Cyber Crimes

Sara Alkhateeb

Abstract: The world becomes closer as the Internet usage is growing daily. One of the Internet quality is to make the world a smaller place to live in for its users. Today, our society require a degree of connectivity between governments and citizens. The internet provides this connectivity and gives users many other benefits. However, The Internet provides a fertile environment for the growth of crime, ranging from stolen identity to phishing to Children abuse. With increased levels of awareness, cybercrimes have gathered a significant interest in research, industry, and normal people society. This paper analyzes cybercrime challenges and concerns, which included, cybercrime markets, cybercrime types, and cybercrime laws.

– – – – – – – – – – ◆ – – – – – – – – – –

Introduction

The Internet offers a level of connectivity that the world has never known before. In fact, the proportion of households with Internet access at home increased from 18% in 2005 to 46% in 2015[1]. However, for all its advantages, increased connectivity brings increased risk of hacking and fraud. Regrettably, people and organizations are not the only ones that have an online presence on the Internet. Hackers and identity thieves are following close behind. Substantially, the more people do and share online, the more vulnerable they may be to targeted attacks to steal their passwords and data. According to Cyber Crime Watch magazine, In U.S., about three-Quarters of the people have experienced some sort of cybercrime such as computer hacking, identity theft, or scam email messages [6]. Actually, about $485 million has spent on reported cybercrimes, According to the Internet Crime Complaint Center.

1. Cybercrime market

Have you ever wondered what exactly would happen to your credit card data after it's stolen? Cyber criminals would either use it for their own benefit or sell it on the online black market. The cybercrime markets or the online black markets are a collection of activates that operate all over the world which ranges from simple to extremely advanced. The under online economy in the virtual world rely on exploiting holes in online regulations. As its name suggests, cybercrime market is a pool of cybercriminals who seek to make dirty money out of unknown web users. By increasing at a rapid rate and impacting all businesses, cybercrime market became a major concern for the technology industry. The black market has already cost approximately $108 billion in the US [21]. By comparing cybercrime market with other underground markets, such as drugs, we can find that cybercrime market offers greater profit and carry less risk.

1.1 Structure

In the early to mid-2000s, hackers in black markets were focused on stolen credit card data services. Recently, they expanded their services to steal other users' social media and e-commerce accounts. Today, some hacking groups focus on serving services for a full lifecycle of an attack, while others offer a particular product or specialized service. [15] According to a number of experts and academic researchers, the days of the lone hacker are passed and cybercrime has become the domain of organized groups. Moreover, not only have computer specialists involved in cybercrimes but also, the conventional organized crime groups have extended their activates to involve digital crimes.[14] In fact, Nearly 80% of cybercrime acts could be the result of organized activates, according to McGuire's (2012) review. Depending on the group activity, cybercrime groups show different levels of the organization. For example, some groups focus on online targets, another group uses online tools to enable the real world crimes. The others, combine the online and offline targets.

There is an absence of evidence about the role and nature of organized cybercrime groups which hinders protection and development. [14] On the other hand and with three main group types, each group divided into 2 subgroups, McGuire (2012) build a suggestion typology of cybercrime groups based on a large sample of known cases. As the digital environment evolves, the cybercrime typology is likely to change.

The first type contains virtual cybercrime groups that operate online. This model is divided into two subtypes:

- Swarms are disorganized organizations without leadership. Swarms are most active in online activities such as hate crimes and political resistance.
- Hubs are more organized and structured than swarms. This model contains a hub of core criminals around which peripheral associates gather. Their online activates varied between phishing attacks, piracy, and online sexual offending. Credit cards black markets also can fit this model.

The second type is so-called 'hybrids' which contain offline and online offending. This model is divided as well into two subtypes:

- Clustered hybrid usually consisting of small groups that focused on specific activates. This type is similar in structure to hubs that move smoothly between online and offline activities.
- Extended hybrid is similar to clustered hybrid with less centralized. It contains subgroups that involved in different criminal activities.

The third type contains groups who operate offline using online technology. Type 3 groups, as the previous types, and based on their level of organization and cohesion, can be divided into two subtypes,

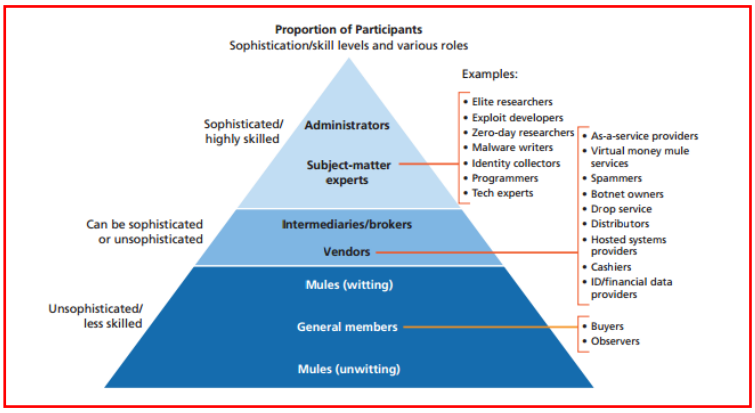
- Hierarchies groups are the best explanation of traditional criminal groups. These groups did some of their activities online. For example, some mafia groups who interested in prostitution has extended their works to pornography websites.
- Aggregate groups are temporary, less organized, and without a clear goal. These groups use online technologies in an ad hoc manner only which nonetheless can cause damage.

