Int. j. adv. multidisc. res. stud. 2023; 3(6):82-86

Received: 13-09-2023
Accepted: 23-10-2023

International Journal of Advanced Multidisciplinary Research and Studies

ISSN: 2583-049X

Analysis of Information System's in Cyber Crimes through Wireless Networks

[1] Dr. A Radha Krishna, [2] A Krishna Veni

[1] Professor & HoD, Department of CSE (AI & ML), Pragati Engineering College, Surampalem, East Godavari District, Andhra Pradesh, India

[2] Assistant Professor, Department of CSE, Aditya Engineering College, Surampalem, East Godavari District, Andhra Pradesh, India

Corresponding Author: **Dr. A Radha Krishna**

Abstract

Growth in using the computer and wirless network with internet has changed the way of daily life, the use of internet increased, but interactions with people face to face communication decreased. By means of the introduction of new customer operations though online using Internet are increased like payment, business, pubic organizational works, entertainment, social media. Accessing of internet through wireless network not only increased the communication but also increased the issues which affect the life of people. High-speed Internet access i.e., Broadband which consists of a number of high-speed communication technologies such as: wireless network, fibers, cable modems etc. The usage of broadband increased issues for users by hacking their passwords and accessing their personal information, Money, business and so on.

Keywords: Cybercrime, Extortion, Theft, Phishing, Attacks

1. Introduction

As we aware of the word "Internet "is interconnection of computer networks of entire globe which uses the IP suite (TCP/IP) protocol to communicate between devices and networks. Among all telecommunication networks, wireless internet connection network is most risk factor, with high mobility, easy installation and no wired required; the wireless internet is being commonly used these days. Wireless internet is different from traditional wired network because in wireless signals travels through wind and which would capable to a large extent vulnerable for those who have targets and follows to perform harmful behavior to others. Using of wireless internet users are increased enormously and the improvement of new computation taken place. At the same time issues also arised in present constitutions and providing security to data becoming difficult. Threats causing lose of information from different scales like smaller organizations, individuals, governmental or public institutions too by Cybercriminals. As usage of wireless internet access increasing at the same time the problems also gradually increasing for people who are accessing internet for different purposes. The issues caused by the Broadband are following:

- Cybercrime Threats/ e-crime
- Cyber Space threats
- Phishing
- Maldistribution of the Digital Content and Unauthorized Use

1.1 Cybercrime Threats:

Any criminal action that involves a computer, network or networked device is called Cybercrime. Cyber crime alternatively referred to as **electronic crime**, **e-crime**, **Computer crime** or **hi-tech crime**. Almost cybercrimes are carried out to produce income for the cybercriminals, some cybercrimes are passed to devices directly to disable or damage them. Financial is a primary cause of cybercrime. There different types of cybercrimes are as follows.

- **Cyber extortion**: An attack that involve together with an insists for money to end the attack.
- **Crypto jacking:** Attacks may engage with the victim's system by loading crypto currency mining software.
- **Identity theft:** An attack that occurs when an individual accesses a computer to collect a user's personal information, like identifications or accessing their accounts, such as credit cards and banking. as well as other types of account, like

webmail video streaming services, audio and video streaming, Personal health and more.

- **Credit Card Fraud:** When hackers penetrate retailers' systems to get the banking information or/and credit card of their users.
- **Cyberespionage:** An attack on gaining access to confidential data held by an organization or government offices other systems or networks.
- **Software piracy:** Copying unlawfully, use and distribution of software programs with the intention of commercial or personal use. Copyright infringements and violations of Trademark, and violations of patent are often involved with this type of cybercrime.

1.2 Cyber Space Threats:

Has the wireless internet increased and the different computations, services are also increased at the same time the cyber criminals also increased with new ways of cyber crimes to attack the users information. One of the reason for increasing the cyber criminal and crime rate due to failing of local and worldwide constitution. "The traversable virtual space and dynamic area established for console is called cyber Space".

1.3 Phishing:

Attack that challenges to whip your identity, or your money, by knowing information you to disclose individual data-such as numbers, bank information, credit card or passwords on websites that make believe to be rightful. There are various types of phishing. They are Spear Phishing, Vishing, Email Phishing, HTTPS Phishing, Online-Fraud, Pop-up Ads, Evil Twin Phishing, Water Holing, Whaling, Clone Phishing.

