Chapter 6

Understanding the Computer-Networking Environment: Beware of the Scam Artists, Bullies, and Lurking Predators!

To be a good computer forensics investigator, you must have sufficient knowledge of existing cybercrime laws and criminal procedure. You must also be familiar with existing technology, computer crimes, and the perpetrators who commit these crimes. Technology is constantly evolving, however, and so are the criminals who commit these crimes. Consequently, as an investigator it is imperative that you stay current in your field, especially with respect to the computer-networking environment in which criminals operate and the types of crimes that criminals are perpetrating within this environment. This chapter explicitly focuses on current online scams, identity theft, cyberbullying, and sexual predators.

Scams and Scam Artists

This section covers a number of different scams and the approaches that a scam artist might use to steal an individual's personal information with the intent to commit fraud. Most scams arrive in the form of unsolicited e-mails, text messages, and phone calls from unknown individuals. The techniques used by scam artists to steal the personal information include, but are not limited to, the following strategies:

- *Dumpster diving.* Criminals may go through the prospective victim's garbage looking for the victim's personal and financial information (e.g., Social Security number, credit card information). Many individuals routinely discard sensitive documents and financial information without shredding them first. One can also dumpster dive at financial institutions. For example, Jonah

Hanneke Nelson stole more than 500 identities by dumpster diving behind banks and other businesses and retrieving sensitive material and blank checks. Sometimes information that is retrieved from the dumpster of a company can be used to obtain sensitive information from employees of that company. For example, the Phonemasters, a criminal group, tricked employees of companies (e.g., AT&T, MCI, Sprint, Equifax) into revealing their usernames and passwords by using the materials they had extracted from the dumpster, which included old phone and technical manuals for the computer systems of these companies.[1]

- *Shoulder surfing.* Criminals may watch prospective victims at automatic teller machines (ATMs) to "steal" the personal identification number (PIN) that each victim enters into the machine. Usually, after watching someone enter the PIN, the offender either distracts the victim and steals the victim's debit or credit card or pickpockets the victim after he or she leaves the ATM.
- *Skimming device.* A skimming device reads the magnetic strip on credit and debit cards. These devices have been surreptitiously placed on ATMs to collect this information unbeknownst to users. Some criminals have handheld devices they use to swipe unsuspecting users' cards so as to steal their data. In one case, employees of the Cheesecake Factory used card-skimming devices to steal the credit card numbers of restaurant customers.[2]
- *Stealing a prospective victim's wallet or breaking into the home or car of the prospective victim to steal documents that contain the victim's personal information.* A recent example of this kind of scam occurred on June 15, 2010, when a famous English playwright, Alan Bennett, had his wallet stolen by thieves. The thieves—two women and one man—threw ice cream at his coat and pretended to clean it up. By distracting him in such a manner, they managed to steal Bennett's wallet, which he claimed contained 1500 pounds.[3]

Various scams that have been used to steal money, financial data, and/or personal information are described next.

Online Auction Scams

In one type of online scam with auction fraud (covered in Chapter 5), the scam artist provides overpayment for an item that is being auctioned. The buyer sends too much money for the item (probably a few hundred dollars over the price of the item) via international money order. The seller, in an effort to maintain a good business relationship with buyer, sends the excess money back to the buyer after the bank has accepted the money order. Several weeks later, the seller is informed by the bank that the money order was a forgery. Consequently, the seller loses both the few hundred dollars refunded to the buyer and the goods that were sold.

Online Rental and Real Estate Scams

According to the website of the Federal Bureau of Investigation (FBI), recent online scams have included rental properties and real estate (**rental and real estate scam**).[4] The technique used in such cases is similar to the scam mentioned previously involving auction sites. The scammer, who disguises himself or herself as an interested buyer or renter, agrees with the seller or landlord on a specific price. The offender then sends the seller or landlord a check for the amount agreed upon. At this point, the scammer backs out of the deal and asks for a full refund. After sending the scammer the amount refunded, the seller or landlord finds out that the check was counterfeit. Not only has the individual lost the money he or she forwarded to the scammers, but now the person has to pay the bank that same amount because the check was counterfeit.

Online Dating Scams

Online **dating scams** are conducted in more or less the same manner by most offenders. The offender poses as an attractive person (and shows the victim pictures to illustrate his or her supposed appearance) on an online dating site and develops an online relationship with the victim. After courting the victim for a few months, the offender informs the victim that he or she must travel abroad for business. While abroad, the offender notifies the victim that an unexpected tragedy has occurred; either the person is the victim of a street crime (e.g., robbery), is detained by authorities, or cannot pay a hotel or hospital bill. The offender then asks the victim for financial assistance. Sometimes the offender will come up with more scenarios that require further financial assistance from the victim. Either way, after one or more payments are made by the victim, the offender vanishes and the victim never hears from him or her again.[5]

Online Lottery Scams

Other ways to fraudulently solicit money from a victim include claiming that the victim won a prize—typically a foreign lottery. The **lottery scam** artist informs the victim that he or she must supply the lottery agency with a bank account number and pay certain fees and taxes in advance to obtain the winnings. The victim is further informed that he or she must take these steps immediately because the deadline to claim the prize will expire soon. After the victim provides the bank account number and money to the "foreign lottery agency," the person never hears from the "agency" again. The bank account for which the victim provided access information will probably be emptied as well.

Participation in a foreign lottery is a violation of U.S. law. Accordingly, the victim is unlikely to report the fraud. Even if a victim does report the crime to the authorities, the money the victim sent to the scam artist cannot be retrieved because he or she has engaged in unlawful activity.[6] An example of a lottery scam, retrieved from the author's own inbox is included in the nearby box. Notice the errors in the original text—such spelling and grammatical errors are characteristic of scams.

Lottery Scam

From: 2010 WORLD CUP AWARD <claimingza@sify.com>
Subject: Call Urgently on +27 839470181
To: xxxxx@xxxxxx.com
Date: Wednesday, June 9, 2010, 7:53 AM

WINNING NOTIFICATION
(2010 WORLD CUP LOTTERY AWARD)

We happily announce to you the draw of South African 2010 World Cup Bid Lottery Award International programs held in U.K your "email address" was attached to ticket number; B9665 75604546 199 serial number 97560 This batch draws the lucky numbers as follows 60/84/27/17/36, bonus number 2, which consequently won the lottery in the second category. Congratulations your email is among the three lucky winning that won **$2,000,000.00{Two million United State Dollars}**in the just concluded south Africa world cup bid 2010 promotion sponsored by Coca-Cola British American tobacco companies south Africa.

COMPLETE THIS INFORMATIONS BELOW:
NAME:.....
ADDRESS:.....
NATIONALITY:.....
SEX:.....
AGE:.....
PRIVATE PHONE/MOBILE NO
PRIVATE FAX NO:.....
OCCUPATION:.....
BATCH/WINNING 60/84/27/17/36

The lottery program took place to promote South African 2010 world cup award.

His contact details are as follows . . .
CONTCAT YOUR CLAIMING AGENT:
Contact: MR.STEPHEN VALE
TEL: + 27-839470181
EMAIL: claimingza@sify.com

Yours Faithfully,
Management.
JOHN CLARK

Charity Scams

Many e-mails are purportedly sent on behalf of charities in the aftermath of a disaster. This rush to capitalize on people's desire to help others in distress happened after the terrorist attacks in the United States on September 11, 2001; the tsunami in Indonesia in December 2004; Hurricane Katrina in September 2005; and the earthquake in Haiti in 2010; to name but a few. For instance, following the 2004 tsunami and Hurricane Katrina, numerous fake websites were set up asking for donations from unsuspecting individuals via PayPal, credit card, or bank account, thereby misdirecting funds from legitimate disaster relief efforts. Additionally, in the immediate aftermath of the earthquake in Haiti, numerous fake e-mails and messages on social networking sites (such as Facebook, MySpace, and Twitter) were sent soliciting funds.

Some scams even claimed to be from legitimate organizations, such as the United Nations International Children's Emergency Fund (UNICEF). Here is how the scam worked: An individual would receive an e-mail that appeared to be from UNICEF. When the individual would click on the link provided in the e-mail, he or she would be diverted to an official-looking UNICEF Web page. This page would ask for personal information (e.g., name, home address, and Social Security number), credit card information, and bank account information. The information provided by the victim would subsequently be used by the offender to commit other crimes (e.g., identify theft).

Another form of scam was developed to divert funds that were obtained from text message short codes. For example, a legitimate short code set up for donations in the aftermath of the Haiti earthquake was "90999". If an individual typed the word "Haiti" and sent the message to this code, $10 was donated to the Red Cross in the United States. Scammers created a text message number to which donors could send money that mimicked the legitimate one. Specifically, variations of the legitimate "90999" code were provided by scam artists (e.g., "99099") to retrieve some of the money that was being donated to Red Cross for Haiti. Indeed, many such false codes were provided following the earthquake in Haiti. Both the FBI and the Federal Trade Commission (FTC) issued warnings to the public soon after the earthquake concerning which charities were legitimate. The FBI and FTC also warned the public about e-mail and text message charity scams.

Government E-mail Scams

There are several ways in which scammers try to steal personal information from an individual's computer. One of the most common ways is the distribution of malicious software through what appear to be legitimate **government e-mails**—at least on the surface. For instance, e-mails have been distributed claiming to be from the FBI, some of which come with an attachment. The e-mail in the nearby box was found among many similar spam emails in the author's inbox; it included an attachment titled "FBI Report.txt". One should be extremely wary when opening attachments to suspicious e-mails as they (more often than not) carry a malicious payload, which is intended to download spyware or keylogging software to retrieve information from a user's computer.

Fake FBI E-mail

From: FBI OFFICE <drdwilson@btconnect.com>
Subject: REPLY NOW
To: xxxxxxxx@xxxxxxx.com
Date: Wednesday, June 23, 2010, 2:37 AM

See attachment below for a current report on our investigation. You are advised to Contact me asap for further clarification. This has to be cleared! You are warned!

In reality, the FBI always uses its official e-mail addresses for communications. Besides, an FBI official would not send such a communication if a matter was truly urgent: It is much more likely that an FBI agent would visit the individual in person. In these types of scams, the e-mail addresses of the supposed FBI officials are typically from free website service accounts, such as Hotmail, Yahoo, or Gmail. In the case of the "Example of Nigerian Scam" e-mail, the message was sent from a communications carrier in the United Kingdom known as BT (British Telecommunications).

