A STUDY OF CYBER CRIME

Sumandeep Kaur
(BCA MSC-IT UGC NET)
Assistant Professor in Computer Science
Department of Govind National College Narangwal Ldh
141204 Punjab India.

ABSTRACT

Cybercrime is defined as a crime where a computer is the object of the crime or is used as a tool to commit an offense. A cyber criminal may use a device to access a user's personal information, confidential business information, government information, or disable a device. It is also a cybercrime to sell or elicit the above information online. There are common-sense steps that can prevent or reduce having one's financial information stolen online, as well as to avoid other scams and threats, but cybercrime in these areas persists largely due to a lack of consumer education. In this paper the concept of cybercrime and it its various types have been studied. Finally, it concluded with various techniques to be used to prevent from cyber attacks.

KEYWORDS*:* Authentication, CAPTCHA**,** Security, Precautions, Attacks.

INTRODUCTION

Criminals use new technologies to commit cyber attacks against governments, businesses and individuals. These crimes know no borders, either physical or virtual, cause serious harm and pose very real threats to victims worldwide. Pure cybercrime' refers to crimes against computers and information systems, where the aim is to gain unauthorized access to a device or deny access to a legitimate user. Traditional forms of crime have also evolved as criminal organizations turn increasingly to the Internet to facilitate their activities and maximize their profit in the shortest time. These 'cyber-enabled' crimes are not necessarily new – such as theft, fraud, illegal gambling, the sale of fake medicines – but they have taken on a new online dimension. Cybercrime is progressing at an incredibly fast pace, with new trends constantly emerging. Police must therefore keep pace with new technologies, to understand the possibilities they create for criminals and how they can be used as tools for fighting cybercrime.

TYPES OF CYBERCRIME & HOW TO PREVENT THEM

In order to protect yourself you need to know about the different ways in which your computer can be compromised and your privacy infringed. In this section, we discuss a few common tools and techniques employed by the cyber criminals. This isn't an exhaustive list by any means, but will give you a comprehensive idea of the loopholes in networks and security systems, which can be exploited by attackers, and also their possible motives for doing so.

1 BOTNETS:-

A botnet is a collection of internet-connected devices, which may include personal computers (PCs), servers, mobile devices and internet of things (IoT) devices that are infected and controlled by a common type of malware. Users are often unaware of a botnet infecting their system. Botnets are networks from compromised computers that are controlled externally by remote hackers. The remote hackers then send spam or attack other computers through these botnets. Botnets can also be used to act as malware and perform malicious tasks.

EXAMPLE

When the Mirai botnet was discovered in September 2016, Akamai was one of its first targets. Our platform continued to receive and successfully defend against attacks from the Mirai botnet thereafter. Akamai research offers a strong indication that Mirai, like many other botnets, is now contributing to the commoditization of DDoS. While many of the botnet's C&C nodes were observed conducting "dedicated attacks" against select IPs, even more were noted as participating in what would be considered "pay-for-play" attacks. In these situations, Mirai C&C nodes were observed attacking IPs for a short duration, going inactive, and then re-emerging to attack different targets.

HOW TO DETECT AND PREVENT BOTNET ATTACKS

Botnet attacks frequently go undetected because they involve a wide network of devices that operate in the background of a user's device and occupy little bandwidth There is no one-size-fits-all solution to botnet detection and prevention, but manufacturers and enterprises can start by incorporating the following:

- **Strong user authentication method.**
- **Secure remote firmware updates.** Only firmware from the original manufacturer should be permitted.
- **Secure boot.** This ensures the device only executes code produced by trusted parties.
- **Advanced behavioral analysis.** This detects unusual behavior in IoT traffic.
- **Automation, machine learning and artificial intelligence (AI).** These enable response to new threats at digital speeds before they cause serious harm.

2. PHISHING

Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords. The information is then used to access important accounts and can result in identity theft and financial loss.

EXAMPLE: The first phishing lawsuit was filed in 2004 against a Californian teenager who created the imitation of the website "America Online". With this fake website, he was able to gain sensitive information from users and access the credit card details to withdraw money from their accounts.

