Cyber Crimes: Real Life and in the Virtual World

Introduction
Cyber crime is a growing concern both domestically and internationally. Cyber crime was the only concern once the Internet was accessible to everyone, but the problem has evolved into something much greater, virtual crime. First we will be discussing the different categories of cyber crimes: real life cyber crimes and virtual crimes. There is a distinction between the two types of crimes, and Cyber crimes are being taken to a whole new level in crime sprees. Due to the evolution of the virtual world and cyber crimes, some virtual crimes have crossed over into the real world.

By definition cyber crimes are “unlawful acts wherein the computer is a tool or a target or both, it is also any form of threat to the public or private health or safety using the computer.” We have all heard about cyber crimes that range from financial crimes, cyber pornography, sales of illegal articles, online gambling, intellectual property crimes, e-mail spoofing, forgery, cyber defamation, and cyber stalking. Virtual Crime, as known as in game crimes, is similar to crimes that happen in real life, however, it happens in the virtual world. These crimes can range from theft, rape, murder, etc. We'll be discussing what happens when real world crimes meet the virtual world. Throughout the course of
this paper we will cover four different major types of cyber crimes with some real world examples, and what we can do to prevent some of these cyber crimes.

The first cyber crime we will be discussing is the computer intrusion, also known as hacking. Hacker is generic term for a computer criminal often with a specific specialty in computer intrusion. While other definitions peculiar to the computer enthusiast community exist, they are rarely used in mainstream context. Computer hacking subculture is often referred to as the network hacker subculture or simply the computer underground (Sherling). Hacking developed directly from Phone Phreaking, a group which explores the phone network without authorization. Today there remains an overlap between both technology and group members of Phone Phreaking (Price). More legitimate forms of hacking are derived from early computer users in academic institutions, especially the MIT hacks. Most historians trace the roots of the hacker underground to the Yippies, a 1960s counterculture movement which published the *Technological Assistance Program* newsletter (Yippies).

**Hacker Groups**

The network hacking subculture is supported by regular real-world gatherings or groups called hacker conventions or "hacker cons." Hacker conventions draw in more people every year, there are several conventions during the year including SummerCon (Summer), DEF CON, HoHoCon (Christmas), PumpCon (Halloween), H.O.P.E. (Hackers on Planet Earth), and HEU (Hacking at the End of the Universe) (Thomas). The conventions have helped expand the definition and solidify the importance of the network hacker subculture in today’s world.

**Hacking in the Media**
Hacking is such a large subculture in our world that has expanded into the area of media, including magazines, books, and even blockbuster movies. The most well known hacker magazines are: The Hacker Quarterly, Cult of the Dead Cow, and Legion of Doom. Hacker magazines are not just in print form, but they come in the form of ezines or internet sites. This gives hackers all over the world access to information in the ever changing culture. The magazines and ezines usually contain outdated information, however, they provide a way for people to improve the reputations of those who contributed by documenting their successes (Thomas).

Fiction and Non-Fiction books about hacking are now very common. They are another way the subculture of hacking has gone mainstream. Some popular titles featuring hackers include: Snow Crash and the Sprawl Trilogy by William Gibson (Staples). Hackers from the network hacking subculture often show an interest in fictional cyberpunk and cyber culture literature and movies. The most well known movies that portray hackers include: Live Free or Die Hard, Swordfish and Enemy of the State.

**Hacker Attitudes**

The term "hacker" has a number of different meanings. Several subgroups with different attitudes and aims use different terms to define themselves from each other, or try to exclude some certain group with whom they do not agree with. In a computer security context, it is often synonymous with a computer intruder. Hackers have what some call Hacker Ethic. Hacker ethic can also be referred to as hacker belief. Hacker belief can be broken down into the following ideals: All information should be free; Mistrust authority- promote decentralization; Hackers should be judged by their hacking, not bogus criteria
such as degrees, age, race, or position; You can create art and beauty on a computer; and Computers can change your life for the better (Taylor).

