WEB OF SCIENTIST: INTERNATIONAL SCIENTIFIC RESEARCH JOURNAL
ISSN: 2776-0979, Volume 4, Issue 7, July, 2023

COMPUTER CRIME

Abdulakhatov Islombek
San Francisco State University, California, US

Abstract:
Computer crime is a growing concern involving the unauthorized use of computer technologies to commit illegal activities. This article explores various forms of computer crime, including hacking, identity theft, fraud, and cyber terrorism. It emphasizes the need to differentiate between computer crimes and computer security breaches, as well as the importance of understanding and preventing these crimes. The article also discusses the prevalence of online fraud schemes, the dangers of pedophiles using the internet, and the risks associated with social media. It concludes by highlighting the need for individuals to take proactive measures to protect their personal information and online activities. [1]

Keywords: Computer crime, computer security breach, hacking, identity theft, fraud, cyber terrorism, online fraud, pedophiles, social media, internet security

INTRODUCTION

Computer crime is a contemporary and innovative action which involves the illegal and unauthorized use of computer and computer-related technologies performed by individuals or group of people. Computer crime includes hacking into the system, stealing passwords, unauthorized downloading or copying data and software programs, which results in multibillion dollars financial cost and emotional damages. These crimes are included in computer administrators hacking into the computer system of employees of the company or even former's employees in order to credit card theft or fraud calls. Computer crimes not only take place in digital data but also includes drug trafficking, sexual exploitation, harassment and different kind of thefts. Today's tendency to increase of risk of computer crimes must be an important concern for people who are responsible for computer and network security and also for law enforcement organizations. In most cases computer crimes involve "computer-security brach", which is different from "computer crime", so some people think that these two terms are the same but they are not synonyms. These two terms seem like really close and similar to each other and computer professional who works with computer crime often got the incorrect assumption that these two factors are same. So, according to certification tests, computer security books, and other resources related to security beaches the main differences between those two that firstly, those

beaches are categorized into types such as privilege escalation, malware(virus, worm, rootlet, Trojan horse, and others), social engineering, password cracking, session hijacking, service denial, and phishing. These are categories of network security attacks, and it could be helpful to identify the mechanism of attack and choose the appropriate way to prevent that attack. On the other hand, computer crime is categorized into groups of activity which make point of specific criminal activity, these are cyberstalking or harassment, identity theft, illegal computer access, fraud, non-access computer crimes.

It is important for us to identify and realize the difference between computer crime and computer-security beaches. Overall, a computer security breach is a method of sidestep normal computer actions, where computer crime is an activity that facilitate criminal activity. In other words, computer crime could be performed without overcoming the normal computer operations, so computer crime could be committed without involving a security breach, where cyberstalking could be a good example for this case. It is important to know the meaning and strategies of these categories of computer crimes and let's discuss more details about these categories. I want to start with Identity theft which one of the most common digital crime nowadays. Identity theft is a process of acquiring personal data, where a commuter is pretended to be somebody. This form of activity is usually used for attaining of victim’s credit pieces of information. Identity theft is defined by the US Department of Justice in a way that identity theft and identity fraud is a type of crime in which someone obtains and uses another person’s personal information wrongfully in order to get an economic gain. As we said identity theft is mostly used for economic benefit, but it also could be used in other ways, which is not related to finance. For example, the perpetrator can use another person’s data to break someone's reputation in the community by ordering such pornographic material to embarrass the victim or just accessing information by hiding his actions. According to the data found by the Federal Trade Commission in 2005, 8.3 million Americans were suffered from identity theft crime, where 3.2 million cases were financial incidents and 1.8 million were an attempt to create a new account using other data. If we will calculate these numbers this will be a number of billions of dollars losses every year. There are several ways that someone can access private data such as hacking, phishing, discarded information, unauthorized access. Hacking is a process where perpetrators find a way to destroy the security system to gain access, which could be done in several ways including searching for the flow of the OS that can be operated to the target system. Phishing is an action to obtain someone's personal information, which is often done using e-mail or fake website creation which is similar to the original website. Discarded information is a data which

wasn't properly utilized and discarded which then became accessible for criminal. Examples could be old bills thrown in the trash, backup discs, paper, drives, etc. Unauthorized access is a situation where there is no access to somebody else rather the only person who has permission to access. An example of unauthorized access could be a patient's record which is sealed by a hospital employee or also a hacker breaking an OS. According to a 1996 US Sentencing Commission report, "defendants in white-collar (including fraud, forgery/counterfeiting, and money laundering) and computer fraud cases typically have no criminal history and are U.S. citizens, male, white, college graduates or high school graduates with some college."