1.4 Maldistribution of the Digital Content and Unauthorized Use:

In current day image ownership verification has drawn a sharp attention due to usual availability of the internet and low-priced digital recording and storage devices has produced surroundings where duplication, unlawful use, and maldistribution of the digital content has become easier that leads cyber crime.

- **Wireless Network Attacks by Hackers**

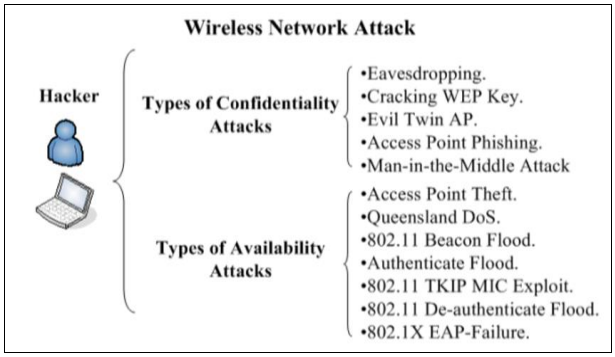

Fig 1: Wireless network attacks by hackers

Consider the worldwide internet usage of internet 2022 based on population.

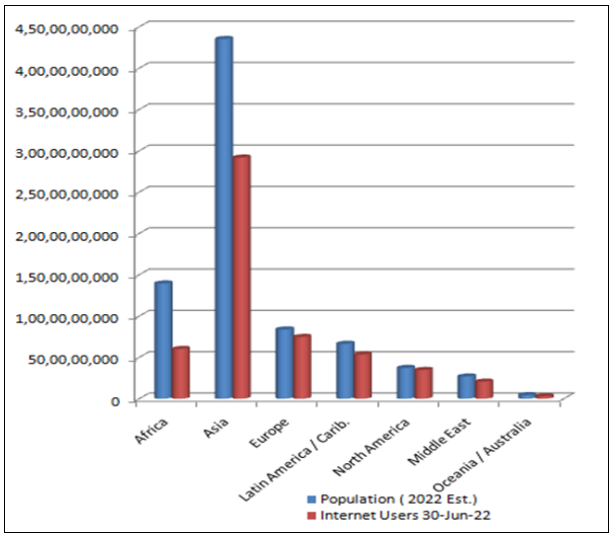

Fig 2: World Internet Usage and Population Statistics

The number of internet users are increasing day to day. At the same time the Cyber crime density in also increasing given below statics presents top 10 countries of cybercrime density in period of 2021 vs 2020.

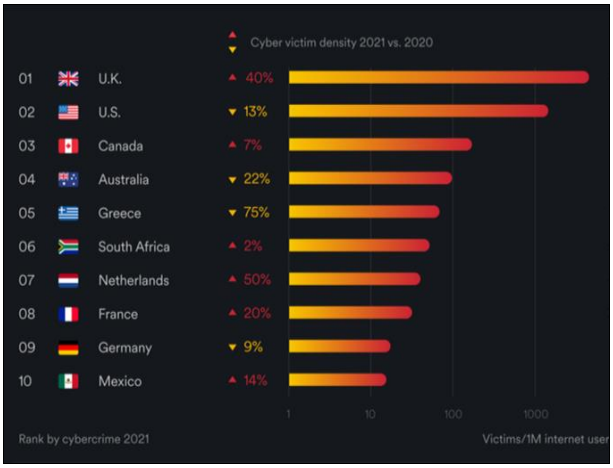

Fig 3: Cybercrime density in period of 2021 vs 2020

Main General Attacks of Cyber Crime are:

The main general attacks of Cyber crime. They are follows:

- Malicious software attack
- Phishing
- MitM Attacks
- DOS Attack
- SQL Injections
- n-day Exploit
- IoT Attacks
- Password cracking Attack
- XSS

Recent Cyber Attacks

2022-On May 8th, 2022 the national emergency was declared due to a continuing attacks of Conti ransomware against several Costa Rican government entities.

2021-Kaseya experiences a ransomware attack concession up to 1500 companies with a overwhelming ransom note of $70 million.
2021-Cyber crime of ZeroX is asking a compensation of $50 million for Saudi Aramco which faced a data breach revealing important information of employees and technological specifications of the associations.
2021-Accellion FTA data breach impacted over 100 industries, associations, institution of higher educations, and supervision agencies approximately the globe.
2020-On February 26th Spartanburg County School District was the victim of a ransomware attack.

Many attacks are done by the cyber criminals on different categories with different attacks.