It is common among hackers to use aliases for the purpose of concealing identity, rather than revealing their real names. Members of the network hacking scene are often being stereotypically described as crackers by the academic hacker subculture, yet they see themselves as hackers and even try to include academic hackers in what they see as one wider hacker culture, a view harshly rejected by the academic hacker subculture itself (Stuart). Hackers have broken themselves up into various groups based on their hacking intension. There are six hacker groups: White hat, Grey hat, Black hat, Cyber terrorist, Script Kiddie, and Hacktivist.

The Following chart matches the hacker group names with their defined intensions (Cordingley).

<table>
<thead>
<tr>
<th>Hacker Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>White Hat</strong></td>
<td>A white hat hacker breaks security for non-malicious reasons.</td>
</tr>
<tr>
<td><strong>Grey Hat</strong></td>
<td>A grey hat hacker is a hacker of ambiguous ethics and/or borderline legality, often frankly admitted.</td>
</tr>
<tr>
<td><strong>Black Hat</strong></td>
<td>A black hat hacker is someone who subverts computer security without authorization or who uses technology for terrorism, vandalism, credit card fraud, identity theft, intellectual property theft, or many other types of crime.</td>
</tr>
<tr>
<td><strong>Cyber terrorist</strong></td>
<td>A Cyberterrorist uses technology to commit terrorism. Their intentions are to cause harm to social, ideological, religious, political, or governmental establishments.</td>
</tr>
<tr>
<td><strong>Script Kiddie</strong></td>
<td>A script kiddie is a non-expert who breaks into computer systems by</td>
</tr>
</tbody>
</table>
using pre-packaged automated tools written by others.

<table>
<thead>
<tr>
<th>Hacktivist</th>
<th>A hacktivist is a hacker who utilizes technology to announce a political message.</th>
</tr>
</thead>
</table>

**Common Methods**

A typical approach in an attack on an Internet-connected system is network enumeration: Discovering information about the intended target. Vulnerability analysis is defined as identifying potential ways of attack. Exploitation is defined as attempting to compromise the system by employing the vulnerabilities found through the vulnerability analysis. In order to do so, there are several recurring tools of the trade and techniques used by computer criminals and security experts (Ajay).

The following Chart list the 10 most common methods used by hackers and how they work (Blomquist).

<table>
<thead>
<tr>
<th>Security</th>
<th>A security exploit is a prepared application that takes advantage of a known weakness.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exploit</td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Vulnerability scanner</td>
<td>A vulnerability scanner is a tool used to quickly check computers on a network for known weaknesses.</td>
</tr>
<tr>
<td>Packet sniffer</td>
<td>A packet sniffer is an application that captures data packets, which can be used to capture passwords and other data in transit over the network.</td>
</tr>
<tr>
<td>Spoofing Attack</td>
<td>A spoofing attack involves one program, system, or website successfully masquerading as another by falsifying data and thereby being treated as a trusted system by a user or another program.</td>
</tr>
<tr>
<td>Rootkit</td>
<td>A rootkit is designed to conceal the compromise of a computer's...</td>
</tr>
</tbody>
</table>
security, and can represent any of a set of programs which work to subvert control of an operating system from its legitimate operators.

<table>
<thead>
<tr>
<th><strong>Social Engineering</strong></th>
<th>Social Engineering is the art of getting persons to reveal sensitive information about a system. This is usually done by impersonating someone or by convincing people to believe you have permissions to obtain such information.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Trojan Horse</strong></td>
<td>A Trojan horse is a program which seems to be doing one thing, but is actually doing another.</td>
</tr>
<tr>
<td><strong>Virus</strong></td>
<td>A virus is a self-replicating program that spreads by inserting copies of itself into other executable code or documents.</td>
</tr>
<tr>
<td><strong>Worm</strong></td>
<td>Like a virus, a worm is also a self-replicating program. A worm differs from a virus in that it propagates through computer networks without user intervention. Many people conflate the terms &quot;virus&quot; and &quot;worm&quot;, using them both to describe any self-propagating program.</td>
</tr>
<tr>
<td><strong>Keg Loggers</strong></td>
<td>A keylogger is a tool designed to record ('log') every keystroke on an affected machine for later retrieval.</td>
</tr>
</tbody>
</table>

A famous hacktivist event is the hacking of the NASA offices in Greenbelt, Maryland. The hacktivists inserted a worm named, WANK, Worms Against Nuclear Killers. "This worm ran a banner across all of NASA system computers as part of a protest to stop the launch of the plutonium-fueled, Jupiter-bound Galileo probe." No one is sure who the hacktivist was, but it was said to have cost NASA nearly a million dollars to clean up (Iozzio).