1.2 Participants

Because it is too easy to be involved in the black market than before, the number of people joining the market is likely to increase. [8] In the cybercriminal ecosystem today, there are more than three elements working side by side while the previous the system was made up of two to three elements, according to Dmitry Bestuzhev, head of Global Research and Analysis Team Latin America for the antivirus and Internet security company, Kaspersky Lab. If we look at the cybercriminal ecosystem as a hierarchy, we will see the following elements:

The first element in that hierarchy would be the organization administrators, who give the roles and manage the group, followed by followed by the subject- matter- experts. These people, who are the second element in the criminal ecosystem, play the main role in the system because they are the persons who have the knowledge of particular areas. The third element in that system would be the vendors or the intermediaries who act as a man-in-the-middle to verify the product and the buyer and seller as well. The fourth element in the hierarchy will be the money mules. The money mules are the people who transfer illegally acquired money on behalf of others in order to turn them into usable money. In this level, and virtual money mule services come into play. Money mules can be witting or unwitting. The fifth element in the system is the general members which include the Observers and the buyers, who can be individuals or organized groups.

The following figure shows the different levels of the cybercriminal system.



1.3 Products and pricing

In the real- world, when the supply goes up, prices go down. The cybercriminal underground economy goes through highs and lows just how like real-life demand affects the market supply.in cybercrime underground market and over the years, the prices of most products and services have been dropping. If we take the Toolkit products as an example of how much underground markets have grown, we can see that they have become much cheaper and more available.

A report published by the RAND Corporation titled "Market for Cybercrime Tools and Stolen Data" listed some of the products and services available and can be exchanged on the underground markets.

Goods and Services on the Black Market

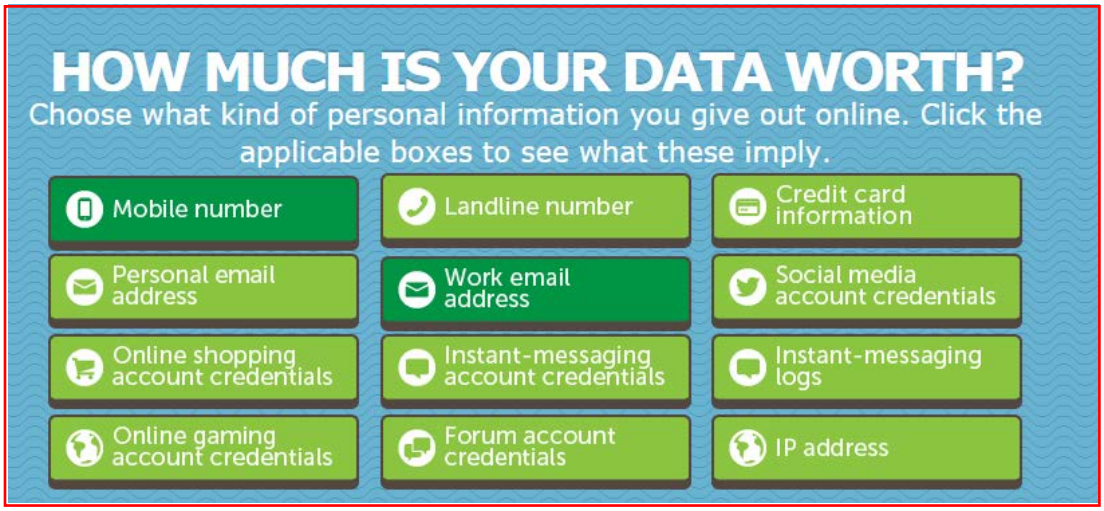
Category	Definition	Examples
Initial Access Tools	Enable a user to perform arbitrary operations on a machine, then deliver payloads; can automate the exploitation of client-side vulnerabilities (Zeltser, 2010)	• Exploit kit (hosted or as-a-service) • Zero-day vulnerabilities (and weaponized exploits)
Payload Parts and Features	Goods and/or services that create, package, or enhance payloads to gain a foothold into a system	• Packers • Crypters • Binders • Obfuscation / evasion
Payloads	Imparts malicious behavior, including destruction, denial, degradation, deception, disruption, or data exfiltration	• Botnet for sale
Enabling Services	Assist a user in finding targets or driving targets to a desired destination to use an initial access tool and/or payload; attack vectors and scaling methods	• Search engine optimization services • Spam services • Pay-per-install and affiliates • Phishing and spear-phishing services • Services to drive / find traffic • Fake website design and development
Full Services (as-a-service)	Package together initial access tools, payloads, and payload parts and features to conduct attacks on a customer's behalf; can provide the full attack lifecycle	• Hackers for hire • Botnets for rent • Doxing • DDoS as a service
Enabling and Operations Support Products	Ensure that initial access tools and hacking services (enabling or full-service) will work as needed, are set up correctly, and can overcome "speed bumps" or obstacles	• Infrastructure (e.g., leasing services, virtual private network [VPN] services, bullet-proof hosting, compromised sites and hosts) • Cryptanalytic services (e.g., password cracking, password hash cracking) • CAPTCHA breaking
Digital Assets	Digital assets are those items obtained from the target or victim (i.e., the hacked or stolen information)	• Credit card information (e.g., fullz, dumps, card verification value) • Account information (e.g., eCommerce, social media, banking) • Email login and passwords • Online payment service accounts • Credentials • PII/protected health information (PHI)
Digital Asset Commerce and Cyber Laundering	Digital asset commerce and cyber laundering, where appropriate, facilitate turning digital assets into cash	• Mule Services • Counterfeit goods and services (e.g., fake documents, identification, currency) • Card cloners, fake ATMs • Credit card processor services • Forwarding products services