One example of this kind of scam can be seen in the e-mails that were distributed on behalf of the FBI purportedly claiming to include an Intelligence Bulletin concerning "New Patterns in Al-Qaeda Financing." This e-mail was accompanied by an attachment of the supposed bulletin, which was actually an executable file ("bulletin.exe") that contained malicious software. Upon being opened, a malicious payload was downloaded that was designed to steal information from the user's computer.[7] Another e-mail masquerading as an official urgent message from the Department of Homeland Security (DHS) and the FBI was distributed that claimed to contain a recording of a speech Osama bin Laden gave directed at Europe.[8] This email also had an executable file ("audio.exe") attached to it; as with the "bulletin" attachment, the attachment contained malicious software designed to steal the user's personal information.

As a general rule, e-mails with attachments from unknown senders should not be opened.

Nigerian Scams

The **Nigerian scam** is also known as the "419 scam," named after the section of the Nigerian criminal code that this scam violates.[9] Many variations of the Nigerian scam exist. Some claim that the victim has received an inheritance from a long-lost relative from Nigeria. Others, which constitute the majority of this type of scam, involve e-mails sent by individuals fraudulently claiming to be government, business, or banking officials.

In the typical Nigerian scam, a victim is contacted by someone impersonating one of the previously mentioned officials. This official informs the victim that he or she has been

Example of Nigerian Scam

From: Mrs. Debbie Anderson <nelson_welter@secreatrias.com>
Subject: Stop Contacting Scam Alert. . . . !
To: xxxxx@xxxxxxx.com
Date: Tuesday, June 8, 2010, 5:55 AM
Attn: My Dear Good Friend

I am Mrs. Debbie Anderson, I am a US citizen, 48 years Old. I reside here in New Braunfels Texas 78132. My residential address is as follows. 108 Crockett Court. Apt 303, New Braunfels Texas, United States, am thinking of relocating since I am now rich. I am one of those that took part in the Compensation in Nigeria many years ago and they refused to pay me, I had paid over $20,000 while in the US, trying to get my payment all to no avail.

So I decided to travel down to Nigeria with all my compensation documents, And I was directed to meet Mr Michael Bolts, who is the member of COMPENSATION AWARD COMMITTEE, and I contacted him and he explained everything to me. He said whoever is contacting us through emails are fake.

He took me to the paying bank for the claim of my Compensation payment. Right now I am the most happiest woman on earth because I have received my compensation funds of $1,600,000.00 Moreover, Mr Nelson Oboh, showed me the full information of those that are yet to receive their payments and I saw your name as one of the beneficiaries, and your email address, that is why I decided to email you to stop dealing with those people, they are not with your fund, they are only making money out of you. I will advise you to contact Mr Nelson Oboh.

You have to contact him directly on this information below.

COMPENSATION AWARD HOUSE
Name : Nelson Oboh
Email: nelson_oboh@secretarias.com
Phone: +234-808-286-2330

You really have to stop dealing with those people that are contacting you and telling you that your fund is with them, it is not in anyway with them, they are only taking advantage of you and they will dry you up until you have nothing.

The only money I paid after I met Mr Nelson Oboh was just $95 for the paper works, take note of that.

Once again stop contacting those people, I will advise you to contact Mr Nelson Oboh so that he can help you to Deliver your fund instead of dealing with those liars that will be turning you around asking for different kind of money to complete your transaction.

Thank You and Be Blessed.
Mrs. Debbie Anderson.

selected to partake in the sharing of a percentage of millions of dollars. To obtain the money, the victim is required to allow the "official" to deposit these millions into the individual's bank account. To do so, the victim is required to provide the "official" with all of the relevant personal and banking information to complete the transaction. The victim is also required to pay certain legal fees, taxes, and bribes to government officials. Of course, the victim is reassured by the "official" that the money provided for the fees, taxes and bribes will be paid back in full. The victim, of course, never sees any money from this scheme, nor will he or she ever get back the money given to the scammers for the fictitious fees, taxes, and bribes. Additionally, if the victim's bank account had any money in it, the scammer will have withdrawn all of it.

Other victims, thinking that they are dealing with legitimate government, business, or bank officials, have been lured to travel to Nigeria to supposedly receive their funds.[10] Before they set out for Nigeria, victims are purposely told that they do not need a visa to enter the country. Entering the country without a visa, however, is illegal in Nigeria. As such, the scammers use the fact that the victim entered the country illegally as leverage to compel the victim into paying the scammers the money that they are demanding. This fraud does not only result in financial loss to the victim; some individuals who have traveled to Nigeria in pursuit of the money purportedly offered to them have died or gone missing. As certain websites have reported, an American was murdered while pursuing such a scam in Lagos, Nigeria, in 1995.[11]

E-mails claiming to need the target's assistance to receive money from Nigeria should be sent to the following e-mail address of the FTC: spam@uce.gov.

Work-at-Home Scams

Many fraudulent advertisements exist concerning work-at-home opportunities. The individuals who are usually victims of **work-at-home scams** are stay-at-home mothers, disabled individuals, and persons who are unemployed and are desperately seeking some form of income. Most offers contain exaggerated claims of potential earnings such as "Make $7000 a week working part-time; no experience required" or "Make $1000 in as little as 4 hours; no experience needed." To convince victims of the scheme's legitimacy, scammers will create false websites containing news articles claiming that such opportunities are real and that many have benefited from them. Either this scam will advertise opportunities for individuals to create their own home business or it will advertise positions in which employers are seeking individuals who can process e-mails, transfer funds, assemble products, reship products, or process payments (to name a few bogus jobs).

When the scam focuses on establishing a home business, the victim is required to pay an advance fee—usually a few hundred dollars—for the materials needed to set up this business. The materials the victim actually receives are useless, meaning the victim has been scammed out of the money paid for the advance fee.

When the scam focuses on working at home for an invisible employer, either the victim never receives money for the job performed or receives very little money in return. Either

way, the person never receives the large sum of money originally promised as compensation. At times, those offering work-at-home jobs solicit individuals to engage in illegal activities by having the victims receive and cash fraudulent checks, transfer the offender's illegally obtained funds, or receive and ship stolen merchandise to the offender.[12]

Virus Protection Scams

Users browsing the Internet may receive pop-up security warnings falsely informing them that their computer has been infected with numerous computer viruses.[13] This type of scam is known as **scareware**, and the goal is to persuade the user to buy fake software and/or to download malicious software on the user's computer—a type of fraud known as a **virus protection scam**.

Many different types of scareware or rogue antivirus software are available online. One very well-known scareware program is XP Protection Center, which may be downloaded on a user's computer through fake, malicious websites and Trojan horses. XP Protection Center was designed to hijack certain websites and redirect users to a website where the program could be purchased.

This type of scareware is also designed to bombard the user's computer with repeated security messages warning of an infection of the system by multiple viruses and malware. If a user is redirected to a website that provides security warnings claiming that the user's computer has multiple infections, the user should not click on the "X" on the upper-right hand corner of the Web page, nor should he or she click on a box on the page that says "No Thanks" to exit the program. Taking either of these actions may cause execution of malicious code. Instead, the user should close his or her browser by clicking on the "File" tab, and then choosing "Exit." The alternative is to right-click on the program icon on the task bar and then click "Close."

Spammers

Terrorists have been known to secure their communications by sending fake streams of e-mail **spam** to disguise a single targeted message.[14] Spam can be sent via both e-mail and cell phones. Spam can be annoying and time-consuming because it fills up individuals' e-mail accounts with junk e-mail that these individuals have to sort through to distinguish it from their legitimate mail. Spammers tend to distribute unsolicited e-mails with the intent to defraud users by, for example, offering deals on products or services. Most often, the advertised products or services the buyer sends money for are never received. At other times, the products received are of very low quality and value—worth much less than what the victim paid for them.

In recent years, spam has become more dangerous because it includes—more often than not—links in the e-mails that may contain malicious software that can install spyware onto an unsuspecting victim's computer system. Sometimes just opening the e-mail can deliver a malicious payload onto a person's computer. For this reason, if an e-mail is suspected to be of the spam variety, the user should just delete it. Additionally, if

an individual responds to spam, his or her personal information and e-mail address are usually sold to other companies. In turn, the victim is subjected to even more spam.

For the recipient of spam, it can be extremely difficult to distinguish between legitimate advertisements and those masquerading as advertisements. The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act) (codified in 15 U.S.C. 7701, et seq.) was developed to remedy this situation and deal with the growing problem of spam. If a glimpse of the author's inbox is any indication as to its effectiveness, however, this measure has definitely fallen short of its stated purpose.

The CAN-SPAM Act was designed to, among other things, afford the user with the option to opt out of services. Not all spammers, however, have abided by these rules. Most spam includes a message at the bottom of the e-mail that states that an individual opted in to receive certain updates and special offers through a partner website (which is not named). It further states that if an individual believes that he or she has received the e-mail in error or does not wish to receive additional updates in the future, the user should click on a link that is provided and unsubscribe. Sometimes those links contain malicious software. At other times, an individual who attempts to unsubscribe to such e-mails may end up receiving more spam because he or she was tricked into entering the e-mail address in a website that sends the user's information to other spammers.

Phishers

Phishers are known for posing as legitimate companies and government agencies and using misleading or disguised hyperlinks and fake e-mail return addresses to trick Internet users into revealing their personal information. Normally, such e-mails claim that a customer's account information needs to be verified to protect the user against identity theft. To ensure that many individuals reply to the phishing email, the message also warns users that if they do not reply in a timely manner, their accounts will be terminated. Some scam artists have even pretended to be part of the Financial Crimes Enforcement Network (FinCEN); in so doing, they have tricked their victims into providing them with personal information, to be later used by these scam artists to commit other crimes.[15]

In another case, phishers targeted senior victims by creating a phishing scam that involved Social Security benefits.[16] They sent e-mails to senior citizens claiming that if they did not update their information by responding to the e-mail, their accounts would be suspended indefinitely and they would lose their Social Security benefits. Many people responded to the e-mail by sending their personal and financial information to the website the phishers provided, which looked like the authentic Social Security Administration website.

Yet another example of phishing involved fraudulent e-mails sent on behalf of the Internal Revenue Service (IRS) concerning the economic stimulus tax rebate implemented during the administration of President George W. Bush.[17] These messages instructed

recipients of the e-mail to provide direct deposit information so that they would receive the rebate faster. Any personal information sent to the phishers was subsequently stolen and used for other fraudulent purposes.