PREVENT PHISHING ATTACKS:

1. Learn to Identify Suspected Phishing Emails

2. Check the Source of Information From Incoming Mail

3. Never Go to Your Bank's Website by Clicking on Links Included in Emails

4. Enhance the Security of Your Computer

5. Enter Your Sensitive Data in Secure Websites Only

6. Have the Slightest Doubt, Do Not Risk It

3. HACKING

Hacking refers to activities that seek to compromise digital devices, such as computers, smartphones, tablets, and even entire networks. And while hacking might not always be for malicious purposes, nowadays most references to hacking, and hackers, characterize it/them as unlawful activity by cybercriminals—motivated by financial gain, protest, information gathering (spying), and even just for the "fun" of the challenge.

Many think that "hacker" refers to some self-taught whiz kid or rogue programmer skilled at modifying computer hardware or software so it can be used in ways outside the original developers' intent. But this is a narrow view that doesn't begin to encompass the wide range of reasons why someone turns to hacking. (For an in-depth look at hackers, read "Under the hoodie: why money, power, and ego drive hackers to cybercrime" by Wendy Zamora.)

HACKING PREVENTION

If your computer, tablet, or phone is at the bull's-eye of the hacker's target, then surround it with concentric rings of precautions:-

- Download a reliable anti-malware product (or app for the phone), which can both detect and neutralize malware and block connections to malicious phishing websites. Of course, whether you're on Windows, Android, a Mac, an iPhone, or in a business network, we recommend the layered protection of Malwarebytes for Windows, Malwarebytes for Mac, Malwarebytes for Android, and Malwarebytes business products.

- Only download phone apps from the legitimate marketplaces that police themselves for malware-carrying apps, such as Google Play and Amazon Appstore. (Note that Apple policy restricts iPhone users to download only from the App Store.) Even so, every time you download an app, check the ratings and reviews first. If it has a low rating and a low number of downloads, it is best to avoid that app.

4. VIRUSES

A computer virus is a malicious software program loaded onto a user’s computer without the user’s knowledge and performs malicious actions. Computer viruses never occur naturally. They are always induced by people. Once created and released, however, their diffusion is not directly under human control. After entering a computer, a virus attaches itself to another program in such a way that execution of the host program triggers the action of the virus simultaneously. It can self-replicate, inserting itself onto other programs or files, infecting them in the process. Not all computer viruses are destructive though. Viruses spread when the software or documents they get attached to are transferred from one computer to another using a network, a disk, file sharing methods, or through infected e-mail attachments. Some viruses use different stealth strategies to avoid their detection from anti-virus software. For example, some can infect files without increasing their sizes, while others try to evade detection by killing the tasks associated with the antivirus software before they can be detected. Some old viruses make sure that the "last modified" date of a host file stays the same when they infect the file.

HOW TO PROTECT FROM VIRUSES

1. Keep your software up to date
2. Don’t click on links within emails
3. Install a *virus protection* or an antivirus software and perform regular updates

4. Back up your computer

5. Use a strong password

6. Use a firewall and enhance your browser’s Privacy Settings

7. Use pop-up blocker and adjust your User Account Control

5. LOGIC BOMBS

A logic bomb is a piece of malicious code that hackers insert into a software or operating system. This code lies dormant until a specific condition occurs. These conditions could be a pre-determined time (often referred to also as a time bomb) or a specific command that the user types in. Once the conditions occur, the logic bomb will wreak havoc on your computer system. Some examples include corrupting your hard drive, stealing your data, or taking your device over.

Hackers often use logic bombs in accordance with viruses, worms, and Trojan horses in order to achieve maximum damage. Indeed, these types of malware, when employed as a logic bomb, will behave in one manner, and then change tactics drastically once the material condition is met.

EXAMPLE

Some logic bombs can be designed to take effect on a specific date or a specific event. For example, Christmas, New Year, or Independence Day. You'll probably have your guard down on those days, which will make it much easier for the hacker to achieve their goals. These logic bombs can also be referred to as time bombs.