[20] the most efficient deliverables in cybercrime industry vary from general "on- the – self" hacking products to custom malicious codes which fit the client's request.

The following list shows the most popular services delivered by the underground markets and their related prices.

- Consulting services such as botnet setup ($350-$400)
- Infection/spreading services (~$100 per 1K installs)
- Botnets & Rentals [Direct Denial of Service (DDoS) $535 for 5 hours a day for one week], email spam ($40 / 20K emails) and Web spam ($2/30 posts)
- Quality Assurance vs. Detection (Crypters, Scanners – $10 per month)
- Affiliate Programs ($5k per day is possible)
- Onshore & Offshore Hosting – Virtual Private Servers ($6 per month)
- Bulletproof/Fast Flux hosting and (VPNs & reverse proxies ($3 per month)
- Blackhat Search Engine Optimization (SEO) ($80 for 20K spammed backlinks)
- Inter-Carrier Money Exchange & Mule services (25% commission)
- CAPTCHA Breaking ($1/1000 CAPTCHAs)—Done through recruited humans
- Crimeware Upgrade Modules: Using Zeus Modules as an example, range anywhere from $500 to $10K.

On the other hand, TRENDMICRO, a global security software company, has published an online calculator that can estimate your personal information value, where the data could be sold and it related price.



With a quick calculation, will get the following:

YOU ARE WORTH:

BRAZIL: $1421 CHINA: $1675.5 RUSSIA: $205

IMPLICATIONS:

Annoyance/Distress	Cybercriminals can use the information they steal from you to cause you distress by spreading rumors or saying hurtful things.
Identity Theft	Cybercriminals steal your identity and use it in illegal dealings like blackmail, extortion, and other kinds of fraud.
Reputation Damage	Cybercriminals can soil your reputation, causing irreparable damage at times. On sites that require membership, this could get your account suspended.
Privacy Invasion	Personal information that you don't want anyone to know of may be exposed to the public.
Physical Endangerment	You may be unknowingly putting yourself at risk by revealing too much about yourself online.
Financial Loss	You may be subjected to extortion; compromised financial account may have unauthorized transactions. In online gaming sites, this could mean getting your virtual goods stolen.

As we can see from the previous calculation, the consumer can get the cheapest price in the Russian market, with the strongest competition, followed by Brazilian then Chinese market.

The Russian market, as we can see, has the strongest competition. A report released by TRENDMICRO, describe the Russian cybercrime market and shows that with $30, a criminal want to be can have access to a wide range of services and products. [16] For example, the average cost would be around $50 to $55 for VPN service for three months, Trojan backdoor is a mere $50, and a one-day DOS attack would cost $30 to $70.

As an example that demonstrates the underground market evolution level, we can see today that the consumer can get a guarantee on the product or service he got from underground market sellers. For example, the seller can guarantee that the credit card is good for a certain amount of money, or a particular malware is good for ten hours before it can be detected by any antivirus.

The Darkness of the internet which allow the criminals to disguise their identities make it more difficult to detect and arrest criminals. On the other hand, the anonymity of the internet made the cybercrimes to be performed easily and simply. As a result, the internet makes cybercrimes in the black markets more difficult to examine.

2. Cybercrime types

Cybercrime refers to any crime committed over the Internet. It is important to note that computer technology has to be involved, and when the use of it carry out an illegal activity, only then can it be classified as cybercrime. [4]There are many types of cybercrimes, some of them will be explained below.

2.1 Hacking

In 1878, before the Internet came into existence, a group of teenagers tried to discover the telephone circuits and switch systems in New York in order to know how they work. As a result, they kicked off the telephone system and hacked the system to see how it worked. However, MIT engineers were the first to popularize the concept of hacking in the 1950s and 1960s. In M.I.T, hacking was intended to be fun learning activities and harmless technical experiments. Later, the term began to be applied to less moral activates. [23]Today in computer security context, a hacker refer to someone who attempts to find and take advantage of weaknesses in a computer network or system, According to Wiki. However, it doesn't mean that the word "hacker" mean bad guy or criminal. Technical writers usually refer to hackers as a black, white, and gray hat. These terms define hackers group, what they do and why [10].