A more recent phishing scheme also involved the IRS. Specifically, Mikalai Mardakhayeu and his co-conspirators participated in a scheme to defraud taxpayers across the United States out of their income tax refunds by luring them to websites that purportedly offered lower-income taxpayers free tax return preparation and electronic filing services.[18] After the unsuspecting victims uploaded their tax return information, Mardakhayeu and his cohorts altered the information they provided and had the tax refunds sent to bank accounts controlled by them.

As this brief survey suggests, phishing schemes abound. In all cases, however, phishing is a form of identity theft. It seeks to dupe individuals into giving away their personal information and passwords. If an individual's password has been compromised, the offender may use the victim's e-mail account to send requests for money to individuals listed in the victim's address book. Specifically, the offender—posing as the victim—may claim that the individual needs money, immediately. The e-mail might state that the victim was in a terrible accident or stuck in a foreign country without any money and needs financial assistance.

Phishing attacks have also occurred by means of social networking sites. One such example involves Twitter. On January 3, 2009, a message with a link in it was sent out via Twitter, disguised as being from a friend or someone who was allowed to follow the victim's tweets. If the victim clicked on the link, he or she was redirected to another website that looked identical to the official Twitter page. When prompted to enter his or her username and password, the victim typed it in. This information was subsequently stolen by phishers, giving them access to the victim's Twitter account.

Vishing

Vishing (voice phishing) is another well-known type of scam. Vishing can occur via voice or text messages sent to cell phones. In one variant of this scheme, an offender poses as a representative of the victim's bank and notifies the victim that his or her account has been compromised. The offender then provides the victim with a number to call that specifically deals with these issues. When the victim calls the number, an official-sounding recording is heard that instructs the victim to provide the account number and password. Once the account number and password are provided, the call is terminated—and the victim's bank account is quickly emptied.

Pharming

Pharming is a type of scam in which the offender creates a website that looks identical to an authentic website. However, the mirror website carries a malicious payload. According to McLean and Young:

> Pharming uses Trojan horse programs to redirect people to counterfeit banking or e-commerce sites (sometimes called "page hijacking"). The compromised computer or server redirects consumers to fraudulent websites . . . The fraudulent sites are formulated to look like authentic, legitimate sites (and may even include a bogus "secure site" logo indicating that the site is genuine). The site may install spyware or prompt the consumer to enter personal information, including user name and password.[19]

Pharming has occurred primarily with pornographic websites. In addition, pharmers have targeted municipal and government websites.

Identity Theft

Identity theft usually occurs when someone steals an individual's identity by obtaining his or her personal information or by accessing an individual's account with the intention of using it to commit illegal activities. For instance, an employee of the New York State Tax Department stole thousands of taxpayers' identities and made more than $200,000 in fraudulent charges with credit card accounts and lines of credit opened with those identities.[20] In another case, a computer technician stole the identities of more than 150 employees of the Bank of New York Mellon Corporation.[21] He subsequently used these identities to conduct criminal activities, stealing more than $1.1 million from charities, nonprofit organizations, and other related groups. A third case involved a former U.S. military contractor who pleaded guilty to exceeding his authorized access to a computer of the Marine Corps Reserve Center and obtaining and selling the names and Social Security numbers of 17,000 military employees.[22]

Terrorists have also engaged in identity theft for a variety of reasons. In fact, investigations of the terrorist attacks on September 11, 2001, revealed that the terrorists responsible for the attack "repeatedly committed acts of identity theft to advance their destructive goals."[23] Indeed, intelligence has shown that terrorists have obtained genuine

Interesting Fact About Pharmed Websites

Suppose you are searching for the link to Best Buy so that you can buy electronics. You type the phrase "Best Buy" into a search engine, such as Google or Bing. Numerous results are found. To determine if a link has been pharmed, you can move your mouse so that it hovers over the title of the first search result (actually, any search result could be used). If the Web address that shows up is www.bestbuy.com, then this is the legitimate site. In contrast, if the Web address revealed is www.bestby.com, then the website is pharmed. Of course, you can avoid pharmed websites altogether if you know the website you are seeking to access and type its locator correctly into the address browser bar.

passports by using falsified personal identity information and fraudulent supporting documents.[24] Because such documents are issued by the appropriate agency, they are indistinguishable from legitimate passports.[25] For example, an al-Qaeda terrorist cell in Spain used "false passports and travel documents . . . to open bank accounts where money for the mujahidin movement was sent to and from countries such as Pakistan, Afghanistan, etc."[26] A cloak of anonymity is provided to those who steal identities. Thus stolen identities afford terrorists with the opportunity to enter and exit the United States (and other countries) undetected.

Terrorists have also engaged in identity theft by bribing employees of the Department of Motor Vehicles (DMV) into providing them with driver's licenses. For example, the terrorists responsible for the September 11 attacks bribed DMV employees so that they could receive driver's licenses. Indeed, examples abound of corrupt DMV employees illegally providing licenses for a fee. One such case involved an identity theft ring that was caught by counterterrorism investigators.[27] A member of this ring, a Pakistani woman named Shamsha Laiwalla, had provided individuals who came to the United States illegally from Pakistan with driver's licenses, Social Security numbers, and birth certificates. To obtain the driver's licenses, Laiwalla bribed DMV workers. Laiwalla is also suspected of providing some of the proceeds of her illicit gains to finance a Lebanon-based terrorist group known as Hezbollah.

Types of Identity Theft

According to the Berkshire, Massachusetts District Attorney's Office, one's personal information is stolen to commit four major types of crimes:[28]

1. *Financial identity theft.* This occurs when an offender uses a victim's identity to obtain money, goods, or services. For example, an offender may take the following actions:
   - Open up a bank account in the victim's name.
   - Obtain debit and credit cards in the victim's name.
   - Take out mortgage loans in the victim's name.
   - Buy an automobile by taking out a loan in the victim's name.
2. *Criminal identity theft.* With this type of identity theft, an offender poses as the victim to commit a crime or claims to be the victim when apprehended for a crime.
3. *Identity cloning.* This occurs when an offender assumes the identity of the victim in his or her daily life. To do so, the offender usually retrieves duplicates of the victim's driver's license, birth certificate, passport, and other personally identifying records. The offender subsequently takes over all of the victim's existing accounts (e.g., bank, phone).

4. *Business/commercial identity theft.* Using this form of identity theft, offenders use another business' or organization's name to obtain credit, funds, goods, or services.

How Can Someone Steal an Identity?

According to the Congressional testimony of Grant Ashley, even one stolen document can assist someone in taking over a person's identity and using it for fraudulent purposes.[29] Consider the following example: If an offender has the name and date of birth of an individual, he or she can go to bureaus that have open records policies and obtain the birth certificate of the individual. This information can be then used to contact the Social Security Administration and obtain the victim's Social Security number. With a Social Security number, credit reports can be obtained. These credit reports allow the offender to determine two things:

- If the victim has good credit with which the offender can open up accounts and apply for credit cards
- Which bank accounts and credit cards the victim has

Using the information the offender has retrieved from the credit report, he or she can place pretext calls to the victim's bank and obtain the victim's bank account number. This information can subsequently be used for a variety of fraudulent purposes.

Criminals can steal a person's identity in many different ways:

- By stealing the victim's personal information (e.g., Social Security number, home address, bank account numbers where your salary is deposited) from an employer
- By bribing an employee from the human resources department who has access to the aforementioned information
- By stealing your mail (especially pre-approved credit card forms) and filling out a change of address form to divert the victim's mail to the criminal
- By hacking into computer systems and stealing personal information

The last tactic is particularly important to note because it is easily forgotten that individuals may become victims of identity as a result of the theft of their personal information from company or government databases. Most governments and private companies provide users with one solution to identity theft: Protect yourself (by, for example, shredding documents containing personal information before putting them in the garbage). This advice distracts the public from one very important fact: Most of their personal data is stored in remote databases beyond the individuals' control and reach.

Thousands of incidents in which these kinds of databases were breached by criminals have been recorded by the Privacy Rights Clearinghouse. Specifically, this organization's

website details cases of data breaches that have resulted from hacking incidents, theft of data from databases, the theft and loss of computers and related devices that store personal data, accidental disclosure of personal data, and careless discarding of documents containing personal data into trash and dumpsters without shredding them first. Each of these possibilities is explored in further detail here.

Numerous examples exist of theft of data from the databases of government agencies and businesses:[30]

- On April 28, 2009, a hacker illegally accessed a database of the West Virginia State Bar that contained lawyers' identification numbers, home addresses, e-mail addresses, and some of the lawyers' Social Security numbers.
- On March 12, 2009, individuals gained unauthorized access to a U.S. Army database that contained the personal data of approximately 1600 soldiers.
- On January 23, 2009, someone gained unauthorized access to a database of Monster.com (a website where people post résumés and search for employment) that contained the usernames, passwords, names, dates of birth, e-mail addresses, gender, and ethnicity of the users.
- On May 12, 2007, a hacker gained unauthorized access to a computer containing approximately 7300 Social Security numbers, dates of birth, names, home addresses, and phone numbers of the students of Goshen College in Indiana.
- On May 8, 2007, a hacker accessed databases at the University of Missouri that contained the names and Social Security numbers of employees who were former or current students of the campus in Columbia, Missouri.

Laptops and related electronic devices of businesses, military, state, and government agencies have also been stolen:[31]

- On June 10, 2008, the billing records of 2.2 million patients at the University of Utah Hospitals and Clinics were stolen from a vehicle.
- On January 29, 2008, a laptop that an employee of Horizon Blue Cross Blue Shield was taking home with him was stolen. This laptop contained the personal information of more than 300,000 members of the health plan.
- On March 30, 2007, three laptops containing sailors' personal data were stolen from the Navy College Office at the San Diego Naval Station.
- On October 20, 2006, a laptop containing the personal information (names, Social Security numbers, and medical data) of 1600 veterans who received care at the Manhattan Veterans Affairs Medical Center was stolen.
- That same day, a laptop containing 130,500 Social Security numbers was stolen from the Los Angeles County Child Support Services.

Many examples also exist of employees who have lost laptops, flash drives, and other electronic storage devices containing sensitive personal information:[32]

- On May 14, 2010, a laptop was stolen from the Department of Veterans Affairs in Washington, D.C., that contained Social Security numbers and other personal data of more than 600 veterans.
- On March 24, 2009, an employee of Massachusetts General Hospital took records home to do work over the weekend and ended up losing confidential medical records by leaving them on a train.
- On June 5, 2006, an IRS employee lost a laptop that contained fingerprints, Social Security numbers, and other personal data of current employees and job applicants during transit on an airline flight.
- On June 1, 2006, an employee of Miami University lost a computer that contained the personal information of students enrolled in the university between June 2001 and May 2006.
- On January 12, 2006, People's Bank lost a computer tape containing customers' personal information and checking account numbers.