A recent hacking incident involved a 17-year-old boy known as "Dshocker." He was well
known in the online gaming world for attacking other hackers. He was recently charged and plead guilty to multiple computer felonies including, computer fraud, interstate threats and four counts of wire fraud. For thus he plead down to only get 11 months in a juvenile detention center. Had he been charged as an adult he would have faced a maximum of 10 years in jail and $250,000 in fines. (Wilson)

The second type of cyber crime is Piracy and Intellectual Property Theft. This is a very popular issue that still is ongoing. There are several laws that were passed and there are several revisions that are still being made today. Piracy of music, movies, software contain heavy fines, in 2006 two men pleaded guilty to music piracy charges, which violated federal copyright laws, so they were charged with 1 year of imprisonment and a fine of $100,000.

For electronic and audio-visual media, unauthorized reproduction and distribution is referred to as piracy. The unlawful downloading of copyrighted material and sharing of recorded music over the Internet in the form of MP3 and other audio files is more prominent now. Since the advent of the Internet, the invention of Mp3, and even after the demise of Napster, a series of infringement suits have been brought out by the American recording industry. Types of online piracy include software piracy, movie piracy, and music piracy.

The third type of cyber crime we'll be discussing is Internet fraud. Internet fraud is any form of fraudulent solicitation to prospective victims. There are several different types of Internet frauds such as Identity Theft Schemes and Purchasing Scams. Purchasing scam is a popular type of financial scam. Sub categories of purchasing scams include:

**Direct solicitations**
The most straightforward type of purchase scam is a buyer in another country approaching many merchants through spamming. These buyers buy, and then directly asking them if they can ship to them while using credit cards to pay.

**Online automotive fraud**

A fraudster posts a vehicle for sale on an online site, generally for luxury or sports cars advertised for thousands less than market value. The details of the vehicle, including photos and description, are typically lifted from sites such as eBay Motors and re-posted elsewhere. An interested buyer, hopeful for a bargain, emails the seller, who responds saying the car is still available but is located overseas. He then instructs the buyer to send a deposit via wire transfer to initiate the "shipping" process. The unwitting buyer wires the funds, and doesn't discover until days or weeks later that they were scammed.

The second most common type of online automotive fraud is where a fraudster feigns interest in an actual vehicle for sale on the Internet. The "buyer" explains that a client of his is interested in the car, but due to an earlier sale that fell through has a certified check for thousands more than the asking price. The “buyer” then pays with the high check, and he requests the seller to send the balance via wire transfer. If the seller agrees to the transaction, the buyer sends the certified check via express courier (typically from Nigeria). The seller takes the check to their bank, which makes the funds available immediately. Thinking the bank has cleared the check, the seller follows through on the transaction by wiring the balance to the buyer. Days later, the check bounces and the seller realizes they have been scammed. But the money has long since been picked up and is not recoverable.

**Cash the check system**
In some cases, fraudsters approach merchants and ask for large orders: $50,000 to $200,000, and agree to pay via wire transfer in advance. After brief negotiation, the buyers give an excuse about the impossibility of sending a bank wire transfer. The buyer then offers to send a check, stating that the merchant can wait for the check to clear before shipping any goods. The check received, however, is a counterfeit of a check from a medium to large U.S. Company. If asked, the buyer will claim that the check is money owed from the large company. The merchant deposits the check and it clears, so the goods are sent. Only later, when the larger company notices the check, will the merchant's account be debited.

Richard has had something similar to this happen to him. When he first bought his house, he needed roommates, because the amount of money required getting into the house. He put an ad out on Craigslist.org for a roommate. When he started getting hits, he found someone that looked like a good roommate. The person e-mailed quite a few times, and claimed to be in the Marines. He said he was coming from the east coast, and wanted to ensure he had a place to live. He claimed he was originally from Tennessee, and that he would pay two months rent, the deposit, and one extra months rent for the troubles. He sent Richard a cashier’s check for $5000 to cover everything and said to send him back what was left. He also said it was an advance from the Marines for moving out here, so he needed the rest to move. Richard was in dire need of a roommate, and had never heard of this type of scam before. In the end it cost him about $4000 because of the loss in rent, money sent back, and bank fees.