2.1.1 Hackers' Types

- **White Hat " ethical hackers"**
  Hackers aren't always known for being Internet ninjas. White hat hacker refers to a good guy, computer security expert who get paid to launch several attacks against companies in order to ensure that the information systems are secure. A white hat hacker who finds a security vulnerability in the system usually tell the developers, allowing them to improve the security and patch the system before it compromised.

- **Black Hat "unethical hackers"**
  Popular media seems to focus on black hat hackers in their movies. Black hat hacker is the bad guy, who break into network or computer, or create computer viruses. Their goal often to be destroying files, stealing data such as credit card numbers for some future purpose, or harvesting personal data to sell them to identity thieves. A black hat hacker who finds a security vulnerability in some systems would use them for his own advantage or sell them to criminal organizations on the black market.

- **Gray Hat**
  A Gray hat hacker is someone who is in between the previous two concepts. A gray hat hacker is a person who doesn't work for his own advantage nor to cause sabotage. However, he might attempt to compromise a company information system without permission. After the fact, he will contact the company and inform them about the vulnerability, allowing them to fix the problem. In fact, he compromised the system without permission, which is illegal. If a gray hat hacker found a security flaw on a website, he may disclose the flaw publically, giving the opportunity for the black hat hacker to take advantage of it before it was fixed.

2.1.2 Notable hacks

Because there is no fixed and uniform definition of the word Hack and because of the volume of hacking cases, it is difficult to list devastated hacks of all times. However, the cases shown below have something in common: each marks a big headline in the evolution of hacking. These hacks show how hackers have developed themselves by their ability to achieve new breakthroughs, and how the low has had to change in order to catch up with technology.

2.1.2.1 Malware:

The definition of malware for mobile devices can be driven from the master definition of malware, which is software that is intended to damage or disable computers and computer systems [11]. Malware includes a backdoor, Trojan, and worm. According to Techopedia [13], the backdoor is a program that provides unauthorized remote access to the device. It is also known as a trapdoor. This program is written by the programmer, who created its code and he is often the only one who knows it. Which makes backdoor a potential security risk. On the other hand, Trojan is a malicious program that performs actions that have not been authorized by the user, [13]. The Trojan appears as a fun or important file on the computer, but when the user runs that file it will perform unwanted actions such as deleting, blocking, modifying, or copying data. It also can disrupt the device performance.

The malware worm is a type of malicious software that self-replicates and distributes copies of itself to its network to infect other devices. What makes the worms extremely dangerous is the fact that they are independent viruses, which can replicate and spread on their own and infect other computers without the user's knowledge. Morris worm was one of the most significant malware outbreak of the dot-com era. Robert Morris, a graduate student at Cornell University, released what would come to be known as the first worm on the Internet. By writing a code of 99 lines and releasing them into the Internet, Morris started his experiment, not for damage. In contrast, his experiment was just to give him ideas of the size of the web. He concealed the worms origins by released it from MIT to exploit vulnerabilities in UNIX Sendmail, finger, and rsh, standard for the remote shell which allow the user to execute non- interactive programs on another system. Quickly, the design flow caused the worm to replicate itself and contaminated machines at a much faster rate than he expected, which caused a significant damage. Computers were becoming unresponsive to commands because some hidden tasks that were overloading these machines. Eventually, this incident forced many system administrators to cut off the Internet from their machines entirely. In 1990 and after the federal identified him as the source of the worm, Robert Morris was the first person to be convicted under the Computer Fraud and Abuse Act. Morris was sentenced to 400 hours of community service, a fine of $10,000, and three years of probation.

2.1.2.2 identity theft

Identity theft is a crime in where the cyber criminals impersonate individuals, usually for financial gain, by stealing their personal information or their credit card numbers. A hacker can use the personal information he stole it to open a bank account, purchase online, or borrow money. [11] A study released by Javelin Strategy & Research regarding the identity fraud stated that in 2014, Hackers have stolen approximately $16 billion from 12.7 million U.S. consumers. In fact, every two seconds in 2014, there was a new victim of identity fraud. According to the Insurance Information Institute, the following table shows how victims' information misused in 2014. Obviously, one of the highest percents was for Credit card fraud.

HOW VICTIMS' INFORMATION IS MISUSED, 2014 (1)

Type of identity theft fraud	Percent
Government documents or benefits fraud	38.7%
Credit card fraud	17.4
Phone or utilities fraud	12.5
Bank fraud (2)	8.2
Attempted identity theft	4.8
Employment-related fraud	4.8
Loan fraud	4.4
Other identity theft	21.8

Three of the most famous attacks that relate to identity theft and credit cards fraud where:

- **Phonemasters**
  In 1994, an international group dubbed the "Phonemasters" penetrated the computer systems of Sprint, AT &T, MCI WorldCom, Equifax, and even the FBI's National Crime Information center. The FBI addressed that the gang formed a fortune in approximately $1.8 million from this attack. They investigated in confidential databases and look around furtively for phone numbers of people the FBI and federal Drug Enforcement Agency were tapping. Moreover, they hacked and downloaded calling cards numbers and personal information from several companies' computer systems, and created telephone accounts for their own use. The first time the federal court gave the permission to the FBI to use "data tap" to monitor the hackers' activities was in this case. Through eavesdropping, the FBI was able to capture them as they exchanged stolen credit card numbers, but they weren't convicted until late 1999. One of the longest sentences for a hacker in U.S. history was for Corey Lindsly, the gang mastermind. He was sentenced to over 41 months in prison. Calvin Cantrell got 24 months, and John Bosanac 18 months.