Incidents of exposure of personal data as a result of an employee error or accidental disclosure have also been noted:[33]

- On September 23, 2009, someone observed that the names and Social Security numbers of more than 5000 employees and students of Eastern Kentucky University were posted online. The data remained online for about a year before someone reported that fact and had them taken down.
- On January 30, 2009, the Social Security numbers of current and former employees of the Indiana Department of Administration were accidentally posted on a website for approximately two hours before someone noticed them and had them removed.
- On January 21, 2009, at Missouri State University, e-mails sent soliciting help with language tutoring included, by mistake, an attachment of a spreadsheet with the names and Social Security numbers of international students.
- On August 29, 2008, the personal data (including Social Security numbers) of 16,587 individuals who applied for benefits appeared on two privately owned websites of the Federal Emergency Management Administration (FEMA). FEMA was unsure how long this information was posted online.
- On April 7, 2008, a spreadsheet with a hidden column that contained the Social Security numbers of officers and civilian employees at the Army Acquisition Center was posted on a website for approximately 5 months before it was discovered.

- On March 20, 2008, the voter registration website of the Pennsylvania Department of State was shut down after it was discovered that it allowed anyone visiting the website to view voters' names, dates of birth, political parties, and driver's license numbers.
- On June 1, 2007, the Jax Federal Credit Union accidentally posted client information—Social Security numbers and bank account numbers—online.

Businesses have also carelessly discarded their clients' personal information:[34]

- On April 9, 2010, an individual in Sparks, Nevada, observed that thousands of documents including customers' personal data, credit card information, and signatures had been discarded in dumpsters (without shredding them) by the local Hollywood Video store when it closed.
- On May 6, 2008, news reporters from Channel 8 found Social Security numbers, bank account numbers, and canceled checks in the dumpster of Northeast Security in New Haven, Massachusetts. When Northeast Security closed and moved out of the store, the company threw its clients' data out without shredding it.
- On May 1, 2007, Healing Hands Chiropractic threw away hundreds of patients' medical records containing names, Social Security numbers, home addresses, and (in certain records) credit card information, without first shredding them.
- That same day, garbage bags containing financial data of customers of J. P. Morgan were found outside five branch offices in New York City.
- Similarly, on that day, documents that included personal data, medical records, and the results of police background checks from the Maine State Lottery Commission were found in a dumpster.

The theft, loss, or accidental disclosure of personal data from such databases is the responsibility of the companies or agencies that hold this information—not the responsibility of the individuals whose data are held within the database. To effectively protect individuals' identities and prevent identity theft, both systemic solutions (security of personal data held in databases) and individual responses (actions that individuals take to protect themselves from becoming victims of identity theft) are required.

Where Can Someone Find Information to Steal?

A plethora of information can be found about individuals online. websites that provide anything from background checks to individuals' photographs, home addresses, phone numbers, e-mail addresses, age, date of birth, work history, education, alumni information, family members, average income, criminal records, and so on include, but are not limited to, the following:

- Yahoo! People Search: http://people.yahoo.com/
- U.S. Search: www.ussearch.com

Things to Remember

To protect yourself from becoming a victim of identity theft, you should take the following precautions:

- Avoid storing your personal information on computers and related electronic devices.
- Shred documents containing personal information before you discard them.
- Check your bank accounts frequently for unusual activity.
- Get a credit report and check your credit score.
- Do not use the same password for all of your accounts. If an offender hacks into one of the accounts of the victim, a similar password will provide the hacker with access to his or her other accounts.

The U.S. Department of Justice provides information on identity theft and identity fraud on its website: http://www.usdoj.gov/criminal/fraud/websites/idtheft.html. Specifically, this site includes information on what identity theft and identity fraud are, what the most common ways to commit these crimes are, which actions the Department of Justice is taking to combat these crimes, how individuals can protect themselves from these crimes, and what actions individuals should take if they become a victim of these crimes. This site also provides links to other sites that have information on identity theft and identity fraud.

- U.S.A. People Search: www.usa-people-search.com
- Pipl: www.pipl.com
- Intelius: http://www.intelius.com/people-search.html
- People Finder: http://www.peoplefinders.com/
- Wink: http://wink.com/
- PeekYou: http://www.peekyou.com/
- PeopleLookup: http://www.peoplelookup.com/

Social networking websites (e.g., Facebook, Twitter, MySpace) also store a vast amount of individuals' personal information. Many individuals holding accounts on social networking sites do not password-protect their accounts and routinely accept strangers' "friend requests," which provides strangers with access to all of the photographs, videos, and information (e.g., home address, e-mail address, and phone number) in the individual's account. Of course, these sites do have privacy protection controls that allow users to limit access to their accounts and even allow users to restrict access to specific areas in the account to a limited number of friends (or users whom the individual has allowed access to his or her account). Many users, however, do not choose these options, even though these measures would enhance the security of their personal information. To verify this fact, just visit these sites and search through the numerous open accounts.

Most personal and financial information can be obtained online if the price is right. Chat rooms, bulletin boards, and advertisements exist that openly sell such data. Indeed, identity thief Robbin Shea Brown bought approximately 4500 credit card numbers, PINs, and personal data relating to the customers' accounts—such as the expiration dates of credit cards, passwords, and Social Security numbers—in online chat rooms from sellers who claimed to have retrieved these data from "phishing, pharming, and spamming unsuspecting victims."[35]

Cyberbullying

With cyberbullying, bullies no longer need to confront their victims face-to-face. Instead, young cyberbullies use communications technologies to annoy, embarrass, humiliate, abuse, threaten, stalk, or harass other children or teenagers. Generally, two types of cyberbullying are distinguished:[36]

- *Direct cyberbullying*. As the name clearly indicates, this type of cyberbullying occurs when an individual attacks a victim directly.
- *Cyberbullying by proxy*. With this type of cyberbullying, an individual enlists the help of others to assist him or her with bullying the victim. Sometimes this occurs without the knowledge of the "helpers." For instance, to alienate a student from her classmates, a girl might pose as the victim and post insulting comments to her fellow students. The students then retaliate against the victim, thinking that she initiated the verbal attack. Depending on where the information is posted and who views it, a victim may be cyberstalked subsequently to fake postings.

There are many different ways in which a cyberbully can either directly attack the victim or orchestrate an attack by proxy. Shielded by anonymity, children (or teenagers) can use websites, tweets (messages sent via Twitter), instant messages, e-mails, blogs, polls, and posts on social networking sites to belittle, verbally attack, stalk, or otherwise threaten other children or teenagers. Cyberbullying can also occur when perpetrators upload embarrassing photos or videos of the victim to websites (e.g., YouTube) or e-mails, and then send them or make them available to numerous people so that they can collectively bully the victim. The harassers can further bully their victims by using text messages or multimedia messages (to send pictures and videos) via cell phones. In particular, cyberbullying may take any of the following forms included in the next subsections.

Stalking the Victim

First, the harasser may stalk the victim, by sending him or her repeated rude, threatening or harassing e-mails, instant messages, or text messages. To see how this works, consider what happened to Amanda Marcuson of Birmingham, Michigan.[37] Marcuson had reported some girls for stealing a pencil case she owned with makeup in it. In retaliation, the girls bombarded her with instant messages calling her a tattletale and a liar. Marcuson

had set up her phone to have e-mails and instant messages sent to her phone. As a result, she received so many messages that her mobile phone inbox was filled to capacity—a phenomenon known as a text war. Text wars occur when a few people get together to send the victim hundreds of messages (instant, e-mail, or text), causing e-mail stress and significantly increasing the costs to the victim (by increasing the cell phone charges from the sheer number of message received on the victim's phone).[38]

Another case involved Lauren Newby of Dallas, Texas. In her situation, a cyberbully started posting offensive and vicious comments about Newby on a website. Other individuals joined in, making insulting comments about her weight and a health issue she had (multiple sclerosis).[39] However, the bullying did not stop there: It moved offline and into the real world. Specifically, "Lauren's car was egged, 'MOO BITCH' was scrawled in shaving cream on the sidewalk in front of her house, and a bottle filled with acid was thrown at her front door."[40]

The communication of violence or threats is prohibited online. In the majority of cases, this behavior violates the terms of use of websites. Indeed, social networking sites (e.g., Facebook and MySpace) typically have terms of service agreements that prohibit any type of verbal abuse, homophobic, racist, or otherwise offensive remarks.[41] For example, according to its website, when you use or access Facebook you agree to its "Statement of Rights and Responsibilities."[42] Under Section 3(6) of Facebook's "Statement of Rights and Responsibilities," an individual cannot bully, intimidate, or harass another user. MySpace has developed similar terms of use that prohibit the users of its site from harassing other users.[43] Other sites, such as Twitter, prohibit the communication of violence. In particular, Twitter's terms of use explicitly forbid the publishing or posting of "direct, specific threats of violence against others."[44]

Sharing the Victim's Personal Information

A cyberbully may share personal information about the victim or post the passwords of the victim online. This type of information may place the victim in harm's way. For example, if someone posts a victim's address online, the individual may be stalked, harassed, or harmed in real life. If the victim's password is posted online, individuals can steal the victim's personal information or can pose as the victim. For instance, upon gaining access to their victim's account, they may steal personal photographs and videos of the victim and send them to others en masse to humiliate the target. If they steal their victim's password, they may access the target's online account and post insulting messages to others to provoke retaliation. This behavior is prohibited by most online sites. In fact, the terms of use of most websites are violated if an individual discloses another person's username and password to a third party or uses "the account, username, or password of another [m]ember at any time."[45]

Posing as the Victim and Soliciting Sex

Third, the cyberbully may pose as the victim and post solicitations for sex in the victim's name. With this approach, the cyberbully typically includes the personal contact infor-

mation of the victim in the solicitations. Sometimes cyberbullies can intentionally seek to harm a victim by posting solicitations for sex online on behalf (and unbeknownst) to the victim along with the victim's telephone number (fixed telephony and mobile) and home address. Sometimes these advertisements are posted on child predator websites. The transmission of material or content that promotes the physical harm or injury of any individual is explicitly forbidden by most online sites.[46]

Posing as the Victim to Send Messages

A cyberbully may send e-mail messages, instant messages, or text messages to others while disguising himself or herself as the victim. Cyberbullies may pose as their victims by using similar screen names (with minor changes that will go unnoticed by most online users) and post inappropriate things to other online users. Those users, thinking it is the victim who is saying such things about them, will most likely retaliate and make similarly offensive remarks about the victim in return. To be cruel, sometimes bullies pose as other victims to embarrass them and alienate them from other classmates. A real life example of this involved Kylie Kenney. Her cyberbullies had chosen screen names that were similar to Kenney's screen name to make sexual remarks about and advances on her female hockey teammates, alleging that the remarks were made by Kenney herself.[47]

Moreover, a cyberbully usually poses as the victim as a form of retaliation for something the victim has done (whether real or perceived) to the cyberbully. Consider the following example: Becky is angry at Maggie for going out with her ex-boyfriend, Mark. She poses as Maggie online and posts messages to the accounts of Mark's friends—Ryan, Tristan, and John—that include insults about Mark and ask his friends to go out with her. Ryan, Tristan, and John respond by insulting Maggie for her inappropriate behavior. They also inform Mark about the messages from Maggie. Mark calls the relationship off with Maggie as a result of the messages he thought she sent to his friends.