Fraudulent schemes often use the Internet to advertise purported business opportunities that will allow individuals to earn thousands of dollars a month in "work-at-home"
ventures. These schemes typically require the individuals to pay anywhere from $35 to several hundred dollars or more, but fail to deliver the materials or information that would be needed to make the work-at-home opportunity a potentially viable business. Often, after paying a registration fee, the applicant will be sent advice on how to place ads similar to the one that recruited him in order to recruit others, which is effectively a pyramid scheme.

**Money Transfers Fraud**

This type of Fraud consists of an employment offer to help transfer money to a foreign company, supposedly because it costs too much to do it through other methods (which is usually not the case). The prospective victim receives an email proposing a job offer. The request is the need to hire agents to receive payments for products in money orders, checks, or wire transfers and to resend the money via Money Gram or Western Union. The job promises 10% - 15% commission and the ability to earn $3,000 - $4,000 per month. The fraudsters will then send fake checks or postal money orders, in the hopes of getting the victims to cash those fake money instruments and then getting real money from the victims.

**Internet ticket fraud**

A variation of Internet marketing fraud is offering tickets to sought-after events such as concerts, shows and sports events. The tickets turn out to be fake or are simply never delivered. The proliferation of online ticket agencies and the existence of experienced and dishonest ticket touts have fuelled this kind of fraud in recent years. Many such scams are run by British ticket touts, though they may base their operations in other countries.
**Internet Marketing SEO Fraud**

This type of fraud involves a supposed Internet marketing specialist presenting a prospective client with detailed graphs and charts that indicate that his web site receives (x) thousands of hits per month, emphasizing that if you pay for his services you will succeed in getting a number clicks converted to customers or clients. When you receive no request for more information and no clients, the fraudster responds that it must be something your web site is not doing right.

**Phishing**

"Phishing" is the act of attempting to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business with a real need for such information in a seemingly official electronic notification or message (most often an email, or an instant message). It is a form of social engineering attack.

Phishing has been widely used by fraudsters using spam messages masquerading as large banks (Citibank, Bank of America) or PayPal. These fraudsters can copy the code and graphics from legitimate websites and use them on their own sites to create legitimate-looking scam web pages. They can also link to the graphics on the legitimate sites to use on their own scam site. These pages are so well done that most people cannot tell that they have navigated to a scam site.

**Auction and retail schemes online**

Fraudsters launch auctions on eBay or TradeMe with very low prices and no reservations especially for high priced items like watches, computers or high value collectibles. They received payment but never deliver, or deliver an item that is less valuable than the one
offered, such as counterfeit, refurbished or used. Some fraudsters also create complete web-stores that appear to be legitimate, but they never deliver the goods. An example of such a fraudulent site is marselle.com, jeremimora.com, thiesbikestore.com. They take payment but never shipped the order. In some cases, some stores or auctioneers are legitimate but eventually they stopped shipping after cashing the customers' payments.

**Stock market manipulation schemes**

These are also called investment schemes online. Criminals use these to try to manipulate securities prices on the market, for their personal profit. According to enforcement officials of the Securities and Exchange Commission, the 2 main methods used by these criminals are:

**Pump-and-dump schemes**

False and/or fraudulent information is disseminated in chat rooms, forums, Internet boards and via email (spamming), with the purpose of causing a dramatic price increase in thinly traded stocks or stocks of shell companies (the "pump"). As soon as the price reaches a certain level, criminals immediately sell off their holdings of those stocks (the "dump"), realizing substantial profits before the stock price falls back to its usual low level. Any buyers of the stock who are unaware of the fraud become victims once the price falls. When they realize the fraud, it is too late to sell. They lost a high percentage of their money. Even if the stock value does increase, the stocks may be hard to sell because of lack of interested buyers, leaving the shareholder with the shares for a far longer term than desired.