- **Albert Gonzalez**
  [17]One of the largest thefts of credit and debit card numbers in American history has done by an American computer hacker called Albert Gonzalez. From 2005 through 2007, Gonzalez stole more than 45.6 card details from TXJ. Other companies, including shoe sellers DSW, BJs Wholesale Club, Dave & Busters, and OfficeMax, were also among alleged victims. In order to intercept the credit card data while it was being processed, He used an SQL injection attacks to deploy backdoors on companies' servers in order to install sniffer software. In 2005, moreover, Gonzalez was the mastermind of the breaching of 40 million records at CardSystsems Solutions, a credit card processing company. Gonzalez and again this time, He launched an SQL injection attack, which inserted a contaminated code into the database via the browser page, placing data into a file and send it back through FTP. Because the company never encrypted users' personal information, he exploited the weakness and gained access to account numbers, cardholders' names, and verifications codes for over than 40 million Visa and MasterCard members. In 2009, he sentenced to 20 years in prison, the longest federal prison sentence ever in the U.S. for hacking.

- **Lulzsec hacks Sony**
  Lulzsec is a black hat computer hacking group, who was responsible for several high-profile attack. On April 26, 2011, Sony Pictures Company claimed its online gaming and movie service had been hacked, with over 77 million accounts being affected, 12 million of which had unencrypted credit card numbers. The group was responsible for this attack using SQL injection attack and stealing customers' personal information. However, the group defended itself by saying that it wasn't a Sabotage attack, but it was just a retaliation for Sony's legal action against hacker George Hotz, who best known for hacking Sony's PlayStation 3. Moreover, the group was responsible for taking the CIA website offline. In 2011, the group was arrested by federal agents.

2.1.2.3 Phishing

Phishing is the method used to trick users in order to reveal persona information for individuals or get his credential/ company data for organizations. As technology becomes more advanced, as phishing techniques become also more advanced. Today, there are several ways and techniques for phishing used to steal users' data. Phishing scam refers to the phisher that may send an email to thousands of users, requesting from them to fill in personal information. After that, he can use this information for illegal activities. Some of this emails may have urgent notes for users to enter their bank credentials and their personal information for example in order to verify the account. Other emails may contain a link that directs them to a fake phishing website, which has the same look and feels as the legitimate website such as user's bank website.
Two of the most famous attacks that relate to phishing where:

- **The RSA Hack**
  Attacks are not limited to certain destinations, the world's top computer security companies could become a victim of an online attack as well. In two days, an attacker sent phishing emails entitled "2011 Recruitment Plan" to two small groups of employees in RSA Security Company. Unfortunately, the email grabs the attention of at least one employee, who in turn retrieved the email from his/ her junk mail and open the attached excel file. The spreadsheet contained malware known as "Zero – day" that used to install a backdoor by taking the advantages of Adobe Flash vulnerability (CVE 2011- 0609). After that, the attacker installed a remote administration tool called Poison Ivy RAT which gave the hacker a remote control to the employees' contaminated devices. Using these computers' information, he stole several account passwords belonging to other employees and used them to gain an access to other systems and access sensitive data. Finally, the hacker shifts the RSA files to the hacked machine in the company then to the hacker hosting provider. There were few traces left over. [19] However, According to an unclassified document from US-CERT, "there were three web addresses used in the intrusion, one of which includes the letters "PRC", which could refer to the People's Republic of China".

- **Saudi Aramco Shamoon**
  Saudi Aramco, Kingdom of Saudi Arabia's national oil company, has both the world's largest proven crude oil reserves, and largest daily oil production, which is based in Dhahran. The monstrous attack carried out against Saudi Aramco was the worst hack the world has ever seen. [24] According to CNNMoney, in fact, "When it comes to sheer cost, the recent cyber-attacks on Sony Pictures and the American government pale in comparison". In mid-2012, a scam email was open by a computer technician on Saudi Aramco information technology team. Moreover, he clicked on the bad link attached to the email. However, the actual attack began when most of the employees were on holiday on 15 August 2012 during the Islamic month of Ramadan. At that day, the employees noticed something really weird. Their computers just shut down without explanation. Their files began to disappear. Screens started flickering. A self- replicating virus struck about 30,000 of Saudi Aramco Windows- based machines that day. For political reasons, a group called "Cutting Sword of Justice" claimed their responsibility of the attack, which later dubbed Shamoon. The virus main function was deleting data from computer hard drives. Saudi Aramco IT employees made sure that every single computer was physically unplugged from the internet in order to stop the spread of the virus. The company was back online five months after the attack without knowing the perpetrator of this attack.