Some online sites specifically forbid impersonation of others. For instance, MySpace prohibits "impersonating or attempting to impersonate MySpace or a MySpace employee, administrator or moderator, another [m]ember, or person or entity (including, without limitation, the use of email addresses associated with or of any of the foregoing)."[48] Twitter also prohibits the impersonation of others "through the Twitter service in a manner that does or is intended to mislead, confuse, or deceive others."[49] Therefore, using a false identity or otherwise attempting to mislead others as to a user's identity or the origin of messages is expressly prohibited.[50] Furthermore, Formspring.me, an online forum that allows users to ask questions and give answers to just about anything, prohibits the transmission of "any material or content that attempts to falsely state or otherwise misrepresent" the user's identity or affiliation with a person or entity.[51]

Creating Polls to Humiliate the Victim

Cyberbullies may create embarrassing, insulting, and oftentimes offensive polls to bully their victims online, such as "Who is the ugliest person in the class?", "Who is the biggest slut in the class?", "Who is Hot? Who is Not?", and so on. Additionally, cyberbullies may

encourage others to participate in Internet polls and share offensive or insulting comments about classmates (e.g., their top 10 ugliest girls or boys in the class). This behavior also violates the terms of use of most websites, because the transmission or encouragement of "harassing, libelous, abusive, threatening, harmful, vulgar, obscene or otherwise objectionable material of any kind or nature" is strictly prohibited.[52]

Creating Websites to Humiliate the Victim

Cyberbullies may create websites that ridicule, humiliate, or intimidate others. This involves uploading or disseminating embarrassing or inappropriate videos or pictures of the victim. Cyberbullies sometimes write about their victims on online blogs as well. Other children can also take part in the quest to humiliate or harass the target of the cyberbullying by creating websites dedicated to verbally attacking and embarrassing the victim.

For example, a website was created about David Knight, titled "Welcome to the website that makes fun of David Knight."[53] This page provided individuals with the opportunity to post hateful comments about Knight, which they did in abundance. Knight was not alone. Jodi Plumb, a 15-year-old girl from Mansfield, England, also discovered a website containing abusive comments concerning her weight and even had the date of the day she was supposedly going to die posted on it.[54] Yet another example of this type of cyberbullying involved Kylie Kenney. Her classmates created websites with names such as "Kill Kylie Incorporated" that contained offensive and homophobic remarks about Kenney.[55]

Sexting Distribution

Another humiliating and degrading form of cyberbullying is sexting. **Sexting** "is the act of sending, receiving, or forwarding sexually explicit messages, photos, or images via cell phone, computer, or other digital device."[56] The original messages and photos are then forwarded beyond the intended recipient, resulting in widespread humiliation and ridicule of the subject of the photo.

An example of this kind of cyberbullying involved Hope Witsell.[57] Witsell sent a photo of her breasts to a boy she liked in her school. This photo was subsequently distributed to others in the school. The distributor of these photos was not the boy to whom Witsell had sent the photos, but rather a girl who had borrowed his phone. When the girl noticed the picture of Witsell, she forwarded the photo to her own phone and to the phones of other students. The picture was viewed by the majority of students in Witsell's school. Witsell was taunted about the picture relentlessly. When the taunting proved too much for her to bear, she hung herself. She was only 13 years old when she died.

In a similar case, an 18-year-old teenager, Jesse Logan, killed herself after an ex-boyfriend forwarded naked pictures of her after they ended their relationship.[58] She, too, could not handle the humiliation she felt as a result of his actions.

It is important to note that pornographic material cannot be posted or distributed on certain websites. Doing so may result in the deletion of the account by the site administrators, as this behavior violates the terms of use of most online sites.[59]

Notification Wars

"Notification wars" (or "warning wars") may occur online. Sometimes cyberbullies will falsely report their victims for terms of use violations on websites on more than one occasion. When a site receives notice of a violation of the terms of service, the victim's account may be temporarily suspended while an investigation ensues or the account may be permanently deleted.[60]

The High Costs of Cyberbullying

Cases involving cyberbullying have led to the death of many of the victims. A recent case involved Phoebe Prince, who was subjected to intolerable ridicule and torment at school. People would insult her and call her names on Facebook, Formspring, and Twitter.[61] Prince was not alone; numerous cases like hers have occurred in the United States. Prince's cyberbullying case is just the most recent. Before her death by suicide, there was the case of Carl Joseph Walker-Hoover, who hung himself after enduring constant bullying at school and being repeatedly subjected to anti-gay slurs.[62]

Sadly, the suicides from cyberbullying do not stop there. Another widely recognized case involved Megan Meier.[63] Meier was a former friend of Lori Drew's daughter, Sarah. Lori Drew and her daughter decided to set up a false identity, "Josh Evans." The elder Drew stated that this was done to see if Meier was spreading rumors about Sarah. Meier believed that "Josh" was a real person. "Josh" complimented Meier and told her she was beautiful; Meier believed that they had formed an online relationship. One day, "Josh" broke off the relationship, claiming that he had heard that she was a cruel person. Meier committed suicide after "Josh" told her that the "world would be a better place without you." She was 13 years old when she took her life.

As a result of the lack of adequate laws on cyberbullying at that time, Lori Drew was charged only with violating the terms of service agreement of MySpace. In 2009, she was acquitted of all charges on appeal. A cyberharassment law was enacted in Missouri in response to the Megan Meier case.

One individual charged with violating this law was Elizabeth Thrasher. Thrasher posed as a 17-year-old girl (the daughter of her ex-boyfriend's girlfriend) and posted sexual advertisements on the "Casual Encounters" section on Craigslist.[64] She also posted a picture, the cell phone number, and e-mail address of the teenager. As a result, the 17-year-old girl received numerous offensive e-mails, calls, text messages, and pornographic photographs from individuals responding to her supposed advertisement on Craigslist.

Another cyberbullying victim was Ryan Patrick Halligan.[65] Rumors about his sexual orientation were spread through the Internet by people he believed to be his friends. He

started talking with one of the most popular girls in school over the summer of 2003. From their conversations, he had believed that they had grown quite close. When the school year started, Halligan approached her to speak with the girl in person. In front of her friends, she ridiculed him and informed him that their online relationship was a hoax. She also informed him that she shared everything that he had confided with her to her friends. Halligan was unable to cope with the rejection and humiliation he felt and ended his life. His family later lobbied successfully to have an anti-cyberbullying statute passed.[66]

Some harassers have even continued bullying individuals even after the death of the victims. Specifically, after Phoebe Prince and Alexis Pilkington died following bullying incidents, their tormentors posted vicious comments on their Facebook memorial pages.[67]

Some children's parents have sought to fight their children's bullies in court. A successful example of such an occurrence involved the parents of Ghyslain Raza, who became known as the "*Star Wars* kid." Ghyslain's classmates uploaded a humiliating video of him pretending to be a *Star Wars* character online. The boy was subjected to extensive ridicule worldwide because of this video. His parents successfully sued the parents of the bullies who posted Raza's video online.

It is clear that technology has made cyberbullying far worse than bullying by conventional (in person) means, as rumors may now be spread much faster to a larger number of individuals. Once the embarrassing or offensive material has been posted, it is extremely difficult (if not impossible) to completely remove it. For instance, in the now famous case of Ghyslain Raza, his video was viewed more than 1 million times approximately one month after it was posted. Anyone can post this kind of information online. Only if these cyberbullies are caught will their accounts be deleted—but by then the damage to the victim is already done. Yet, cyberbullies may continue on, even after their accounts have been deleted, because it is very easy for them to open up accounts under a false name, as long as a different e-mail address is provided. This is possible because the majority of websites do not authenticate the personal information that individuals provide.

Child Exploitation Online

Computer forensics investigators often use Internet resources to gather evidence on **child exploitation**. Specifically, the Internet can assist investigators and members of the public in identifying predators and child molesters.

The **National Sex Offender Registry** is one such website that can provide investigators with information on **sexual predators**. The Family Watchdog website (http://www.familywatchdog.us) provides access to such a registry. This site offers many essential tools for parents, concerned citizens, and law enforcement agencies with which to protect children. Parents and concerned citizens can search this site for registered sex offenders in their neighborhood. Investigators can type in the victim's address and locate any sex offenders who live close by using these types of websites. If an incident occurs at a school, an investigator can locate the school on the map of the residences as well as areas of local

employment of sex offenders, thereby determining whether a sex offender is in close proximity to that school.

Another very important tool for investigations is the reverse e-mail lookup. This tool scans various social and picture sites to see where e-mail addresses have been registered. Investigators can use this information to track down user profiles created by the sex offenders on these social sites and determine whether these individuals have contacted children using the sites by looking at their "friends" lists. Many sites are available online that provide reverse e-mail searches, including the following sites:

- AnyWho (http://www.anywho.com/rl) provides reverse phone lookup.
- People Search Pro (http://www.peoplesearchpro.com/resources/email-search/reverse-email-lookup/) provides reverse e-mail lookup.
- Reverse Records (http://www.reverserecords.org/?hop=haskinsmic) provides reverse e-mail, phone, cell phone, and home address lookups.