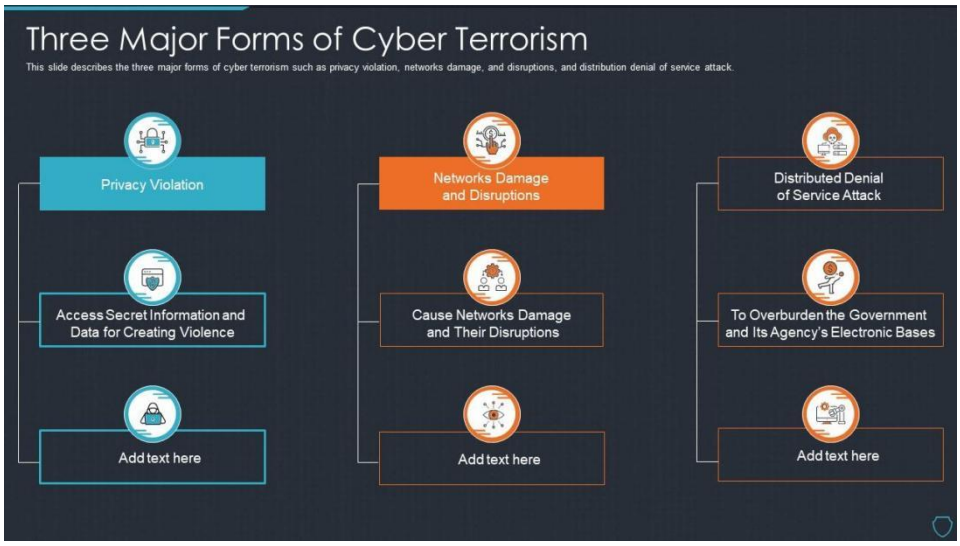
Another way of computer crime is a fraud technique that is easier to perpetrate on the internet, this technique is not new and existed even before the Internet. There are several types of fraud schemes and methods used to perpetrate crime actions. One of the most common ways of fraud is auction fraud, as we know that auction is a place where someone bids for winning an item, nowadays anyone could participate online or offline. Being auctions online created an opportunity for criminals to perform their illegal and fraudulent actions. Let's understand how online auction works, simply it is a way of participating in an auction using the Internet, where customers don't see the real item, after winning in the bidding you have to wait for it to be delivered. One of the best-fit examples for online auction could be eBay where anyone can search and find merchandise at a suitable price. But, it needs to be taken into consideration that any online auction websites could contain a peril, and there are questions, such as, will you receive the item you see on-site in good condition? We can list three types of online fraud, which are failing to send the item, sending different or less value item than shown in the advertisement, failure to mention all information about a product and conditions of sale. So, the most common clear-cut example of fraud is failure to deliver sold items and it is a simple and easy way to perpetuate. For example, after the victim has paid for the product, the seller doesn't send an item and takes the victim's money. Committer uses fake identification and email service in order to process an action. For better results, they involve more advertisements and several items at the same time and then collect money on auction and will not send any of the purchased goods. The second way of fraud is delivering of product with a poor value that is other than advertised. For instance, the seller promoted a new recently published book with a newer edition, but at a result ship you an old edition book with different quality. But there could be a mistake factor by the seller, when the wrong item was shipped by mistake of the seller, it could be known after contacting with the vendor. Mostly when the person sends a product with less value or quality it is likely to deliberate fraud. On the other hand, according to the Federal Trade Commission (FTC), there are other

lists of bidding fraud categories that are growing in popularity on the Internet. These are shill bidding when fraudulent sellers take part on the bid of the seller and increase a bid price in order to drive up the price. The other one is bid shielding is when fraudulent buyers place high prices to discourage other bidders, further the fake buyer retract high bid prices and the person in their team will able to buy the product at a lower price. Another way of deception is bid siphoning, when the same item is offered in another website at a low price, simultaneously this trick attracts customers. By purchasing off-site buyers could lose some obligation, which could be provided by the other official site such as guarantees, feedback forms or insurance. It is important to mention problems related with investment offers, which are becoming one of the popular activity today. Major trade companies make their income by cold calling, which is just calling people to attract them in investment in a specific stock. This way of trading stocks is generally a legal and legitimate way of working with investment. But we need to take into consideration that this also becomes an area for perpetrating stock fraud. While the Internet reached popularity it allowed to both real and fake investment opportunities to spread easily among the general public. Most of us usually see investment offers which are appeared in our email accounts, some of these e-mail notifications persuade you to be involved in a specific investment plan, in addition, there could be offered free stock opportunities as well. We need to filter online fraudulent activities because there could real and legitimate information which could help to investors. Let's briefly discuss some fraud investment schemes with some examples. Investment fraud could exist in a different form, one of the most common ways involves an e-mail that gives you suggestions of buying of stock with minimum investment and make a big amount of money. One of the most famous of these schemes is Nigerian Fraud, in this scenario, the main goal is to send an offer to a large random amount of recipient's email addresses, at a result even a small volume of responders could become a significant target for the perpetrator. Every e-mail contains a text which states that message is from a relative of some deceased government official or Nigerian doctor, who is well known social standing person. This method at the same time could increase the chance that the offer would be viewed positively. After gaining the confidence of the victim-perpetrator tries explain what to do. According to their plan, a person has a sum of money which should be transferred to another country, for security reasons that person is not able to use usual normal way. He would ask you to use your bank account to store their money for some time, and they will offer you a large fee for your service. If victim agreed with them then they will send you some official-looking documents which is similar to legal document via formal-looking rented e-mails, which is hard to investigate. Then they ask you to