2.1.3 Prevention

Hacking is the biggest problem that can happen online. When it comes to hackers attacks, both the individuals and the companies are targeted. In fact, everything that connects to the internet can get hacked. There are some tips that should be followed, vary from the individuals to the companies, in order to keep the personal data or the information systems secure.

- **Individuals**

Even if is a big challenge to secure your computer or phone from expert hackers, people can reduce the possibility of computer's being hacked into by implementing security measures. By following a few tips, users can mitigate the risk of hacking. The biggest factor in protecting the user's computer from hackers is the user himself. Vigilance is the only thing needed to avoid installing anything the user don't trust from any source such as website, email, or even pop-up windows. Moreover, hackers attack where they see weakness. Hackers can take advantage of a system that has flaws because it hasn't been updated recently. Up to date operating systems, firewalls, and Antiviruses can ban hackers and viruses from getting access to the system. Moreover, by using a unique, long, and strong password for each website the user sign up to, the possibility of guessing the password and stealing personal information becomes less. Today, most of the online shopping and banks website are using HTTPS connection, which keeps users' personal information protected. Users should always deal with this type of connections.

- **Organizations:**

Many employees make it easy for hackers to attack their computers by using easy to guess passwords. In fact, about 65% of the employees use same passwords for different purposes including websites, access to corporate applications, and personal banking, According to a report by infosecurtiy Europe. By using the public computers and/or free Wi-Fi such as Internet cafes and airports, the hacker can easily capture the employee credential by installing a keylogger. Managers should make sure that they have educated employees in order to make sure no sensitive data is being sent or received through an unsecured connection, and they should make Awareness sessions for them on a regular basis.

It is good for companies to use a Two-step authentication, which sufficiently great cuts down on cybercrime. This will typically require access to employee mobile phone where an SMS can be sent to him with a verification code. Company manager or owner should put some laws that could reduce the risk of attacks. In addition, companies can pay white hat hackers to find bugs in their systems. By monitoring what do employees download to their computers can protect the company network from malware or hackers. To protect the company network from known vulnerabilities, IT department should keep current with security patches. This is a simple and effective means of securing the company network. Finally, Managers can make sure that only those who are knowledgeable are making changes to the network by limiting the employees who are granted administrator access.

2.2 Intellectual property theft

Intellectual property (IP) theft refers to the theft of materials that are copyrighted. In fact, intellectual property theft via the Internet is one of the internet crimes that held accountable by law. Copyright is a form of protection provided by the law to the creator of the work to exclusively distribute, print, or publish the work in public. Movies, computer software, and computer games are the most commonly copyrighted materials stolen online. Today, theft of IP affects the entire sector of the U.S. economy. In reality, U.S. is losing millions of dollars annually due to IP pirates [5]. For example, cyber criminals sell pirated computer software, games, music, movies, or programs to millions of internet users. This causes the original creator undoubted financial loss because the company that actually produced the real product loses these sales. Before the spread of the Internet, IP crimes involved a lot of time and labor. Theft should copy the movie or music into tapes, produce them physically, and transport them for sale. In addition, an individual had to make the sale in person. However, the spread of computing and the Internet file sharing networks have made it easier to IP pirates. Not only does theft of materials that are copyrighted, but also theft of trade secrets, and trademark violations considered IP theft as well.

Generally, a trade secret is some information used in a business. Theft of trade secrets means the theft of methods, technologies, ideas, or any sensitive information from all types of industries. Trade secrets included recipes, business plans, marketing strategies, computer algorithms, or manufacturing techniques. Trade secret gives the business the competitive edge. By stealing trade secrets, the business competitive edge will be damaged therefore the economic base of a business.