HOW TO PREVENT LOGIC BOMBS

There are a few disaster recovery plans in place to deal with logic bomb attacks. However, there are also things you can do to prevent them from happening in the first place.

- Firstly, it is important to periodically scan all files. Logic bombs are hidden among code, so it is therefore very important to check compressed files to make sure there is nothing hidden in them.
- Secondly, it is very important to keep your anti-virus software updated regularly. If the software doesn't have all the patches for the most current viruses, logic bombs will be able to slip through in the form of whatever new strain of malware exists.
- Avoid pirated software. This is one of the most popular methods for delivering malware.
- Train employees on spotting phishing emails. Email attachments is another very common malware delivering system.
- Never trust unsecured web links. They may lead you to an infected site.

6, DENIAL-OF-SERVICE ATTACK

A "denial of service" or DoS attack is used to tie up a website's resources so that users who need to access the site cannot do so. Many major companies have been the focus of DoS attacks. Because a DoS attack can be easily engineered from nearly any location, finding those responsible can be extremely difficult.

EXAMPLE

The GitHub Attack Happened in Feb 2018

The biggest DDoS attack so far took place in Feb 2018. This attack was directed at GitHub, a well-known online code management service used by numerous developers.

At its peak, it was sending packets at a speed of 126.9 million/sec, with incoming traffic at a rate of 1.3 Tbps

HOW TO HELP PREVENT DOS ATTACKS

If you rely on a website to do business, you probably want to know about DoS attack prevention. A general rule: The earlier you can identify an attack-in-progress, the quicker you can contain the damage. Here are some things you can do.

1: Get help recognizing attacks

Companies often use technology or anti-DDoS services to help defend themselves. These can help you recognize between legitimate spikes in network traffic and a DDoS attack.

2: Contact your Internet Service provider

If you find your company is under attack, you should notify your Internet Service Provider as soon as possible to determine if your traffic can be rerouted. Having a backup ISP is a good idea, too. Also, consider services that can disperse the massive DDoS traffic among a network of servers. That can help render an attack ineffective.

3: Investigate black hole routing

Internet service providers can use “black hole routing.” It directs excessive traffic into a null route, sometimes referred to as a black hole. This can help prevent the targeted website or network from crashing. The drawback is that both legitimate and illegitimate traffic is rerouted in the same way.

7. EMAIL BOMBING AND EMAIL SPAMMING

Email bombing is characterized by an abuser sending huge volumes of email to a target address resulting in victim’s email account or mail servers crashing. The message is meaningless and excessively long in order to consume network resources. If multiple accounts of a mail server are targeted, it may have a denial-of-service impact. Such mail arriving frequently in your inbox can be easily detected by spam filters. Email bombing is commonly carried out using botnets (private internet connected computers whose security has been compromised by malware and under the attacker’s control) as a DDoS attack.

This type of attack is more difficult to control due to multiple source addresses and the bots which are programmed to send different messages to defeat spam filters. "Spamming" is a variant of email bombing. Here unsolicited bulk messages are sent to a large number of users, indiscriminately. Opening links given in spam mails may lead you to phishing web sites hosting malware. Spam mail may also have infected files as attachments. Email spamming worsens when the recipient replies to the email causing all the original addressees to receive the reply. Spammers collect email addresses from customer lists, newsgroups, chat-rooms, web sites and viruses which harvest users' address books, and sell them to other spammers as well. A large amount of spam is sent to invalid email addresses.

HOW CAN I PREVENT LIST BOMBING?

- Use confirmed opt-in: A confirmed opt-in process sends an email with a unique link to new signups. Once they've clicked the link, you can verify that they are a real user who owns the address they've signed up with, and at that point, you can begin sending them welcome email. List bombers won't be able to verify that address, and will be prevented from causing damage.
- Implement a reCAPTCHA: reCAPTCHA utilizes technology to determine if a human is using your platform. It can require entering a series of numbers or checking a specific box to prove that the person signing up is a real pers

8. WEB JACKING

Web jacking derives its name from "hijacking". Here, the hacker takes control of a web site fraudu-lently. He may change the content of the original site or even redirect the user to another fake similar looking page controlled by him. The owner of the web site has no more control and the attacker may use the web site for his own selfish interests. The knowledge about cyber security is very important as they can be aware of the hackers. These websites are hacked by using password hacking system which is of two types .at first ,pre dictionary words are used multiple times to crack the password and secondly, Brute force is used where the hackers guess the passwords of the users by trying all combination of numbers, symbols and alphabets.