The Dru Sjodin National Sex Offender public website provides real-time access to state and territory sex offender registries, including registries from all 50 states and the U.S. territories of Guam, Puerto Rico, the District of Columbia, and participating tribes.[68] This registry was named after Dru Sjodin, who was kidnapped, brutally raped, and murdered by a three-time convicted sex offender, Alfonso Rodriguez, Jr. The public outcry in the wake of this crime led to "Dru's law," which called for establishment of a national sex offender registry.

Dru's law became part of the **Adam Walsh Protection and Safety Act of 2006**, which was passed in response to the abduction of Adam Walsh, the son of former *America's Most Wanted* host John Walsh, from a mall in Florida and his subsequent murder. Adam Walsh's killer was never caught. Title I of the Adam Walsh Child Protection and Safety Act is known as the **Sex Offender Registration and Notification Act of 2006** (SORNA). SORNA created a national sex offender registry, where the offenders' photographs, full names and any aliases, home and work addresses, dates of birth, and offenses committed are posted. The Adam Walsh Children Protection and Safety Act also strengthened the national sex offender registry by requiring more data to be included about sex offenders, such as their physical description, fingerprints, palm prints, DNA samples, criminal history, and a detailed summary of their crimes. This law was intended to standardize state sex offender laws nationwide. It further provided for a three-tier system to be used when categorizing sex offenders for the purposes of the registry:

- Tier 1 offenders must be registered for 15 years and update their information annually.
- Tier 2 offenders must be registered for 25 years and update their information biannually.
- Tier 3 offenders—the most dangerous offenders—must register for life and are required to update their information in the database every three months (to ensure that it remains up-to-date).

Moreover, the **Campus Sex Crimes Prevention Act of 2000** requires that sex offenders who enroll or work at a community college, college, university, or trade school must notify local law enforcement agencies.

Prior to the passage of the Adam Walsh Children Protection and Safety Act, legislators at both the federal and state levels had passed several other laws that paved the way for national registration of sex offenders. These laws were triggered by the abduction and murder of children by sexual offenders. In particular, in 1990, Megan Kanka was raped and murdered by a neighbor who was a sex offender. Her parents were unaware that a sex offender lived in their neighborhood. The young girl's death triggered the creation of state and federal laws that focused on sex offender registration and notification of residents of neighborhoods when sex offenders move in. The **Jacob Wetterling Crimes Against Children and Sexually Violent Offender Act of 1994** (codified in 42 U.S.C. § 14071), named after another victim, was enacted as part of the **Violent Crime Control and Law Enforcement Act of 1994** and required states to implement a sex offender registry.

Some state sex offender registries provide users with the option to track sexual predators. For instance, Florida has an offender alert system comprising a free service that provides e-mail alerts when an offender or predator moves close to any address in Florida that an individual chooses to monitor.[69]

Furthermore, America's Missing: Broadcasting Emergency Response (AMBER) alerts were developed to give notice to the public of recent child abductions. The **AMBER alert** system was named after Amber Hagerman, who was abducted outside of a Winn-Dixie store in her hometown of Arlington, Texas, as she was riding her bike. Four days after her abduction, the child's lifeless body was found in a drainage ditch. According to the U.S. Department of Justice, as of 2009, AMBER alerts have helped rescue 495 children.[70] For an AMBER alter to be issued, the following conditions must be met:

- Law enforcement agents must confirm that the child has been abducted.
- The abducted child must be at risk of serious harm or death.
- A sufficient description of the child, the child's abductor, or the abductor's vehicle must exist.
- The abducted child must be 17 years old or younger.

Apart from appearing on televisions, radios, websites, and highway traffic boards, AMBER alerts can be issued through messages sent to wireless devices, should users opt to receive such alerts relative to their geographical location.

Online Sexual Predators

Sexual predators have been known to frequent chat rooms and monitor ongoing conversations in search of their next victims. Once they find a potentially suitable target, they engage in conversation with him or her. Sometimes they attempt to engage the target in a private conversation. Slowly they develop a relationship of trust with their victim, encour-

The Child Pornography Protection Act of 1996

The sections of the **Child Pornography Protection Act** that explicitly criminalize the exploitation of children online include, but are not limited to, the following:

- 18 U.S.C. § 2251: prohibits the sexual exploitation of children.
- 18 U.S.C. § 2251A: provides severe penalties for persons who buy and sell children for sexual exploitation.
- 18 U.S.C. § 2252: covers activities relating to material involving the sexual exploitation of minors.
- 18 U.S.C. § 2252A: prohibits activities relating to material constituting or containing **child pornography**.

aging the victim to confide in them by convincing the victim to share his or her personal information (e.g., age, home address, phone number, relationship status). They may also try to convince the minor to engage in sexually explicit conduct. For example, Ivory Dickerson persuaded and enticed "female minors into engaging in sexually explicit conduct for the purpose of manufacturing child pornography."[71] His computer also contained more than 600 child pornography images. Mark Wayne Miller posed as a young male to persuade his victims—young girls to engage in sexually explicit conduct.[72] He recorded these sessions and even distributed some of these sessions to third parties via active Webcams.

Eventually, sexual predators try to set up a meeting with their victims. Some even travel across states to meet these youths. In one case, an individual violated 18 U.S.C. § 2423(b), which prohibits a "person from traveling in interstate commerce, or conspiring to do so, for the purpose of engaging in criminal sexual activity with a minor," when he traveled across state lines (from Minnesota to Wisconsin) to meet with a minor (a 14–year-old girl) he met in an online chat room and engage in sexual acts.[73]

Adults may identify themselves as children on websites to lure children into dangerous situations. One cannot definitively know that the person with whom an individual is communicating in chat rooms and social networking sites or through e-mails and instant messages is not a sexual predator. In an attempt to remedy this problem, the **Keeping the Internet Devoid of Sexual Predators Act of 2008** (KIDS Act) was enacted. The KIDS Act requires sex offenders to submit their e-mail addresses and online screen names to the national sex offender registry.

The Internet also provides these predators with anonymity. They can pretend to be any age—some have even entered chats among 10-year-olds pretending to be the same age. When these adults pretend to be children or teenagers, their victims are more likely to develop friendships and online relationships with these individuals. At other times,

offenders have pretended to be a different gender. William Ciccotto, a 51–year-old male, posed as a young girl (between the age of 13 and 14 years old).[74] Specifically, he opened a Hotmail account and a MySpace account under the name "Cindy Westin" through which he proceeded to send friend requests to young girls and chat with them within this site and via AOL instant messages. Under this persona, Ciccotto convinced the girls to send nude photos of themselves, sometimes convincing his correspondents to take photos of themselves engaging in sexually explicit conduct and send them to "Cindy." Ciccotto then distributed the photos through a private peer-to-peer (P2P) network.

Child Pornography Images and Videos

The Internet provides sexual predators with easy, fast, convenient, and anonymous access to vast quantities of pornographic material featuring children worldwide for a low cost. Sometimes child pornography images can be stored in servers beyond U.S. law enforcement agencies' reach. Thus child pornography poses unique challenges to law enforcement agencies. Coordinating responses with multiple jurisdictions may be required to track even one child pornography distributor.

In the United States, case law and statutes have outlawed the manufacture, possession, and distribution of child pornography. For instance, the **Sexual Exploitation of Children Act of 1978** made it illegal for someone to manufacture and commercially distribute obscene materials that involve minors younger than 16 years old. Ten years later, the **Child Protection and Obscenity Enforcement Act of 1988** was enacted. This Act made it illegal for an individual to use a computer to depict or advertise child pornography. Later, in 1990, the *Osborne v. Ohio*[75] ruling stated that private possession of child pornography was illegal.

Child pornography can be found in the following areas on the Internet:[76]

- *Newsgroups.* Members may share child pornography images and information on child pornography websites through this medium to avoid unwanted attention by Internet service providers (ISPs) and law enforcement agencies. They may use code to discuss child pornography websites or hide the images of child pornography among legal adult pornographic images.
- *Bulletin boards.* Discussions on child pornography often occur in this forum, and websites containing child pornography are frequently rated and shared among child pornographers. These forums may be password protected to avoid infiltration by undercover law enforcement agents and individuals who oppose child pornography collection and distribution.
- *Chat rooms.* These areas are used to exchange child pornography images and find minors to sexually exploit and victimize.
- *Peer-to-peer networks.* These networks enable the sharing of child pornography images (files) to closed groups to avoid detection.

- *E-mails.* This method is not often used by seasoned sexual predators to share images because of their fear that they might unwittingly transfer such material to undercover law enforcement agents.

In a landmark, but controversial case, *Ashcroft v. Free Speech Coalition*,[77] the U.S. Supreme Court held that virtual (i.e., computer-generated) images of child pornography were legal—as long as a real child was not used to produce the image. This ruling raised significant issues for prosecutors of child pornography cases because the burden of proof is now on prosecutors to show that the images depict actual children, rather than adult models made to look like children. The **Child Victim Identification Program**, which houses the largest database of child pornography images for the purpose of identifying victims of child exploitation and abuse, was developed in the aftermath of the Supreme Court's ruling in the *Ashcroft* case.

In 1998, the Child Protector and Sexual Predator Punishment Act was enacted, which required ISPs) to report incidents of child pornography to authorities when they come across them. ISPs are not actively required to monitor their websites or customers, however. Additionally, Section 508 of the **Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today Act of 2003** (PROTECT Act) amended the **Victims of Child Abuse Act of 1990** to

> authorize a provider of electronic communication or remote computing services that reasonably believes it has obtained knowledge of facts and circumstances indicating a State criminal law child pornography violation to disclose such information to an appropriate State or local law enforcement official.

In addition, the PROTECT Act prohibited the use of misleading domain names with the intent to deceive a minor into viewing online material that is harmful to minors. For example, John Zuccarini used the Internet domain names of a famous amusement park, celebrities, and cartoons to deceive minors into logging into pornography websites.[78] Specifically, he intentionally misspelled versions of a domain name (www.dinseyland.com) owned by the Walt Disney Company (www.disneyland.com). Zuccarini also used 16 misspellings and variations of the name of the legitimate website of the popular female singer Britney Spears (www.britneyspears.com). In addition, Zuccarini used misspellings and variations of the domain names of legitimate websites depicting two popular cartoon characters, Bob the Builder and Teletubbies—for example, www.bobthebiulder.com and www.teltubbies.com.[79]

The **Securing Adolescents from Exploitation Online Act of 2007** (SAFE Act) expanded the definition of an ISP to include wireless hot spots such as libraries, hotels, and municipalities. It also required such service providers to "provide information relating to the Internet identity of any individual who appears to have violated a child exploitation or pornography law, including the geographic location of such [an] individual and images of any apparent child pornography." Moreover, the SAFE Act required these ISPs to preserve images of child pornography that were observed for evidentiary

purposes. Failure to do so or to report instances of child pornography will result in significant penalties to an ISP. If civilians find websites that exhibit child pornography, the Child Exploitation and Obscenity Section (CEOS) website states that these individuals should contact the **National Center for Missing and Exploited Children** (NCMEC).