**Short-selling or "scalping" schemes**

This scheme takes a similar approach to the "pump-and-dump" scheme, by disseminating
false or fraudulent information through chat rooms, forums, Internet boards and via email (spamming), but this time with the purpose of causing dramatic price decreases in a specific company's stock. Once the stock reaches a certain low level, criminals buy the stock or options on the stock, and then reverse the false information or just wait for it to wear off with time or to be disproved by the company or the media. Once the stock goes back to its normal level, the criminal sells the stock or option at a profit.

There are times when a cyber crime crosses over into the real world incidents. How are we going to handle situations that cross that line?

In an article posted by fox news In 2006, there was a case of a young 14 year old girl named Megan that was being "cyber-bulled," and ultimately at the end she took her own life. A neighbor named pretended to be a 16 year old boy, named Josh. Megan and Josh exchanged messages via Myspace and at the end "Josh" told Megan that "the world would be a better place without you." Megan was distraught over the message and hung herself in the closet shortly after receiving the message. Prosecutors in the case said the adult neighbor knew of Megan condition, that she was depressed and emotionally fragile. The adult neighbor was cyber-bullying Megan because she was seeking revenge for her daughter.

**Some of the ways to protect yourself from Identity theft**

Since cyber crime has become a rising problem there has been several efforts to create laws to prosecute those that have committed the crimes. There are several projects in the work now to help prevent these crimes. Some of things people can do to prevent any efforts. The first intervention was made in the United States. The United States Department of Justice created a new sector called Computer Crime and Intellectual
Property Section. The Computer Crime and Intellectual Property Section was created for the purpose of Cyber Security Enhancement Act of 2002. Another cyber crime that is being enforced in the virtual world is found under the DMCA or the Digital Millennium Copyright Act. This act "provides a process for a copyright owner to give notification to an online service provider concerning alleged copyright infringement" (Secondlife.com). This act ensures that no other company or person profits off of another company or person. When someone is served with a notice, the content must be taken down immediately. This act is not only affecting the virtual world, it is affecting the media world as well. For example during the presidential elections this year, John McCain had to remove some "YouTube" content because he wasn't authorized to use some pop music soundtracks and debate footage (Wired.com).

Has anyone thought about what it take would create laws and who would be enforcing these laws? Others have and so have we. Who are the people that are going to be making these definitions? Our overall perception about these virtual crimes should have their boundaries, but there is no real monetary value, or is there? When someone steals another gamers "virtual asset" and sell it in real life for real monetary gain, that should be clearly listed as theft. When there are adults that are creating online characters in the second life doing criminal acts like having some sort of sexual act on a virtual child, should that be considered child pornography? Consider the facts, that there are two consensual adults that are using a second life to commit this act. There was no real child that was harmed. If someone was charged with child pornography would that be fair? This is crime is committed in a second life, where it is a fantasy or know as an intangible place be, policed and have the crimes punished?
Laws against cyber crime

The current laws against cyber crime are for actual crimes that occur in the real world. Although there are many virtual crimes occurring, the laws today only fight against real world crimes.

The Anti-phishing Act of 2005 criminalizes Internet scams involving fraudulently obtaining personal information. This act enters two new crimes into the U.S. Code. The first crime is creating a website that represents itself as a legitimate business and attempts to take personal information from its victim. The second crime is creating an email that represents itself as a legitimate business and attempts to take personal information from its victim. Both these crimes must have the intent to commit a crime of fraud or identity theft (Anti-phishing Act of 2005).

The laws against identity theft work mostly towards the prevention of identity theft and the penalties to those involved. The Comprehensive Identity Theft Prevention Act was created to provide for comprehensive identity theft prevention through regulations, penalties, and actions (Comprehensive Identity Theft Prevention Act, 2005). The Fair and Accurate Credit Transactions Act of 2003 was created to prevent identity theft, improve resolution of consumer disputes, improve the accuracy of consumer records, and make improvements in the use of consumer access to credit information (Fair and Accurate Credit Transactions Act of 2003). The Identity Theft Penalty Enhancement Act establishes penalties for aggravated identity theft (Identity Theft Penalty Enhancement Act, 2004). The Identity Theft and Assumption Deterrence Act of 1998 clarify the circumstances of the offense to assign to a certain punishment (Identity Theft and Assumption Deterrence Act of 1998). The Identity Theft Victims Assistance Act of 2002
was created to prevent the crime of identity theft and to mitigate the harm to individuals victimized by identity theft (Identity Theft Victims Assistance Act of).

