to provide either credit card account information or a Social Security number.
- Computer forensic investigators must keep current on the latest scams and frauds. Scammers have the advantage and are usually one step ahead or the authorities, however investigators can take advantage of the situation by proactively surfing Web sites for new scams.

Activities That Initiate Personal Asset Crimes

- The best way to avoid scams, fraud, theft, and identity theft is to exercise caution and guar personal information that applies to personal financial assets. Awareness and education are the key.

- The following questions relate to protecting personal information and can be used to prompt a victim to provide an answer of some investigative value:
  - Has the victim provided a Social Security number, birth date, back account number, driver's license number, or credit card number to anyone recently?
  - Has the victim received any telephone calls or e-mail asking fore personal information?
  - Does the victim use a mailbox for paying bills?
  - Has the victim received application for credit cards, catalogs, contests, work-at-home or moneymaking opportunities?
  - Does the victim post logins and passwords in a conspicuous location?
  - Has the victim responded to any requests for information over the internet?

- Tips: Protection techniques
  - Beware of imposters
  - Do not provide a credit card number unless you are actually purchasing something
  - Keep Social Security numbers confidential
  - Keep personal mail safe
  - Memorize computer passwords and PIN numbers
  - Practice safe Internet usage
  - Remove entries form credit marketing lists
  - Secure personal data

Identity theft

- Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain.
- Besides mail theft, dumpster driving, and lost/stolen wallets, criminals are stealing information by overheating conversations made on cell phones, from faxes and e-mails, by hacking into computers, from telephone and e-mail scams, and even from careless online shopping and banking.
- In many cases, a victim's losses may include not only out-of-pocket financial losses, but substantial additional financial costs associated with trying to restore the individual's reputation in the community and correcting erroneous information for which the criminal is responsible.
- With enough identifying information about an individual, a criminal can take over that individual's identity to conduct a wide range of crimes.
- For example, false applications for loans and credit cards, fraudulent withdrawals from bank accounts, fraudulent use of telephone calling cards, or obtaining other goods or privileges that the criminal might be denied if a real name was used.
- The criminal might take steps to ensure that bill for the falsely obtained credit cards, or bank statements showing the unauthorized withdrawals, are sent to an address other than the victim's. The victim may not become aware of what is happening until the criminal has already inflicted substantial damage on the victim's assets, credit, and reputation.

Identity theft (cont.)

Avoid Becoming a Victim of Identify Theft

- To reduce or minimize the risk of becoming a victim of identity theft or fraud, there are some basic steps an individual can take.
- Be careful about giving out personal information to others unless there is a reason to trust them, regardless of location.
  - Start by adopting a “need to know” approach to personal data.
  - Individuals should restrict the amount of information printed on personal bank checks.
  - Do not routinely provide personal data to people who may not need that information.
  - When travelling, have personal mail held at the local post office, or ask someone you know well and trust, such as a family member, friend, or neighbor, to collect and hold your mail while you are away.
  - Check financial information regularly, and look for what should and what should be there.
  - Unauthorized debits or charges against financial accounts can occur if someone has gotten personal financial data.
  - It is possible for a skimmer to be used on an ATM to capture confidential information. Be wary of odd-looking ATM card readers, as they might be skimmers devices.
  - If someone has managed to get access to personal mail or other data, it will be necessary to take immediate action.
  - Maintain careful records of personal banking and financial accounts.
  - The latest technique used by cyber-thieves is to use the wireless network to steal information from personal computers.
  - Wireless users must change the default logon/password and initiate the security protection attributes of the laptop and personal digital assistant.
  - Generally not associated with Internet fraud and identity theft is the transmission of documents over the fax machines. There is a possibility that transmissions from fax machines could be intercepted by some technique and copied without the user's knowledge

Victims of Identity Theft

Victims of identity theft or fraud should act immediately to minimize the damage and impact on personal funds and financial accounts, as well as personal reputation.