HOW DO I PREVENT WEB JACKING?

- **Software Update:** Web jacking has been resolved in the past by some software update. Update your browsers and add-ons.
- **Block Scripts:** It's advisable to install Noscript addon if you're using Firefox. They provide protection against frame based attack, by preventing scripts from loading.
- **Frame Busting:** Frame burst is a method implemented by developers using javascript to restrict frame usage."It is a technical approach that requires the Web developer to send an HTTP response

header, named X-FRAME- OPTIONS, with HTML pages to restrict how the page can be framed." says Linda Richard, at Brighthub, in a blog post.

9. CYBER STALKING

Cyber stalking is stalking that takes place using electronic devices or the internet. It is the technological harassment directed towards a specific individual. There are several **forms of cyber stalking** that can take place including:

- placing orders for delivery in someone else's name
- gathering personal information on the victim
- spreading false rumors
- encouraging others to join in the harassment
- threatening harm through email
- creating fear and paranoia for someone else
- hacking into online accounts

Cyber stalking can cause extreme distress for the victim. It can impact their career, personal relationships, and quality of life. Often times victims do not know who the perpetrator is and start wondering if they are being watched or followed. The common denominator amongst cyber stalking cases is that they are typically against the law, unsolicited by the victim, and unrelenting.

HOW TO AVOID CYBER STALKING?

1. Update Your Software

Keeping your software up-to-date may not be the first thing that springs to mind when you think about cyber stalking prevention. However, regular software updates are crucial when it comes to preventing information leaks.

2. Hide your IP address

Many applications and services reveal your IP address to the person with whom you're communicating. This may seem unimportant, but this information is directly related to your personal data. To mask your IP address you can use a Virtual Private Network (VPN). This hides your real IP address and replaces it with from a location of your choice, so you could even appear to be in a different country. It also encrypts all of your internet traffic, keeping it safe from the prying eyes of hackers.

3. Maintain good digital hygiene

‘Digital hygiene’ is a new term but represents a very important topic, especially with regard to social networks. Maintaining good digital hygiene helps protect you from cyber harassment, cyber bullying and cyber stalking.

Adjusting privacy settings is one of the first steps you can take to “clean up” your accounts. Most social media platforms and some other types of online accounts will let you adjust who can see your profile and contact you.

4. Avoid disclosing sensitive information

Surprisingly, many people constantly share personal information about themselves, even outside of social media platforms. By filling out questionnaires or submitting applications for coupons, you are increasing the likelihood of someone getting their hand on your personal data and possibly making cyber stalking more accessible.

10. DATA DIDDLING OR DATA ALTERATION

Data Diddling is unauthorized altering of data before or during entry into a computer system, and then changing it back after processing is done. Using this technique, the attacker may modify the expected output and is difficult to track. In other words, the original information to be entered is changed, either by a person typing in the data, a virus that’s programmed to change the data, the programmer of the database or application, or anyone else involved in the process of creating, recording, encoding, examining, checking, converting or transmitting data. This is one of the simplest methods of committing a computer-related crime, because even a computer amateur can do it. Despite this being an effortless task, it can have detrimental effects.

EXAMPLE

"Examples of data diddling are forging, misrepresenting, to counterfeiting documents; exchanging valid computer tapes or disks with prepared replacements; keyboard entry falsifications; failure to enter data; and neutralizing or avoiding controls."

PREVENT DATA DIDDLING

- **Vulnerability and Compliance Management**

Using a vulnerability and compliance management (VCM) tool or at the very least completing a vulnerability assessment will help you identify the gaps, weaknesses, and security misconfigurations within your physical and virtual environments. VCM can continuously monitor your infrastructure and IT assets for vulnerabilities and compliance weaknesses and configuration best practices.