The E-privacy act or the Encryption Protects the Rights of Individuals from Violation and Abuse in Cyberspace Act protects the privacy and rights of Americans, regarding law enforcement access to decryption assistance for encrypted communications and stored electronic information, to affirm the rights of Americans to use and sell encryption products (Encryption Protects the Rights of Individuals from Violation and Abuse in Cyberspace Act, 1998).

The Check Clearing for the 21st Century Act is used to improve the security and efficiency of the check collection system (Check Clearing for the 21st Century Act, 2003).

These laws about privacy protect the owners of computers and their personal information.

The Computer Owners’ Bill of Rights was created to protect owners of computers through the computer industry (Computer Owners’ Bill of Rights, 2003). The Online Privacy Protection Act of 2005 provides guidelines for an Internet service provider, online service provider or commercial website operators that they may not collect, use, or disclose personally identifiable information without following the proper guide lines (Online Personal Privacy Act of 2005). The SPY BLOCK (Software Principles Yielding Better Levels of Consumer Knowledge) Act was created to regulate the unauthorized installation of computer software and to require clear disclosure to computer users of certain computer software features that may pose a threat to user privacy (SPY BLOCK Act, 2005). The Spyware Control and Privacy Protection Act of 2000 provide disclosure
of the collection of information through computer software (Spyware Control and Privacy Protection Act of 2000).

The laws about spam and spyware provide protection for users from illegal spam, spyware, and other forms of collecting information. The Enhanced Consumer Protection Against Spyware Act of 2005 was created to provide the Federal Trade Commission with the resources necessary to protect users of the Internet from the unfair and deceptive acts and practices associated with spyware (Enhanced Consumer Protection Against Spyware Act of 2005). The U.S. SAFE WEB (Undertaking Spam, Spyware, and Fraud Enforcement with Enforcers beyond Borders) Act of 2006 was created to enhance Federal Trade Commission enforcement against illegal spam, spyware, and cross-border fraud and deception (U.S. SAFE WEB Act of 2006). The SPY ACT (Securely Protect Yourself Against Cyber Trespass) was created to protect users of the Internet from unknowing transmission of their personally identifiable information through spyware programs, and for other purposes (SPY ACT, 2004).

**Conclusion**

We can see how cyber crimes have evolved over the last couple of decades and there will be no stopping to the changes. The crimes start from the basic level of hacking, to the advance levels of stealing information from victims, to cyber theft, and to cyber harassment. There are several cases where victims are not emotionally distraught, but there have been several incidents where it has. The laws for cyber crimes needs to constantly evolve in a way that will keep up with the ever changing Internet system. The advancement of technology and how systems become obsolete quickly is affecting the security systems.
Sometimes the computer takes people to a place that isn't real, which makes them think life isn't real. This creates problems in the virtual world and real world. In virtual life people need to understand the difference between real life and virtual life. Just because the virtual world is lawless, doesn't mean real life is lawless, therefore, our recommendation is for a set of real life virtual laws. If the virtual world had laws associated with, the crimes seen today probably wouldn't be as common. Another great recommendation is to help virtual users cope with the transition between real and virtual life.
Antes, Conley, Morris, Schossow, Yee

**Works Cited**

http://www.cidap.gov.in/cybercrimes.aspx


Counterfeit U.S. Postal Money Orders Counterfeit postal money orders are reportedly in circulation (FDIC) March 9, 2005

A Common Currency for Online Fraud Forgers of U.S. Postal Money Orders Grow by Tom Zeller Jr (NYT) April 26, 2005


Kelly Burke: "British fraud ran Beijing ticket scam". The Sydney Morning Herald, August 6, 2008.


David Price: Blind Whistling Phreaks and the FBI's Historical Reliance on Phone Tap Criminality CounterPunch, June 30, 2008


Yippies | St. James Encyclopedia of Pop Culture | Find Articles at BNET.com