send some money for transfer fee and taxes, if you send the money then you lost. This kind of scheme could be seen in social network messengers as well. If we think logically we should ask a question to ourselves. Why they trust me? Why do they want to hold their $5 million in my account, where could be a chance that I can steal their money? Unfortunately, there are people who become a victim of these fraud techniques.

When we talk about computer crime we need to include cyber terrorism. According to Lourdeau, 2004 cyber-terrorism is defined as "A criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services, where the intended purpose is to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social or ideological agenda (FBI, 2004)." There is a confusion on the meaning of "cyber terror" that it is a usage of cyberspace activities by terrorists or terrorist group. Terrorists use cyberspace as we all do for global information exchanges, planning, controlling of command, fundraising, and influence their public opinions. The national government may be considered these actions as cybercrime or just crime, but it will not be considered as "terrorism" as claimed by several legal systems. What makes different cyber terrorism from cybercrime and hacktivism. So when cyberspace is used as a weapon or target, when its involved psychological effect to the chosen audience, long term intention which influences social or political change and political decision making. What can we say about real cyber terrorism attacks which had occurred in history. The first one is a Nagorno-Karabakh conflict in 1999. On the authority of unconfirmed reports, hackers were able to change blood types in patience records in the hospital database, which caused the death of patients through receiving an incorrect blood transfusion. The second case is physical targeting of Telehouse telecommunication and in internet centers in 2006-2007 by Al Qa'ida related terrorist organization in the Docklands area of London. In August 2006, the effect of the attack was demonstrated by power disturbance at Telehouse, which took down hundred thousand customers and thousands of websites of Plusnet service for several hours. On the other hand, there are lots of cases where mass media defines ICT-disruption caused by cybercrime, hacktivism of system down by nature or mistake

defined as a cyber-terror act. However, according to the real definition of cyber terror, there is not a clear act of occurrence of cyber terrorism.



Above all, one of the problematic aspects in computer crime is a case related to pedophiles who use the Internet in order to traffic in child pornography and search a new victim. There is a program called “Catch a predator” which points out important facts which is that there is a sexual predator in every region who uses the Internet to find new sufferers and predators could everyone who around us. They may be any persons like programmers, teachers, physicians and also police officers. As ProtectKids.com mentions, graphic and also pornographic content could be accessible to anyone in the Internet and there is a possibility that our children accidentally could find it. Numbers show that every second over $3,000 spent for pornography, 28,258 view pornography, 372 of them are turn on an adult search term and every 39 minutes in the US a new pornographic movie made. The most common ways online predators act are first, teenagers attractive places on Internet, where predators visit chat rooms or social sites and begin a conversation with youths. Online predators are usually aware of current and popular trends which is interesting for youth including kinds of music, movies, games and fads. Conversations with minors are mostly about trending interests and predators firs look for key factors of the child who may become a target. These signs are a lonely child, a child who is not getting enough parent’s attention, a child with family-related problems and a child with low confidence. After identifying a target they will try to extend conversations in private chats and slowly easing sexual content. They do these steps really carefully and prepare a child to be comfortable with sexual topics.