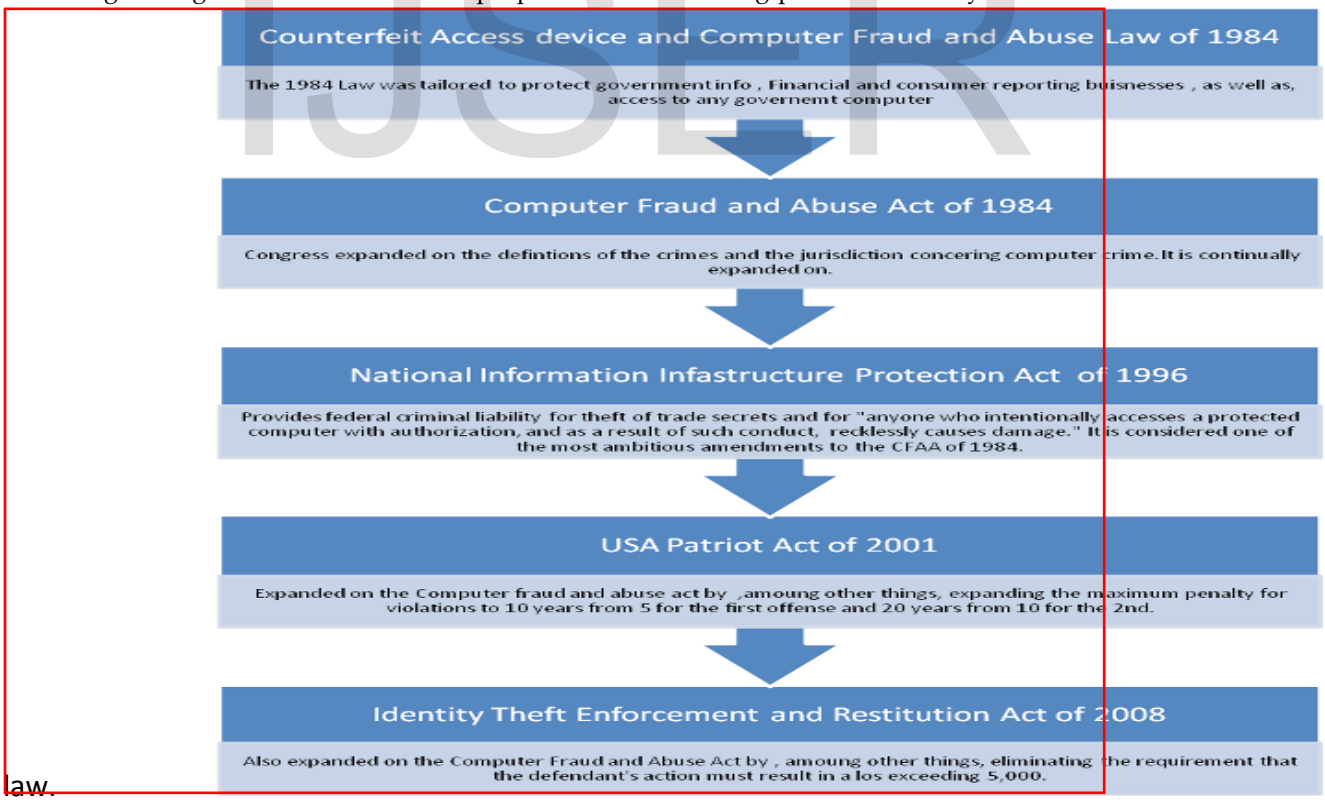
A trademark is a registered name, design, or any combination thereof that can be used only by the product's owner. A trademark violation refers to any counterfeiting or copying brand name products and selling them as the original product.

According to FBI, preventing intellectual property theft is a priority for its criminal investigative program. Moreover, much of the IP theft take place overseas, where laws are often not sufficiently strict and enforcement more difficult [2]. The FBI is focusing on theft of trade secrets and product infringements of products that may affect consumer's safety and health.

Obviously, Intellectual theft could have formed in several forms. However, all of them are performing to the same conclusion namely destroying the country's economy.

3. Cybercrime Laws

The internet provides a place for cyber criminals to prosper. As a result, new laws appeared against cyber-crimes to reduce them. The prosecution was based on the physicality of a criminal possession before the Internet. Currently, however, computer forensic digital emerged in response to cybercrimes. The criminal justice system which response to cybercrimes is the development of the field of digital forensic. Digital forensics is the science of gathering, preserving and analyzing the data found in digital devices, according to dcccd [9]. The goal of this science is to maintain the evidence in its most original form while performing a structured realization by gathering, identifying, analyzing, and validating the digital information for the purpose of reconstructing past events a way that can be used in a court of law.



Cybercrime laws vary internationally. The above image shows computer crimes laws in U.S. [12]. Similar to the Computer Fraud and Abuse Act law which has enacted in 1984 in U.S.A, Australia has enacted it in 2001 to address this type of crimes. Moreover, Similar to the points that have addressed by the U.S. federal cybercrime legislation, the

Unauthorized Computer Access Law has enacted in Japan in 1999 to cover some computer crimes areas. An international agreement is important to fight cybercrimes because political is not a hurdle to conducting it. For example, 30 countries, Including the United States, signed the Council of Europe's Convention on Cybercrime to solve the problems posed by criminal activity on computer networks. Countries who signed this Conventions agree to have criminal laws within their own nation to address cybercrimes. Moreover, it enables international cooperation in combating crimes through provisions to obtain and share electronic evidence.