Internet service providers can help fight against the proliferation of child pornography by taking the following steps:[80]

- Removing illegal sites wherever and whenever they encounter them.
- Establishing websites and hotlines where individuals can complain about any child pornography images or websites encountered.
- Taking responsibility for the content of sites they host and notifying authorities when child pornography is encountered.
- Preserving their records to make them available for law enforcement agencies during investigations of child pornography creation, collection, and distribution.
- Requiring the verification of personally identifying information given by individuals to open up accounts. Individuals may use fake names, home addresses, and phone numbers to open up accounts, for example, because this information is not authenticated by ISPs. This factor makes it extremely difficult for law enforcement authorities to trace and find those persons who are responsible for these illegal activities.

Law enforcement responses to child pornography should include the following measures:[81]

- Locate and take down child pornography websites.
- Find out who is signed up to download and post child pornography from these websites.
- Conduct undercover sting operations. For instance, an undercover FBI agent downloaded child pornography images from P2P networks from a user known as "Boys20096."[82] The undercover agent traced the IP address of "Boys20096" to a residence in Wheaton, Illinois. A laptop seized at the residence was believed to belong to a live-in nanny, Lubos Albrecht. The laptop contained approximately 6000 images or videos of child pornography. The FBI eventually linked Albrecht to the laptop and the P2P sharing network from which the child pornography images were obtained.
- Create "honeypots" to lure child pornographers in an attempt to identity them. Honeypots also discourage other child pornographers from visiting these websites for fear that they are not real child pornography websites, but rather fake websites designed to bait and catch them.
- Publicizing captures of individuals engaging in sexual conduct with minors and the creation, collection, and distribution of child pornography. This publicity is

meant to instill fear and uncertainty in the offender or potential offenders that their online illegal actions may be brought to the attention of authorities—for which they will certainly be punished.

Chapter Summary

This chapter explored the computer-networking environment in which scam artists, identity thieves, cyberbullies, and sexual predators operate in and the crimes they commit. Through auction, rental, retail, dating, lottery, employment, and virus protection scams, individuals' personal, financial, and banking details can be stolen. Individuals posing as international or national government officials may also seek to take advantage of unsuspecting victims and steal their money and/or identities. Identity thieves can steal victims' identities for profit, so as to avoid detection or deceive law enforcement authorities and to commit other crimes. Indeed, individuals' personal information is readily available online from a variety of sources.

Cyberbullies may verbally attack their victims through text messaging on their cell phones and in cyberspace through websites, instant messages, e-mails, posts on social networking sites, or blogs. Their victims are exposed to demeaning text messages, embarrassing photos, humiliating videos, and crude opinion polls that make this type of bullying particularly disturbing. By providing bullies with the ability to post their hurtful messages anonymously, the Internet has created a breeding ground for cyberbullying.

Children may attract unwanted attention from online sexual predators as well. Sexual predators use the Internet to stalk their victims under the cloak of anonymity afforded to them by the online environment. The predator may use multiple personas to lure the victim into a false sense of security. Many laws have been passed to prohibit the sexual exploitation of children and the creation, collection, and distribution of child pornography online. Because of problems related to the Internet's lack of boundaries and single jurisdictions, the regulation of child pornography, prevention of child exploitation, and investigation of child sexual predators pose unique challenges to law enforcement agencies worldwide.

Practical Exercise

Consider the cyberbullying case that resulted in the death of 13-year-old Megan Meier. After Meier's suicide in 2006, Missouri revised its harassment statutes to include bullying, stalking, and harassment via telecommunications and electronic communications. Why do you think this happened?

In considering this question, refer *United States v. Drew*[83] to provide a brief description of the case. In your answer, indicate which law the suspect was charged with violating. Given that these charges were later overturned, also explain why this happened in your answer.

Review Questions

1. Which types of scams do scam artists use to steal the personal, financial, and banking information of victims?
2. What is the "419 scam," and what does it involve?
3. Why is spam dangerous to the victim?
4. What are the similarities and differences between vishing, phishing, and pharming?
5. What are four types of identity theft?
6. How have existing practices in storing individuals' personal information facilitated identity theft?
7. Where can offenders find the personal information of a victim?
8. What is cyberbullying, and where does it occur?
9. What is sexting?
10. Where can child pornography be found online?
11. How have ISPs contributed to the fight against child pornography?
12. How have law enforcement agencies sought to combat child pornography?

Key Terms

Adam Walsh Protection and Safety Act of 2006
AMBER alert
Campus Sex Crimes Prevention Act of 2000
Child exploitation
Child pornography
Child Pornography Protection Act of 1996
Child Protection and Obscenity Enforcement Act of 1988
Child Victim Identification Program
Dating scam
Dru's law
Government e-mail scam
Identity theft
Jacob Wetterling Crimes Against Children and Sexually Violent Offender Act of 1994
Keeping the Internet Devoid of Sexual Predators Act of 2008
Lottery scam
National Center for Missing and Exploited Children
National Sex Offender Registry
Nigerian scam
Pharming
Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today Act of 2003
Rental and real estate scam
Scareware
Securing Adolescents from Exploitation Online Act of 2007
Sex Offender Registration and Notification Act of 2006
Sexting
Sexual Exploitation of Children Act of 1978

Sexual predator
Spam
Victims of Child Abuse Act of 1990
Violent Crime Control and Law Enforcement Act of 1994
Virus protection scam
Vishing
Work-at-home scam

Footnotes

[1]Pethia, R. (2006). Information assurance and computer security incident response: Past, present, future. CERT, Software Engineering Institute, Carnegie Mellon University. Retrieved from http://search.first.org/conference/2006/papers/pethia-richard-slides.pdf

[2]White, J. (2010, May 24). District food servers charged in theft of patron's credit card numbers. *Washington Post* [online]. Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2010/05/23/AR2010052302921.html?hpid=newswell

[3]For further information, see Winterman, D. (2010, June 15). How not to get scammed like Alan Bennett. *BBC News* [online]. Retrieved from http://news.bbc.co.uk/2/hi/uk_news/magazine/8740984.stm

[4]Federal Bureau of Investigation. (2010, March 12). Rental and real estate scams. *New E-Scams & Warnings*. U.S. Department of Justice, Investigative Programs: Cyber Investigations. Retrieved from http://www.fbi.gov/cyberinvest/escams.htm

[5]For more information on this scam, see US Department of State. (2007, February). International financial scams: Internet dating, inheritance, work permits, overpayment, and money-laundering. Retrieved from http://travel.state.gov/pdf/international_financial_scams_brochure.pdf

[6]For further information on this scam, see US Department of State. (2009, August 5). Lottery scams. Retrieved from http://travel.state.gov/travel/cis_pa_tw/cis/cis_2475.html

[7]Federal Bureau of Investigation. (2009, October 5). Fraudulent email claiming to contain FBI "Intelligence Bulletin No. 267." *New E-Scams & Warnings*. US Department of Justice, Investigative Programs: Cyber Investigations. Retrieved from http://www.fbi.gov/cyberinvest/escams.htm

[8]Federal Bureau of Investigation. (2009, October 5). Fraudulent email claiming to be from DHS and the FBI Counterterrorism Division. *New E-Scams & Warnings*. US Department of Justice, Investigative Programs: Cyber Investigations. Retrieved from http://www.fbi.gov/cyberinvest/escams.htm

[9]Internet Crime Complaint Center. (n.d.). Internet crime schemes. Retrieved from http://www.ic3.gov/crimeschemes.aspx

[10]See Fraud Watch International. (n.d.). Nigerian 419 scams. Retrieved from http://www.fraudwatchinternational.com/nigerian-419/

[11]See, for example, http://www.scam-info-links.info/; http://www.internetscamswatch.com/; http://www.fraudaid.com/ScamSpeak/Nigerian/nigerian_scam_letters.htm

[12]Federal Bureau of Investigation. (2009, February 9). Work-at-home scams. *New E-Scams & Warnings*. US Department of Justice, Investigative Programs: Cyber Investigations. Retrieved from http://www.fbi.gov/cyberinvest/escams.htm

[13]Federal Bureau of Investigation. (2009, December 11). Pop-up advertisements offering anti-virus software pose threat to Internet users. *New E-Scams & Warnings*. US Department of Justice, Investigative Programs: Cyber Investigations. Retrieved at: http://www.fbi.gov/cyberinvest/escams.htm

[14]Thomas, T. L. (2003). Al Qaeda and the Internet: The danger of "cyberplanning." *Parameters*, p. 115.

[15]Financial Crimes Enforcement Network. (2008, July 18). FinCEN reminds public to be aware of financial scams. Retrieved from http://www.fincen.gov/news_room/nr/pdf/20080718.pdf

[16]Social Security Administration. (2006, November 7). Public warned about email scam. News release. Retrieved from http://www.internetcases.com/library/statutes/can_spam_act.pdf

[17]Federal Bureau of Investigation. (2008, May 8). Phishing related to issuance of economic stimulus checks. *New E-Scams & Warnings.* US Department of Justice, Investigative Programs: Cyber Investigations. Retrieved from http://www.fbi.gov/cyberinvest/escams.htm

[18]US Department of Justice, (2010, June 24). Nantucket man arrested and charged with operating international online "phishing" scheme to steal income tax refunds. Retrieved from http://www.justice.gov/criminal/cybercrime/mardakhayeuIndict.htm

[19]McLean, P. S., & Young, M. M. (2006, March/April). Phishing and pharming and Trojans: Oh my!. *Utah Bar Journal, 19,* 32.

[20]New York State Attorney General. (2009, April 22). Attorney General Cuomo announces arrest of former State Tax Department employee for using position to steal taxpayer's identities. Retrieved from http://www.ag.ny.gov/media_center/2009/apr/apr22a_09.html

[21]Sandholm, D. (2009, October 28). NY computer repairman accused of identity theft in $1.1M scheme. *ABC News* [online]. Retrieved from http://abcnews.go.com/Blotter/man-allegedly-orchestrated-11m-fraud-scheme/story?id=8940921

[22]Gross, G. (2008, May 2). Military contractor convicted on ID theft charges. *IDG News Service* [online]. Retrieved from http://www.networkworld.com/news/2008/050208-military-computer-contractor-convicted-on.html

[23]Brown seeks identity theft law. (2002, June 2). *New York Law Journal*, p. 9.

