# Cyber crime

Law, Crime

Crime is on the rise just about everywhere these days, but nowhere has this up rise in crime become more apparent than in cyber space. Like so many other aspects of our lives, major fraud has gone high tech.

The FBI estimates that businesses alone lose an upwards of $1. 5 trillion annually as a direct result of cyber crimes. The number of these crimes has tripled in the past two years and the numbers continue to climb. (O'Leary & O'Leary) p. 287

Through the duration of this essay we will be embarking on a journey into the dark and seedy world of cyber crime. Within this text you will find, the definition of cyber crime, the most typical types of cyber criminals, as well as the most common forms of cyber crime.

The exact definition of cyber crime is still evolving. ( www. davislogic. com/cybercrime. htm ). Cyber crime, or computer crime, is an extremely broad term. This term is most commonly used to describe criminal activity committed where a computer or network is the source, tool, or target of a crime. Like traditional crime, cyber crime can take many shapes and occur at any time or any place.

When an individual is the main target of cyber crime, the computer can be considered a tool rather than the target. These crimes generally involve less technical expertise as the damage done manifests itself in the real world. In these types of cases the damage dealt is primarily psychological.

By now many of us are all too familiar with spam. Spam or spamming refers to the abuse of electronic messaging systems to send unsolicited bulk messages indiscriminately. While the most widely recognized form of spam is e-mail spam, the term can also be applied to similar abuses in other media.

Some of these abuses include; instant messaging spam, web search engine spam, spam in blogs, wiki spam, mobile phone messaging spam, social networking spam, as well as internet forum spam. As applied to email, specific anti-spam laws are relatively new, however limits on unsolicited electronic communications have existed in some forms for some time.

Another common crime plauging cyber space is identity theft. Internet identity theft is different from common identity theft in a few different ways. Common identity theft is different from common identity theft takes place after something is physically stolen from you like a wallet containing credit cards and a driver's license or an un-shredded credit card statement from your garbage bin.

The thief would take these stolen articles and use them to make a fraudulent purchase or something of that nature. Internet identity theft can be much more devastating than conventional identity theft at times due to the fact that most victims of internet identity theft are completely unaware that anything has been stolen from them until it is far too late.
Gone are the days when we had to step outside to purchase our

groceries, book flights, and vacations, or simply transfermoneybetween bank accounts.

Today, we can simply grab our checkbooks, debit cards or credit cards, sit down at a computer in the comfort and safety of our home, and complete these transactions with passwords and PIN numbers.

Thanks to advances intechnology, the types of transactions we can now complete online are virtually endless. Unfortunately, the increase in online transactions has been accompanied by an increase in online identity theft. Fraudulent access to personal information over the internet is increasingly prevalent and sophisticated.

Two forms of identity theft are at the forefront of this internet piracy are phishing and pharming. Both pharming and phishing are methods used to steal personal information from unsuspecting people over the internet. Phishing typically involves fraudulent bulk email messages that guide recipients to (legitimate looking) fake web sites and try to get them to supply personal information like account passwords. Pharming is in many ways similar to phishing.

Pharmers also send emails. The consumer, however, can be duped by the pharmer without even opening an email attachment. The consumer compromises his personal financial information simply by opening the email message.

The pharming email message contains a virus that installs a small software program on the end user’s computer. Subsequently, when the

consumer tries to visit an official web site, the pharmer's software program redirects the browser to the pharmer's fake version of the web site. This allows the pharmer to capture the personal financial information that the consumer enters into the counterfeit web site, and the consumer's account is again compromised.

The latest form of pharming does not require email at all. Password stealing Trojan horses can attack through Microsoft Messenger where key loggers are run. Key loggers are viruses that track a user's keystrokes on legitimate sites and steal passwords, allowing a thief to have access to a consumer's password for future fraudulent transactions.

The most common blunder people make when the topic of a computer virus arises is to refer to a worm or Trojan horse as a virus. While the words Trojan, worm and virus are often used interchangeably, they are not exactly the same.

Viruses, worms and Trojan horses are all malicious programs that can cause damage to your computer, but there are differences among the three, and knowing those differences can help you to better protect your computer from their often damaging effects.