Conclusion

In the past years, cybercrimes have been an emerging problem. People are now realizing that their computer devices, personal Information, and Information systems are under attack. This paper had discussed three major aspects of cybercrimes. The first aspect was the cybercrime markets which they really do match the world's technology trends. Today, cybercrimes markets contain computer specialists as well as conventional organized crime groups who have extended their activates to involve digital crimes. Cybercrime groups show different levels of organization depending on their activities such as virtual cybercrime groups that operate online, hybrids groups, and groups who operate offline using online technology. Moreover, because it is too easy to be involved in the black market than before, the market tend to become more complex and hierarchical. In addition, the paper discussed some of the services that can be obtained on the market and their prices. The second aspect the paper discussed was two types of the cybercrimes which are, hacking and Intellectual property theft. Hacking issues are probably the biggest problem that can happen online.in this paper. Malware could be classified as a kind of hacking and Morris worms is an example in this context. In addition, identity theft is another kind of hacking. Phonemasters, Lulzsec, and Albert Gonzalez are examples for groups and individual hackers who were identified through identity theft. Phishing was the last kind of hacking discussed in this paper. Phishing attacks that have been waged on both RSA security and Saudi Aramco Company are two of the well-known attacks in this context. Finally, the paper gave some tips and guidelines to individuals and companies for protection or to mitigate the risk of attacks. Intellectual property theft is the second type of cybercrimes that has discussed in the paper. The paper discussed what the meaning of IP is and how much this type of cybercrimes can affect and destroy the country's economy. The third last aspect was how U.S. and other countries deal with cybercrimes. Moreover, how do they deal with International cybercrimes? At the end, technology is critical. However, society and corporate culture play a central role in stopping the big breaches.

References

1. (n.d.). Retrieved November 29, 2015, from https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf
2. (2010, April 16). Retrieved November 29, 2015, from https://www.fbi.gov/about-us/investigate/white_collar/ipr/ipr
3. 10 hacks that made headlines. (2012, May 16). Retrieved November 29, 2015, from http://www.techworld.com/security/10-hacks-that-made-headlines-3358062/
4. Cross Domain Solutions. (n.d.). Retrieved November 29, 2015, from http://www.crossdomainsolutions.com/cyber-crime/
5. Cyber Crime - Intellectual Property Theft. (n.d.). Retrieved November 29, 2015, from http://law.jrank.org/pages/11992/Cyber-Crime-Intellectual-property-theft.html
6. Cyber Crime Facts. (n.d.). Retrieved November 29, 2015, from http://science.opposingviews.com/cyber-crime-1523.html
7. Cybercrime. (n.d.). Retrieved November 29, 2015, from http://itlaw.wikia.com/wiki/Cybercrime
8. Cybercriminals Work in a Sophisticated Market Structure. (n.d.). Retrieved November 29, 2015, from http://blogs.wsj.com/riskandcompliance/2013/06/27/cybercriminals-work-in-a-sophisticated-market-structure/
9. Digital Forensics. (n.d.). Retrieved November 29, 2015, from https://www.dcccd.edu/CD/DCC/Comps/DigFor/Pages/default.aspx
10. Hacker Hat Colors Explained: Black Hats, White Hats, and Gray Hats. (n.d.). Retrieved November 29, 2015, from http://www.howtogeek.com/157460/hacker-hat-colors-explained-black-hats-white-hats-and-gray-hats/
11. Identity Theft and Cybercrime. (n.d.). Retrieved November 29, 2015, from http://www.iii.org/fact-statistic/identity-theft-and-cybercrime

12. Jurisdiction of Cybercrime. (n.d.). Retrieved November 29, 2015, from http://nickleghorn.com/ist432/US.html
13. Lookout. (n.d.). Retrieved November 29, 2015, from https://www.lookout.com/resources/know-your-mobile/what-is-a-mobile-threat
14. McGuire, M. (2012). Organised Crime in the Digital Age. London: John Grieve Centre for Policing and Security
15. Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime. (n.d.). Retrieved November 29, 2015, from http://www.cybercrimejournal.com/broadhurstetalijcc2014vol8issue1.pdf
16. Russian Underground 101. (2012). Retrieved November 29, 2015, from http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf
17. TJX suspect indicted in Heartland, Hannaford breaches. (2009, August 17). Retrieved November 29, 2015, from http://www.theregister.co.uk/2009/08/17/heartland_payment_suspect/
18. The 11 Worst Online Security Breaches - 4. Sony's PlayStation Network. (2011, April 20). Retrieved November 29, 2015, from http://www.complex.com/pop-culture/2012/05/the-11-worst-online-security-breaches-hacks/sony-psn-hack
19. The RSA Hack: How They Did It. (2011, April 2). Retrieved November 29, 2015, from http://bits.blogs.nytimes.com/2011/04/02/the-rsa-hack-how-they-did-it/
20. The "company" cybercrime seen by Fortinet. (2012, December 26). Retrieved November 29, 2015, from http://securityaffairs.co/wordpress/11282/cyber-crime/the-company-cybercrime-seen-by-fortinet.html
21. Welcome to Market Realist. (n.d.). Retrieved November 29, 2015, from http://marketrealist.com/2015/09/growing-technology-repercussions-cybercrime-threats/
22. What is a Backdoor? - Definition from Techopedia. (n.d.). Retrieved November 29, 2015, from http://www.techopedia.com/definition/3743/backdoor
23. Https://en.wikipedia.org/wiki/Hacker_ (computer_security). (n.d.). Retrieved November 29, 2015, from https://en.wikipedia.org/wiki/Hacker_(computer_security)
24. Time, A. (n.d.). The inside story of the biggest hack in history. Retrieved November 29, 2015, from http://money.cnn.com/2015/08/05/technology/aramco-hack/