Contacts

- Contact all creditors where name or other identifying data has been fraudulently used.
- Contact all financial institutions where an identity thief has taken covered over a personal account or accounts that have been created in someone's name but without his or her knowledge

Credit Report Agencies

- Consumer suspecting a crime can call the fraud units of the three principal credit reporting companies.
- They are:
  - *Equifax: www.equifax.com*
  - *Experian: www.experian.com*
  - *Trans Union: www.tuc.com*

Victims of Identity Theft (cont.)

Federal Deposit Insurance Corporation (FDIC)

- The FDIC's Consumer Response Center has responsibility for investigating all types of consumer complaints about FDIC-supervised institutions and for responding to inquiries about consumer laws and regulation and banking practices. The FDIC staff can provide an avenue for efficient and effective resolution of consumer complaints or inquiries.

Check-Verification Companies

- If clients have checks stolen or bank accounts set up by an identity thief, contact the major check-verification services. In particular, where a particular merchant has received a stolen check, contact the merchant's verification company.
- These might include:
  - *Check rite:* www.checkrite.com
  - *CrossCheck:* www.crosscheck.com
  - *Equifax:* www.equifax.com
  - *National Processing Co. (NPC):* www.npc.net
  - *TeleCheck:* www.telecheck.com

Internet Fraud

Fraud is a deception deliberately practice I order to secure unfair or unlawful gain. How can the Web user discern whether the offer is valid or a fraud? First, if the offer smells fishy and sounds too good to be true, it probably is a fraud.

Internet Fraud Tips

- The investigator can research the dealer or vendor. If the seller or charity is unfamiliar, check with the state or local consumer protection agency and the Better Business Bureau. Also check with the Secretary of State for incorporations.
  - Look for promises of easy money. It is probably a scam
  - Beware of pressure tactics for a quick answer. Legitimate companies and charities will be happy to provide time to make a decision.
  - Be cautions about unsolicited e-mails. They are often fraudulent.
  - Be aware of imposters.
  - Guard personal information. Do not provide a credit card or bank account number unless you are actually paying for something.
  - Beware of "dangerous" downloads. Only download program from known and trusted Web sites.
  - Credit cards are the safest way to pay for online purchases because **consumers** can dispute the charges if they never get the
  - goods or services or the offer was misrepresented.

Internet Fraud (cont.)

New Solutions

- Bank of America's online customer have a new way to help prevent fraud and identity theft with the launch of an industry-leading protection service with its online banking. Anew free service, called Sitekey™, allows customers to pick one of thousands of images, write a brief phrase, and select three challenge questions. The customer and the bank can pass that information securely back and forth to confirm each other's identity.

Internet Fraud Statistics

- Statistics have been developed that show the percentage of frauds for various scams initiated over the Internet. The top ten frauds identified by the National Fraud Information Center are as follows:

Type of Fraud	*Percent*
Online auctions	*51*
General merchandize	*19*
Phishing	*9*
Information/adult services	*3*
Lotteries/lottery clubs	*2*
Fake check scams	*2*
Computer equipment/software	*1*
Fake escrow services	*1*
Internet access services	*1*

Combating Identity Theft and Fraud

A number of government and private organization have information about various aspects of identify theft and fraud: how it can occur, what can get done about it and how to guard personal privacy.

Government Contacts

- Consumer.gov: www.consumer.gove
- FBI: www.fbi.gove
- Federal Deposit Insurance Corporation: www.fdic.gov
- Federal Trade Commission: www.ftc.gov
- United States Postal Inspection Services: www.usps.com/postalinspector
- United States Secret Service: www.secretservice.gov/index.shtml

Nongovernment Contacts

- American Association of Retired Persons (AARP): www.aarp.org
- Better Business Bureau: www.bbb.org
- Center for Democracy and Technology: www.cdt.org
- National Association of Attorneys General (NAAG): www.naag.org
- National Consumers League: www.nclnet.org
- National Fraud Information Center: www.fraud.org
- Privacy Rights Clearinghouse: www.privacyrights.org
- Chamber of Commerce: www.uschamber.com/default

Combating Identity Theft and Fraud (cont.)