[24]Rudner, M. (2008). Misuse of passports: Identity fraud, the propensity to travel, and international terrorism. *Studies in Conflict & Terrorism, 31*(2), 103.

[25]*Ibid*.

[26]Lormel, D. M. (2002, July 9). Hearing on S.2541, "The Identity Theft Penalty Enhancement Act." Testimony of Chief of Terrorist Financial Review Group, FBI Before the Senate Judiciary Committee Subcommittee on Technology, Terrorism and Government Information. Retrieved from http://www.fbi.gov/congress/congress02/idtheft.htm

[27]ID theft ring allegedly bribed DMV. (2010, January 7). *NBC News, Los Angeles* [online]. Retrieved from http://www.nbclosangeles.com/news/local-beat/ID-Theft-Ring-Allegedly-Bribed-DMV-Employees.html

[28]Berkshire District Attorney. (2010). Identity theft. Commonwealth of Massachusetts. Retrieved from http://www.mass.gov/?pageID=berterminal&L=2&L0=Home&L1=Crime+Awareness+%26+Prevention&sid=Dber&b=terminalcontent&f=awareness_prevention_identity_theft&csid=Dber

[29]Ashley, G. D. (2002, September 19). Preserving the integrity of Social Security numbers and preventing their misuse by terrorists and identity thieves. Testimony of Assistant Director, Criminal Investigation Division, FBI, Before the House Ways and Means Committee, Subcommittee on Social Security. Retrieved from http://www.fbi.gov/congress/congress02/ashley091902.htm

[30]Privacy Rights Clearinghouse. (2010, June 25). Chronology of data breaches. Retrieved from http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP

[31]*Ibid*.

[32]*Ibid*.

[33]*Ibid*.

[34]*Ibid*.

[35]United States Attorney's Office, District of Arizona. (2008, June 3). Tucson man sentenced to over 5 years in prison for aggravated identity theft. US Department of Justice, Computer Crime & Intellectual Property Section. Retrieved from http://www.cybercrime.gov/brownSent1.pdf

[36]WiredKids, Inc. (n.d.). How cyberbullying works. Retrieved from http://www.stopcyberbullying.org/how_it_works/direct_attacks.html

[37]Jackson, D. (2005). Examples of cyberbullying. Retrieved from http://www.slais.ubc.ca/courses/libr500/04-05-wt2/www/D_Jackson/examples.htm

[38]Division of Criminal Justice Services. (2007). Cyberbullying. New York State. Retrieved from http://www.criminaljustice.state.ny.us/missing/i_safety/cyberbullying.htm

[39]Jackson, D. (2005). Examples of cyberbullying. Retrieved from http://www.slais.ubc.ca/courses/libr500/04-05-wt2/www/D_Jackson/examples.htm

[40]*Ibid*.

[41]See Section 8.1, MySpace.com. (2009, June 25). Terms of use agreement. Retrieved from http://www.myspace.com/index.cfm?fuseaction=misc.terms

[42]Statement of Rights and Responsibilities. (n.d.). *Facebook*. Retrieved from http://www.facebook.com/terms.php?ref=pf

[43]Section 8.2, MySpace. (n.d.). Terms of use agreement. Retrieved from http://www.myspace.com/index.cfm?fuseaction=misc.terms

[44]See The Twitter rules. (2009, January 14). Retrieved from http://twitter.zendesk.com/forums/26257/entries/18311

[45]Section 8.28, MySpace. (n.d.). Terms of use agreement. Retrieved from http://www.myspace.com/index.cfm?fuseaction=misc.terms

[46]See, for example, Formspring.me terms of service. (n.d.). Retrieved from http://about.formspring.me/terms

[47]Chaker, A. M. (n.d.). Schools move to stop spread of "cyberbullying." *Pittsburg-Post Gazette* [online]. Retrieved from http://www.post-gazette.com/pg/07024/756408-96.stm

[48]Section 8.27, MySpace. (n.d.). Terms of use agreement. Retrieved from http://www.myspace.com/index.cfm?fuseaction=misc.terms

[49]The Twitter rules. (2009, January 14). Retrieved from http://twitter.zendesk.com/forums/26257/entries/18311

[50]Formspring.me terms of service. (n.d.). Retrieved from http://about.formspring.me/terms

[51]*Ibid*.

[52]*Ibid*.

[53]Division of Criminal Justice Services. (2007). Cyberbullying. New York State. Retrieved from http://www.criminaljustice.state.ny.us/missing/i_safety/cyberbullying.htm

[54]*Ibid*.

[55]Chaker, A. M. (n.d.). Schools move to stop spread of "cyberbullying." *Pittsburg-Post Gazette* [online]. Retrieved from http://www.post-gazette.com/pg/07024/756408-96.stm

[56]Berkshire District Attorney. (2010). Sexting. Commonwealth of Massachusetts. Retrieved from http://www.mass.gov/?pageID=berterminal&L=3&L0=Home&L1=Crime+Awareness+%26+Prevention&L2=Parents+%26+Youth&sid=Dber&b=terminalcontent&f=parents_youth_sexting&csid=Dber

[57]Murrhee, K. C. (2010, Winter). Cyber bullying: Hot air or harmful speech?. *University of Florida, Levin College of Law*. Retrieved from http://www.law.ufl.edu/uflaw/10winter/features/hot-air-or-harmful-speech

[58]Inbar, M. (2009, December 2). "Sexting" bullying cited in teen's suicide. *MSNBC News* [online]. Retrieved from http://today.msnbc.msn.com/id/34236377/ns/today-today_people/

[59]See terms of use of social networking websites such as Facebook, MySpace, and Twitter.

[60]See, for example, the terms of use of Twitter and MySpace.

[61]Ellis, R. (2010, March 30). 9 teens indicted as a result of bullying Phoebe Prince to suicide. *NY Parenting Issues Examiner*. Retrieved from http://www.examiner.com/examiner/x-29163-NY-Parenting-Issues-Examiner~y2010m3d30-9-teens-indicted-as-a-result-of-bullying-Phoebe-Prince-to-suicide

[62]James, S. D. (2009, April 14). Carl Joseph Walker-Hoover commits suicide after anti-gay slurs. *Huffington Post* [online]. Retrieved from http://www.huffingtonpost.com/2009/04/14/carl-joseph-walker-hoover_n_186911.html

[63]*United States v. Drew*, No. 08-00582 (C.D. Cal. May 15, 2008).

[64]Harvey, M. (2009, August 19). American woman Elizabeth Thrasher faces jail over "cyber-bullying." *The Times* [online]. Retrieved from http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article6802494.ece

[65]For more information on Ryan Patrick Halligan's story, see the website that is dedicated to him: http://ryanpatrickhalligan.org/. It also contains important information and links on cyberbullying.

[66]VT. STAT. ANN. Title 16, § 1161a(a)(6) (2007).

[67]Ellis, R. (2010, March 25). Long Island teen commits suicide: Is cyberbullying to blame? *Cyber Safety Examiner*. Retrieved from http://www.examiner.com/x-39476-NY-Cyber-Safety-Examiner~y2010m3d25-Long-Island-teen-commits-suicide-Is-cyberbullying-to-blame

[68]US Department of Justice. (n.d.). Dru Sjodin National Sex Offender Public Website. Retrieved from http://www.nsopw.gov/Core/Conditions.aspx?AspxAutoDetectCookieSupport=1

[69]Florida Department of Law Enforcement. (n.d.) Florida Offender Alert System. Retrieved from http://www.nsopw.gov/Core/ResultDetails.aspx?index=3&x=0AD7C0B4-EA7E-41C9-AD1D-C0BDF0167096

[70]US Department of Justice. (2010, January). Amber alert timeline. Retrieved from http://www.ojp.usdoj.gov/newsroom/pdfs/amberchronology.pdf

[71]United States Attorney, Middle District of Florida. (2007, November 30). North Carolina man sentenced to 110 years for computer hacking and child pornography. US Department of Justice, Computer Crime & Intellectual Property Section. Retrieved from http://www.justice.gov/criminal/cybercrime/dickersonSent.pdf

[72]United States Attorney, Southern District of Ohio. (2006, January 19). Dayton man pleads guilty to sexual exploitation crimes involving minors. US Department of Justice, Computer Crime & Intellectual Property Section. Retrieved from http://www.justice.gov/criminal/cybercrime/millerPlea.htm

[73]Working Group on Unlawful Conduct on the Internet. (1999, August 5). Appendix C: Online child pornography, child luring, and related offenses. Retrieved from http://www.cybercrime.gov/append.htm

[74]United States Attorney's Office, Middle District of Florida. (2010, April 30). Brevard man pleads guilty to producing child pornography. Federal Bureau of Investigation Tampa. Retrieved from http://tampa.fbi.gov/dojpressrel/pressrel10/ta043010.htm

[75]495 U.S. 103 (1990).

[76]Wortley, R., & Smallbone, S. (2006, May). Child pornography on the Internet. US Department of Justice, Office of Community Oriented Policing Services, *Problem-Oriented Guides*, Series No. 41. Retrieved from http://www.cops.usdoj.gov/files/RIC/Publications/e04062000.pdf

[77]535 U.S. 234 (2002).

[78]United States Attorney, Southern District of New York. (2004, February 26). "Cyberscammer" sentenced to 30 months for using deceptive Internet names to mislead minors to X-rated sites. US Department of Justice, Computer Crime & Intellectual Property. Retrieved from http://www.justice.gov/criminal/cybercrime/zuccariniSent.htm

[79]The legitimate websites were www.bobthebuilder.com and www.teletubbies.com.

[80]Wortley, R., & Smallbone, S. (2006, May). Child pornography on the Internet. US Department of Justice, Office of Community Oriented Policing Services, *Problem-Oriented Guides,* Series No. 41. Retrieved from http://www.cops.usdoj.gov/files/RIC/Publications/e04062000.pdf

[81]*Ibid*.

[82]US Department of Justice. (2010, March 16). Wheaton nanny arrested for distribution of child pornography. Federal Bureau of Investigation Chicago. Retrieved from http://chicago.fbi.gov/pressrel/pressrel10/cg032610.htm

[83]No. 08-00582 (C.D. Cal. May 15, 2008).