Threats	Likely to Affect	Need to Understand Better
Virus	64%	41%
Spyware	62%	42%
Phishing	52%	32%
Firmware Hacking	34%	29%
IP Spoofing	32%	29%
Ransomware	31%	30%
Attacks on Virtualization	30%	30%
Social Engineering	26%	26%
Hardware-Based Attacks	26%	25%
DDoS	24%	22%
IoT-Based Attacks	23%	22%
Botnets	22%	23%
Rootkits	21%	21%
Man in the Middle Attacks	20%	23%
SQL Injection	18%	20%

Fig 4: Cyber threats need to be understand

Now how should protect the information of different organization and internet users from cyber attacks ?
To protect the information of different organization and internet users, hardware, software which are connected to internet through Cyber Security.

2. Cyber Security

Cyber security is defined as the practice of protecting computers, mobile devices, servers, networks, electronic systems, and information from wicked attacks. It's also well-known as electronic security of information or information technology security.

Types of Cyber Security:

Cyber security can be classified into few dissimilar types:

- Critical infrastructure security
- Network security
- Application security
- IoT security
- Cloud security
- Operational protection
- Awareness Program for End users
- Rectifying affect and Improving Business

In the year 2006 According to survey conducted in on cyber fraud and computer crime, The continent like Africa placed in the 3rd top position and Nigeria was the one of internet defrauding country in Africa continent.
Some of the methods are proposed to protect the internet users and information from cyber attacks.

2.1 Standard Operation Procedure to Forensic Performance Evaluate for Wireless Network

A. Cyber Criminal Behavior in Wireless Network

There are no conditions like time and place to use the wireless network it will permit to access internet. It is easy to open the gate too hackers, as a result the hacker has additional chance for attacks and interferences.
Attackers key behaviors are:

1. The cyber criminals Cracks the Wireless Internet networks for attacks and access the network.
2. Cyber Criminals attacks another network workstation by means of the similar base station of wireless network.
3. Stealing private information and the account passwords. The hackers attack the wireless networks and intercepts network packets, records the data of the discussions.
4. Phishing attacks are carried by the wireless base stations.

B. For Wireless Cybercrime Investigation

First, three stages are divided investigation of wireless network crime connected through the information discovery as well as devices which are utilized, as shown in Figure
Stage 1: examining as well as evaluating of cyber crime in wireless networks.
Stage 2: Be aware of the criminal source and behavior.
Stage 3: Arresting the person behind crime.

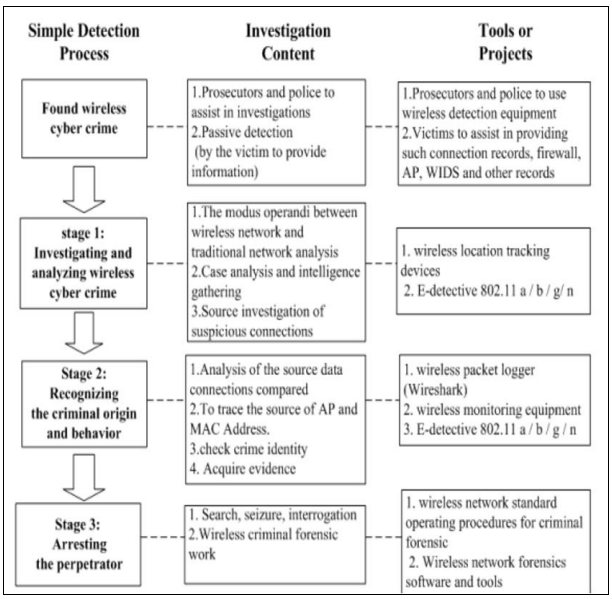

Fig 5: Wireless cybercrime investigation Flow chart

C. For Wireless Network Cyber Crimes the Typical Working Measures of Digital Forensics

By Professor Lin Yilong projected the DFSOP (Digital Forensics Standard Operating Procedures for wireless crime) for wireless network crime. Within this the examination of misdeeds connected to wireless networks, exhibited in Fig 6. It would be exact reference for examination of misdeeds associated to wireless internet.