A computer virus attaches itself to a program or file enabling it to spread from one computer to another, leaving infections as it travels. Like a human virus, a computer virus can range in severity. Some viruses may cause only mildly annoying effects while others can damage your hardware, software or files.

Almost all viruses are attached to an executable file, which means the virus may exist on your computer, however, it may not actually infect your computer unless you run or open the malicious program.

It is important to note that a virus cannot be spread without human action, such as running an infected program in order to keep it going. People continue the spread of a computer virus, mostly unknowingly, by sharing infecting files or sending emails viruses as attachments in the email.

In summary, the same types of fraud schemes that have victimized consumers and investors for many years before the creation of the internet are now appearing online.

In the process, they not only cause harm to consumers and investors, but also undermine consumer confidence in legitimate e-commerce and the internet.

People who commit cyber crime are cyber criminals. Like cyber crime, cyber criminals can take many forms. These criminals are typically terrorists, child predators, members of organized crime, employees, outside users, hackers and crackers.

It is important to point out the difference between hackers and crackers. Hackers are individuals who gain unauthorized access to a computer system simply for the thrill of it. Crackers do the same thing, but for malicious purposes.

Computer hacking is most common among teenagers and young adults, although there are many older hackers as well. Many hackers

are true technology buffs who enjoy learning more about how computers work and consider computer hacking an art form. They often enjoy programming and have expert level skills in one particular program.

For these individuals, computer hacking is a real life application of their problem solving skills. It is perceived as a chance to demonstrate, or showcase their abilities, and talents, and not an opportunity to harm others.

Cracking is the act of breaking into a computer system, often on a network. Contrary to popular belief, crackers are hardly mediocre hackers. Computer hackers were early pioneers of computing. These early pioneers were frantically dedicated to inventing and exploring how things worked. As a part of the sixties generation, these hackers were also prone toward being anti-establishment and somewhat disrespectful towards property rights.

Eventually a pair of these hackers, Steve Wozniak and Steven Jobs, hacked together the first commercially successful personal computer, the Apple. The sixties generation hackers flooded this new industry and many quickly attained positions of wealth and authority creating the information communications ecology that dominates Western life. Meanwhile, two things happened.

1. A new generation of hackers emerged.

2. The world economic and social order went completely digital, and so crime as we know it went digital as well.

It is somewhere at the interstices of the new generation of alienated young hackers ( they sometimes refer to themselves as " cyberpunks" ) and the world of sometimes organized crime that we locate the concept of the cracker. The term is, to some degree, an attempt by the now established older-generation hackers to separate themselves from computer crime.

The debate still rages as to what constitutes the difference between hacking and cracking. Some say that cracking represents any and all forms of rule breaking and illegal activity using a computer. Others would define cracking only as particularly destructive criminal acts.

Others would claim that the early hackers were explicitly anarchistic and that acts of willful destruction against " the system" have a place in the hacker ethos, and that therefore the term cracker is unnecessary and insulting.

This concludes our journey into the world of cyber crime. Through the course of our journey we have successfully defined cyber crime, identified typical cyber criminals, and discussed some of the most common forms of cyber crime.

The effects of cyber crime are far reaching. It would be a difficult task to find someone who has never been affected by malicious internet activity, or who does not at the very least know someone who has been negatively impacted by cyber criminals.

Advances in internet technology and services continue to open up innumerable opportunities for learning, networking and increasing

productivity. However, malware authors, spammers and phishers are also rapidly adopting new and varied attack vectors.

If the internet is to become a safer place, it is imperative to understand the trends and developments taking place in the internet threat landscape and maintain online security practices. Internet threats continue to increase in volume and severity.

It is important that computer users are on guard in order to make themselves less vulnerable to risks and threats. Staying on top of the trends and developments taking place in online security is critical for both industry researchers and all computer users alike.

References

O’Leary, T. J. , & O’Leary L. I. ( 2008 ) . Computing essentials introductory 2008.

New York: The McGraw-Hill Companies.

Cyber Crime. ( 2008 ) . Types of cyber crime. Retrieved September 27th , 2008 ,

From http://www. davislogic. com/cybercrime. htm