- **Regular Audits on Security Posture**

Completing regular audits to identify potential new gaps in compliance or governance will help in validating your security posture. A security audit will be more a more thorough assessment of your security policies compared to the vulnerability assessment or penetration testing. A security audit considers the dynamic nature of the organization as well as how the organization handles information security.

- **Train & Educate Your Staff**

After completing your security policy audits, you can then enforce a written employee policy around data privacy and security. You will want to hold regular security trainings so that all employees are aware of these newly created policies – after all, people cannot voluntarily comply with unfamiliar policies. When establishing your security policy for employees

11._IDENTITY THEFT AND CREDIT CARD FRAUD

Credit card fraud is a potential consequence of identity theft. Here, a thief steals your credit card information and then makes purchases in a store or online. Most credit card companies have a liability limit of $50. This means that even if a thief has charged thousands of dollars to your card, you'd likely only have to pay $50. More often than not, credit card companies simply wipe out any charges that are the result of fraud.

In contrast, identity theft involves much more than a few fraudulent charges. Identity thieves can steal your personal information to open a new line of credit, open a new credit card or obtain a false ID in your name. Unlike credit card fraud, there's no liability limit. That means you might end up paying for *all* the damage caused by an identity thief.

IDENTITY THEFT PROTECTION

Before examining the services available, try these common-sense, no-cost measures to protect against identity theft and fraud:

- **Guard your information online.** These days, many of us do most of our shopping and banking on the web. With all those account numbers and passwords floating around, it's easy for someone to nab your information and go on a spree.
- Clear your logins and passwords. This is especially important if you've been working on a public computer. Change logins and passwords monthly.
- Pay for online purchases with your credit card, which has better guarantees under federal law than your online payment services or your debit card.
- **Monitor your bank and credit card statements.** Check your accounts regularly so you know when something's awry. Purchases you didn't make should be obvious—like a gas fill-up halfway across the country.
- **Verify your mailing address with the post office and financial institutions.** Identity bandits may fill out change of address forms so that delinquent credit notices remain off your paper billing radar.

12. SALAMI SLICING ATTACK

Salami Slicing is a form of financial cyber attack where the criminal takes an amount of money that is so insignificant that a single case is completely unnoticed. The amount of money taking in every case would be very little (say Rs.5), however the number of cases would be large. Therefore, each individual victim would incur a very small loss, but the criminal would make a sizeable amount. For example, a bank employee inserts a program into the bank's servers that takes away a very small amount (say Rs.5) a month from every account. None of the account holders would notice this unauthorized removal of money because it is too small to notice. However due to the sheer number of accounts from which money is taken, the employee would make a sizable amount of money every month.

PREVENTION OF SALAMI SLICING

a) Banks have to update their security so that the attacker doesn't familiarize himself/herself with the way the framework is designed. before finally hacking into it states Raj B Lonsane.

b) Raj B Lonsane adds that banks should advise customers on reporting any kind of money deduction that they aren't aware that they were a part of. Whether a small or big amount, banks should encourage customers to come forward and openly tell them that this could mean that an act of fraud could very well be the scenario.

13. SOFTWARE PIRACY

The unauthorized copying of software. Most retail programs are licensed for use at just one computer site or for use by only one user at any time. By buying the software, you become a *licensed user* rather than an owner (see *EULA*). You are allowed to make copies of the program for backup purposes, but it is against the law to give copies to friends and colleagues.

Software piracy is all but impossible to stop, although software companies are launching more and more lawsuits against major infractors. Originally, software companies tried to stop software piracy by copy-protecting their software. This strategy failed, however, because it was inconvenient for users and was not 100 percent foolproof. Most software now requires some sort of registration, which may discourage would-be pirates, but doesn't really stop software piracy.

Some common types of software piracy include counterfeit software, OEM unbundling, soft lifting, hard disk loading, corporate software piracy, and Internet software piracy.