Finally, they call the child for face-to-face meetings promising them activities like video games or watching a movie, which could then end with the sexual act. Knowing these factors of cyber crimes we always have to take the necessary precautions to protect ourselves, our family, money and personal belongings. We all spend lots of time online, but we are not realizing how we could become a victim by not obey some security rules. Some simple examples will help us understand how easily we can lose our data or personal pieces of information. For example, just by visiting the website with infected ads could damage our CPU power, typing credit card data to official-looking web sites, download funny video sent by our friends, and more ways that could bring us issues related to our privacy, then we spend our time, money and delete our personal data to wipe out infections. In other words, if we live in a "bad" neighborhood with the probability of crime, we will try to make precautionary action in order to save our dependability. We install some additional video cameras, lock doors, carry our money in a safe place, and other precautions actions which could assist our certainty. However, if we live in a good neighborhood with low offenses, then we feel more relaxed. But, in our online life, we all live in a "bad" neighborhood, for this reason, we all need to always practice online defense techniques, otherwise, it will be late when attackers succeed, which then will make feel us frustrated, angry and bring us some expenses. There are five basic habits that we have to know when we are online. These are device updates, enable two-factor authentication, use password manager, check antivirus update and installment, back up your data. In our daily life, we can hear some myths told by people where people do not believe that someone can hack them and steal any pieces of information. As an example let's list some ordinary myths. There is a wrong ideology like: if a hacker wants to access my data they anyway will do it because even huge companies or governmental systems get hacked. Other is: No one is interested in my data, which could be valuable to bad guys because I am not a famous person or public figure. Or like this: all applications in Google Play or in App Store are always monitored by security companies and they totally secure. There are people who believe that law enforcement agencies are able to catch bad actors and return back all staled data. In addition, there are some myths about file storage where people believe that when they store their data in Apple iCloud and in Google drive, it is safe because these platforms always back up files. Other groups of people believe that two-factor authentication takes too long, and strong and unique passwords could prevent hacking. Other people confident that websites with a lock symbol in the URL are not causing danger or public Wi-Fi with passwords is secure. There are also identity theft myths among the population. In particular, people agree that identity theft could be protected by credit monitoring and fraud alerts, or statements like we

don't need to shred sensitive documents because no one will sift garbage to steal data. Some people trust doctor's offices when they ask for a Social Security number when requested and other stories. In fact, we can secure and defend our online surroundings by obeying the rules above. Today tendency of using social media is increasing every second. Every 15-second new social media user is created by joining 3 billion of social media users. In the statistic, we can see how many bad actors are in social media. In Facebook, there are 2.2 billion user accounts, where 270 million are fake accounts. In Twitter, there are 1.3 billion user accounts, where 328 million active accounts and 23 million are fake bot accounts. Instagram has 800 million monthly active users, 64 of them are fake bots as well. LinkedIn covers 200 countries with 500 million members, however, we don't know the real number of fake accounts, because it is still in the studying process, but if we will use and apply the percentage we used for Facebook the amount could be more than 40 million fake users. Social media is a favorite and comfortable place for predators because they can create lots of profiles and posts to attract an audience, furthermore, it is an easy source to collect personal data. Bad actors already developed tools and techniques to collect information in a large scale from social media users and send personalized posts and messages on a big amount. Unfortunately, it works, 60% of phishing messages sent by social media are opened, which is two times more than phishing through emails. How we can protect our social media personal data. There are some techniques and ways which could help us to defend our information. These are enabling two-factor authentication, using of a password manager to manage and create unique passwords, enabling security and activity alerts, don't click unknown links, accepting friend requests by validating an individual's identity, think deeply about posting information.

CONCLUSION

In conclusion, as Information Technology is developing rapidly and with this computer crimes will take place all the time until we will not obey security preventing rules to protect our data and keep them safe. If we know the rules and categories of computer crime we can manage them and take actions against them. We also need to be aware of what our children do and how he or she spends time on the Internet. We should control access to computer for our children and explain to them rules about using of computer and the Internet. Additionally, teach them the danger of giving personal information on the web furthermore, there are software applications which will help the parent to control and manage the child's internet activity. These kinds of rules could be applied not only to children but for adults as well. We need to work together to protect our security, privacy, mind, and money. All of us have a right to

enjoy technologies, the Internet, online offers we can use. Protecting our security doesn't eventually mean that we need to keep something in secret, this is the protection of our and loved one's identities, which are our money, credit record, medical record, online activities, and others. Cyber warnings impact most parts of our lives, and we have to establish the right habits.

References

1. Easttom, Chuck; Taylor, Jeff. Computer Crime, Investigation, and the Law. Course technology PTR, 2010.
2. Moon, Byongook ; McCluskey, John D ; McCluskey, Cynthia P ; Lee, Sangwon. Gender, General Theory of Crime and Computer Crime: An Empirical Test. International journal of offender therapy and comparative criminology, 2013-04, Vol.57 (4), p.460-478.
3. Russell Brewer, Melissa de Vel-Palumbo, Alice Hutchings, Thomas Holt, Andrew Goldsmith, David Maimon. Cybercrime Prevention - Theory and Applications. Palgrave Pivot, Cham, 2019.
4. Babak Akhgar, Andrew Staniforth, Francesca Bosco. Cyber Crime and Cyber Terrorism Investigator's Handbook. Elsevier Science & Technology Books, 2014.
5. McDonough, Bart R. Cyber Smart : Five Habits to Protect Your Family, Money, and Identity from Cyber Criminals. John Wiley & Sons, Incorporated, 2019.
6. Mark Sherman. Introduction to Cyber Crime. Federal Justice Center, 2000.