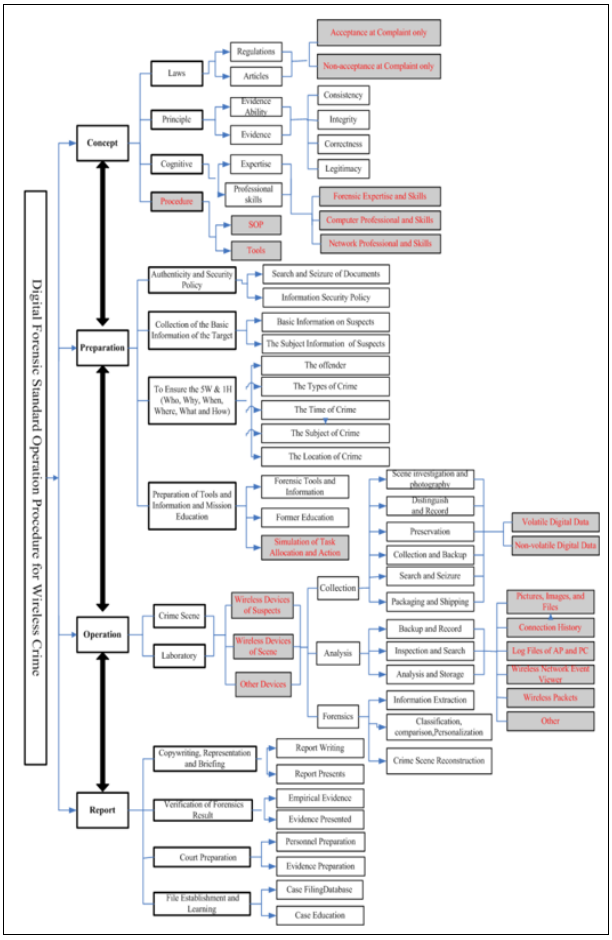

Fig 6: For Wireless Network Cyber Crimes the typical working measures of Digital Forensics

And also, to deal with electronic crime problems efficiently, behavior as well as psychology of criminals have to be investigated. Simulation model is a systemic model that affords decision makers with a absolute visualization for electronic-crime behavior as well as psychology. Hence, decision makers and possibly law-making committees can observe the simulation results and take appropriate action.

2.2 Cyber Space Crime

The forceful raise of cyber space attack is rigorous on international as well as local constitutions, and the inventive thoughts of criminals have with regard to innovative kinds of cyber attacks and latest ways to entrust these attacks.

A. Threats and Trends for Primary Cyber Space

The primary threats and trends to cyber space identified about specific to Africa. Alike threats and trends could be observable in other countries transversely the world, these observable fact are appropriate in the current African cyber space surroundings.

1. Bandwidth ease of use
2. Lack of IT education
3. Deficiency of African languages
4. Lack of consistent procedures
5. Operating system distribution

B. Threats and Trends for Secondary Cyber Space

These attacks are like: Viruses, botnets, Trojans, Junk Email, and SQLI, among others.

With this increasing amount of cyber crimes, it is very important to take exact contradict actions to deal with attacks of cyber space.

Some of the recognized contradict actions include

- Exact cyber space proposals,
- CSIRT-(Computer Security Incident Response Teams)
- Cyber security consciousness campaigns.

2.3 Attack Model of Phishing

The phishing attack model is simple and can attack from anyplace in the earth using Internet connection a number of the steps is able to be performed.

In step 1: The online banking attack engages the aiming of the particular person.

Throws a email of phishing purpose or Trojan lure email to thousands millions of potential victims by the cyber criminal.

Those who getting a email actually react by authenticating their account information in the fake websites of banking highest percentage.

A small minority goes behind the link in a Trojan tempt email and have their PC cooperated and a key logging Trojan is loaded.

In Step 2: After login into their account using their credentials immediately their Online Banking credentials are captured by fraud.

In Step 3: The fraud will perform actions and takes the money of the client from the account.

In Step 4: The fraud need to bring in their present bank account details and sends the information or amount to their account.

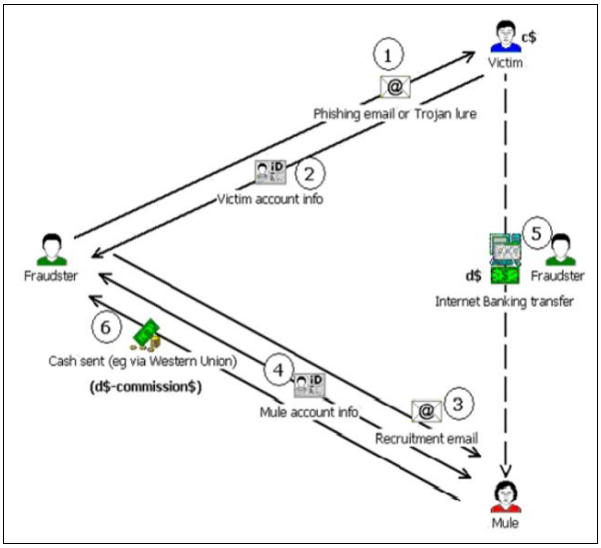

Fig 7: Fraud attack structure of an Online Banking

To protect from phishing attacks there some strategy mentioned below.