TIPS FOR PREVENTING SOFTWARE PIRACY

1. Read the BSA "Guide to Software Management."
2. Establish office policies for purchasing software and respecting intellectual property rights.
3. Explain to employees the importance of protecting computers from unlicensed software.
4. Compare the number of software installations to the number of licenses.
5. Obtain any licenses needed for compliance.
6. Schedule regular software audits to guard against piracy.

13. CYBER EXTORTION

Cyber extortion is the act of cyber-criminals demanding payment through the use of or threat of some form of malicious activity against a victim, such as data compromise or denial of service attack. Cyber extortion permeates actions such as ransomware, email ransom campaigns, and distributed denial of service (DDoS) attacks. Cyber extortionists have several common techniques for breaking into your computer hardware, software, and networks and incapacitating them until you pay a fee.

HOW DO I PROTECT MYSELF FROM ONLINE EXTORTION?

Everything you do on the Internet leaves behind a "digital footprint," which unscrupulous people can use against you. Therefore, it's important to put as little sensitive information online as possible.

Don't think you're safe because you only share things with your close friend group. Even if you send a communication or image in confidence, there's no guarantee that the person you send it to will keep it secret. If you're not sure whether to trust someone with something personal or intimate, it's best to err on the side of caution and keep it to yourself. Similarly, don't store anything on your online devices that you wouldn't want anybody else to see; this way, you can still be safe if someone hacks your computer, phone, or tablet.

Here are some more tips to protect yourself:

- Don’t open any emails or attachments from strangers.
- Regularly monitor your bank account and credit report for any suspicious activity.
- Use strong passwords and avoid using the same password for multiple websites.
- Never give out any personal information via email.
- Adjust your social media security settings to provide the highest level of protection.
- Before entering any personally identifiable information on a website, check that the site is using “https” or the status bar displays a “lock” icon.

14. CYBER BULLYING

Cyber bullying is the harassment or bullying executed through digital devices like computers, laptops, smartphones, and tablets. The platforms where cyber bullying can occur include social media, chat rooms, and gaming platforms where people can view and participate in the sharing of content. The different types of cyber bullying involve causing humiliation through hateful comments on online platforms/apps, or through SMS or messaging. It comprises posting, sending or sharing negative, nasty or false information about another individual for causing humiliation and character assassination

The most common places where cyber bullying occurs are:

- Social Media, such as Facebook, Instagram, Snapchat, and Tik Tok
- Text messaging and messaging apps on mobile or tablet devices
- Instant messaging, direct messaging, and online chatting over the internet
- Online forums, chat rooms, and message boards, such as Reddit
- Email
- Online gaming communities

PREVENT CYBER BULLYING

1. Be Wary of Your Child’s Online Activities

In this digital era, children are growing up with technology at their fingertips. Thus, different types of cyber bullying have become a household occurrence. Teenagers and adolescents are more vulnerable to cyber bullying as they have limited understanding of the good and the bad.

As a parent, it is your responsibility to be aware of your child’s online activities in order to prevent cyber bullying. Be cognizant of the apps and digital media that your child is using. It is imperative that you ensure that your child engages more in offline activities than an addiction to computers, online gaming, and smartphones.

2. Watch out for These Signs

The following are some warning signs that your child is being cyber bullied or is cyber bullying others.

- Considerable increase or decrease in your child's usage of a mobile, laptop or tablet
- Display of emotional responses such as sadness, anger or happiness to the activities on their device
- The tendency to avoid discussion on their online activities
- Hiding of the device screen when others are close by
- Indifference to social activities and gatherings, and outdoor activities
- Sudden deactivation of their social media accounts or opening of new ones
- Becoming depressed and withdrawn

15. CHILD PORNOGRAPHY

Child sexual abuse material (legally known as child pornography) refers to any content that depicts sexually explicit activities involving a child. Visual depictions include photographs, videos, digital or computer generated images indistinguishable from an actual minor. These images and videos that involve the documentation of an actual crime scene are then circulated for personal consumption. More recently, live-streaming sexual abuse has begun to surface. In these instances individuals pay to watch the live abuse of a child via a video streaming service. This type of abuse is incredibly difficult to detect, due to its real-time nature and the lack of digital evidence left behind following the crime. Though child sexual abuse material (CSAM) is a global issue, the United States remains one of the largest producers and consumers of child abuse content in the world. It's important to understand the true nature and pervasiveness of child sexual abuse material to convey the urgent need to address this crime