Awareness and Education

Identity theft and fraud can be avoided or minimized if the population becomes aware of the emormity of the problem.

Education and awareness are must-have attributes. It is obvious criminals are just waiting to take advantage of anyone who lets his or her guard down.

Using the Internet for Investigation

- The Internet provides a valuable tool for the forensic investigator. Learning the techniques for surfing can provide surprising amount of leads during an investigation.
- Cyber-thieves can use information provided over chat rooms, blogs, and e-mail to compromise the security of naïve network users. There is no reason that the law enforcement cannot benefit from the same resources.

Exploiting Children on the Web

A survey by the National Center for Missing and Exploited Children and Cox Communications revealed that 42 percent of parents do not review the content of what their teenagers read or type in chat rooms or via instant messaging.
Studies reveal that many parents are not involved in their children's Internet habits and behaviors. Children may impact the security and safety of the entire family due to their inexperience and naiveté.

Child Predators

Child molestation, trafficking, abuse, and child pornography cases are the rise. Compute forensic investigator and examiners must learn the tactics of these predators and identify techniques to develop evidence that will hold p in court.

A pedophile is an adult whose primary sexual interest is in children.

There are a number of attributes and objectives that are common to child sexual predators:

- *Prey on the innocence of a child*
- *Feed on the thrill of violating a child's trust*
- *Find the perfect game and capture their victim*
- *Spend time watching children, talking to them, evaluating their mind frame*
- *Dig deep into the psyche of a child*
- *Watch a child's every move and observe his or her feelings*
- *Play the game slowly*
- *Befriend the child, play with him or her, and get to know him or her*
- *See a chance to advance the game, and take each calculated move as it comes*
- *Gain the child's trust, reinforce it, and them eventually violate it.*

Exploiting Children on the Web (cont.)

Child Predators on the Internet

While the computer age has opened a whole new world for children to explore and learn form, the information superhighway also has a dark side. Just as they prey on the land, pedophiles lurk on the Internet waiting to lure innocent children into their web of deviance, as they look for their next victim.

The deviates meet other s who claim children for their victims; they share stories, pictures, and encourage each other along the way.

Child predators are cons and their goals are as varied as their egos.

Investigating child-predator crimes is difficult for law enforcement since everyone has a computer at his or her residence, school, church, fast-food store, book store, and often children are unsupervised when they are using these computers.

There are a set of rules to reduce a child's risk of exploitation:

- *NEVER allow children to give out any personal information such as last name, address, telephone number, parent's first or list names, work phone numbers, name of employer's or business names, or the school name or location.*
- *NEVER let a child send anyone a photograph or any other items via the Internet without obtaining the parent's permission*
- *NEVER let children respond to any messages that make them uncomfortable. Do not allow someone to say mean or naughty things.*
- *NEVER let he child get together or meet with anyone met online*

Exploiting Children on the Web (cont.)

Child Predators and Privacy Laws

Megan's Law mandates that every state develop a procedure for notifying residents of sex offenders residing there. The act requires the states to register sex offenders convicted of sex crimes against children.

The Unites States Children's Online Privacy Protection Act of 1998 (COPPA), applies to the online collection of personal information by persons or entities under U.S. jurisdiction from children under 13.

Child Predators Investigation

NetSmartz and the Internet Crimes Against Children (ICAC) Task Force Program have developed age-appropriate presentations for grades K-2, 3-6, middle and high school, law enforcement, parents, and communities.

The U.S Congress established the Exploited Child Unite (ECU). This serves as a technical and informational resources for law enforcement. Investigating child sexual-exploitation cases may require specialized technical skills outside the scope of usual investigation methods.

The technical assistance services available from the ECU are listed below:

- *Child Victim-Identification Project*
- *CyberTipline historical searches*
- *Internet searches*
- *Internet service providers (ISP) contacts*
- *Law-enforcement contacts*
- *Public-records database searches*
- *Technical expertise.*