1. To focus law enforcement efforts on money transfer agents such as Western Union.
2. Governments should convey force to allow on the governments of Eastern Europe to ensure there is no "legal vacuum" or safe place of protection in which cyber criminals can function.
3. Phishing infrastructure should developed in by the IT Security community then there is good scope to get better recognize Online money mule accounts and growth of monitor assaults.

4. The bank sector has to mainly concentrate on enlightening potential Online Mules Money to avoid them being cheat.

2.4 Maldistribution of the Digital Content and Unauthorized Use

Accessibility of the internet and inexpensive storage peripherals and digital recording has created a situation where duplication, maldistribution of the digital content, and unauthorized use has become easier that show the way to cyber crime.

To prevent this type of cyber crimes already proposed for inserting a color watermark inside a color host image by different fragile color image watermarking frameworks.

Watermarking framework, it permit a users through an suitable a hash function and secret key to check the reliability, authencity as well as owner rights of an picture.

Suppose a faker executes the watermark extraction through a wrong key as input and unsuitable hash function, the client gets an image that looks like noise.

For this type method we are supply that an integrated solution for ownership authentication in someplace of the watermark is exclusive for particular one of host picture, as a result the confirmation is providing in a well-organized way.

On the extracting of watermark closing stages, we have utilized method like blind extraction, i.e., host picture or the watermark picture is necessary at the time of watermark extraction.

Some of the solutions are provided for the cyber crime attacks or electronic-crime and unauthorized use of information.

3. Precautions

Some of the following precautions are taken to control the cyber attacks to prevent.

Suspicious Emails and URLs: Should awareness to the employees about the URL's and emails which are coming from spoofed address.

Password Setting: Should make awareness of keeping of password with use of different characters and same password should not use for long time which not a good idea.

Identifiable Personally Information: Most of the people uses the other devices for browsing their personal information sometimes and shares their information in social media which leads to attacks. So, we should raise the awareness for employees.

Updates and Backups: it is the biggest challenge of IT industries about the securing of their data. So, they have to keep backup of their data daily and systems should be updated daily.

Securing the Devices Physically: Creating awareness of employees and family members to keep their devices lock properly when they are leaving out from their work or handovering their devices to someone for purposively.

Summary

Table 1: Various Cyber Attacks and their remedies

S. No.	Name of Attack	Measure
1.	Cyber Crime Attack	• Creating awareness in people • Establishing the high protection measures like anti-virus. • Keeping Backup of data daily. • Maintaining hardware.
2	Phishing Attack	• Employee should aware of junk emails sent by frauder.
3	Maldistribution of the Digital Content and Unauthorized Use	• Watermarking framework • Blind extraction method
4	E-crime	• Simulation model is a systemic model

4. Conclusion

The usage of internet technology changed the world made the working easier at the same time problems are also arised like Cyber-attacks/e-crimes or Phishing etc which affects the life of people and business. To secure information of users and business from cyber criminals some the methods are already proposed, the challenges and solution to those are discussed. Some of the precautions also mention in this paper which will leads to decreases the cyber attacks chances.

5. References

1. I-Long Lin. A Study on Digital Forensics Standard Operation Procedure for Wireless Cybercrime.
2. Stephen McCombi. Winning the Phishing War: A Strategy for Australia.
3. Marthie Grobler. Broadband broadens scope for cyber crime in Africa.
4. Deng-Yiv Chiu Information Management Dept Attacking and defending perspective of e-Crime behavior and psychology: A systemic dynamic simulation approach.
5. Prof Alai Chaudhuri. A New Invisible Color Image Watermarking Framework through Alpha Channel.
6. Mortaza Bargh S. Exploring a Warrior Paradigm to Design out Cybercrime.
7. Newman GR. Cybercrime, In M. D. Krohn, A. J. Lizotte, and G. Penly Hall, editors, Handbook on Crime and Deviance, Springer, 2009, 551-584.
8. Homepage of TNO (Netherlands Organization for Applied Scientific Research) at http://www.tno.nl/