Since every country has a different legal stand on this subject matter, pornography is rampant online. However, according to the Indian Constitution, largely, pornography falls under the category of obscenity and is punishable by law. Child pornography is a serious offence, and can attract the harshest punishments provided for by law. Pedophiles lurk in chat rooms to lure children. The internet allows long-term victimization of such children, because the pictures once put up, spread like wild-fire, and may never get taken down completely. Internet crimes against children are a matter of grave concern, and are being addressed by the authorities, but this problem has no easy solution.

CONCLUSION:

New technologies create new criminal opportunities but few new types of crime. What distinguishes cybercrime from traditional criminal activity? Obviously, one difference is the use of the digital computer, but technology alone is insufficient for any distinction that might exist between different realms of criminal activity. Criminals do not need a computer to commit fraud, traffic in child pornography and intellectual property, steal an identity, or violate someone's privacy. All those activities existed before the "cyber" prefix became ubiquitous. Cybercrime, especially involving the Internet, represents an extension of existing criminal behavior alongside some novel illegal activities.

REFERENCES

[1] Prashant Mahajan & Penelope forbes, (Nov 2012), Digital crime and forensics project
http://www.slideshare.net/prashant3535/digital-crime-forensics

[2] M.E.Kabay, (2008), A Brief History of Computer Crime: An Introduction for Students. MSIA School of Graduate Studies, Norwich University.

[3] Eoghan Casey (2011). Digital Evidence and Computer Crime (3rd Ed.). Elsevier Inc publisher.

[4] Nabat Arfi, Shalini Agarwal, (2013) "Assessment of Types of Cyber Crime Faced By Elderly Across Residence", The International Journal of Engineering and Science (IJES), Vol. 2, No. 6, PP 01-03.

[5] United Nations Office on Drugs and Crime (UNODC), (Feb 2013), Comprehensive Study on Cybercrime.

[6] Adel Ismail Al-Alawi, (2014), "Cybercrimes.Computer Forensics and their Impact in Business Climate:Bahrain Status", Research Journal of Business Management, Vol.8, No. 3, PP 139-156.

[7] Johan Burger, (Sep.2013), National crisis' of cybercrime poses major threat to SA business
http://www.bdlive.co.za/opinion/2013/09/18/national-crisis-of-cybercrime-poses-major-threat-to-sa-business

[8] Pierluigi Paganini, (Nov.2013), 2013 – The Impact of Cybercrime. http://resources.infosecinstitute.com/2013-impact-cybercrime/

[9] 1 million cyber crime victims in SA, (Nov 2013) http://businesstech.co.za/news/general/48854/1-million-cyber-crime-victims-in-sa/

[10] Daniel Shane, (Sep. 2011), Cybercrime 'costs UAE $612m'. http://www.itp.net/586045-cybercrime-costs-uae-612m

[11] George Mason University (School of Public Policy), Virginia Economic Development Partnership's (VEDP), (2014), Cyber Security Export Market: Saudi Arabia.

[12] PwC Middle East Economic Crime Survey, (Feb 2014), Economic Crime in the ArabWorld.

[13] Computer Crime Investigation & Computer Forensic, (1997) Information Systems Security, Vol. 6 No. 2, p56, p25.

[14] AARON PHILIPP, DAVID COWEN, CHRIS DAVIS (2010). Hacking Exposed Computer Forensics (2nd Ed.). McGraw-Hill

[15] Yunus Yusoff, Roslan Ismail and Zainuddin Hassan, (June 2011) "Common Phases of computer Forensic Investigation Models". International Journal of Computer Science & information Technology (IJCSIT), Vol. 3, No. 3

[16] ACPO guidelines,(July 2007) http://7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence_v4_web.pdf

[17] Judge Stein Schjolberg, (Dec.2011), Global Phenomenon and its Challenges Courmayeur. ISPAC International Conference on Cybercrime, Italy.