

Challenges in Cyber Crime and Security

Shaveta Bhatia, Harshit Popli, Mitali Jain



Abstract- Definition: - Computer crime is an offence or an attack done by the third party or the individual or group of people. It may be done in terms of many possible reasons like to steal some crucial information or data or money and all that possible things that may affect the victim mentally, financially or physically. **Resources:** - Internet, phone, hardware devices. **Effects:** - The coders may pollute some sort of codes which termed as viruses in the computers of the country men and may affect the security of the people at a very nominal grade but this is not all, it may also affects the norms and the rules of the organizational companies and may steal their crucial information. These types of people are termed as HACKER in the context of Cyber Security They also have an adverse effect on the economy of the country as the country may not have the proper rules and the cyber experts for securing of data and in that type of country no businessman may invest . **Securing yourself:** - Actually the computer polluters are the well-known people who have good enough knowledge of their work but we can still get out the attack held on us by using some precaution and using the proper paid and genuine antivirus as an survey has declared that in 58% of pc's people have viruses due to their unpaid and local antivirus.

I. INTRODUCTION

Computer crime and security are the two different roads having a same crossway as cyber-crime may be defined as the intelligent way of stealing , using , deleting and doing all sort of alteration without the proper admin permission whereas security is termed as an extra and over then normal way of getting rid of the illegal and unsecure cyber-attacks . In the actual way the hackers gets the idea for stealing the data from our daily life routine and they just apply it on the required need .By taking an instance for getting water from a rubber pipe which has only one way out and now if we think like a hacker we can hole that pipe from where we want the water and then we have different outlet for getting water which can be easily accessed but if we replace it with the steel or some other metal pipe then it would not be easy for any person to hole it(for that he need some special and dedicated tools) like this we did a work of an antivirus or cyber expert (to protect our data) .

II. WHY PEOPLE ARE READY TO BECOME HACKERS: -

Today if we see world and compare it with few years back we can easily measure the dramatically changed environment,

but from where and why this drastic changes comes? If we talk about the world that why these illegal elements and brains are so in demand by the profit organizations as well as nonprofit organizations then it would counter few of the elements: 1_Knowing [6] serious talks
2_Snatching without [7]ineloquence
3_wanting new thoughts and ideas
4_coming on top

If we consider the above written points and have a dense and a seivour talk then we could find he reality behind the hackers and why they are so in demand.

III. ADVANTAGES AND DISADVANTAGES: -

The major advantage behind the thoughts of an hacker are that they just want to steal and have some sort of secret and crucial information's for a particular or any organization which may have that [8]credentials that anyone can pay for that material which is being hacked or stolen by the hackers. Hacker may also be defined as a group or individual or an automated machine or any device which works for stealing the data without having accurate authority for the same. Some hackers are being employed and governed by the ministerial organization for the fulfilment of their necessary needs but except that all are the illegal and are unauthorized if perceive or found doing hacking/stealing/accessing unauthorized material or anything which termed as illegal .

(A)Diagrammatical representation of cybercrime: -

Revised Manuscript Received on May 30, 2020.

* Correspondence Author

Dr. Shaveta Bhatia*, Associate Professor Faculty of Computer Applications, Manav Rachna International Institute of Research and Studies, Faridabad,India.

Harshit Popli, (Student) Faculty of Computer Applications, Manav Rachna International Institute of Research and Studies, Faridabad ,India.

Mitali Jain, (Student) Faculty of Computer Applications, Manav Rachna International Institute of Research and Studies, Faridabad,India.

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an [open access](https://creativecommons.org/licenses/by-nc-nd/4.0/) article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>)

Challenges in Cyber Crime and Security

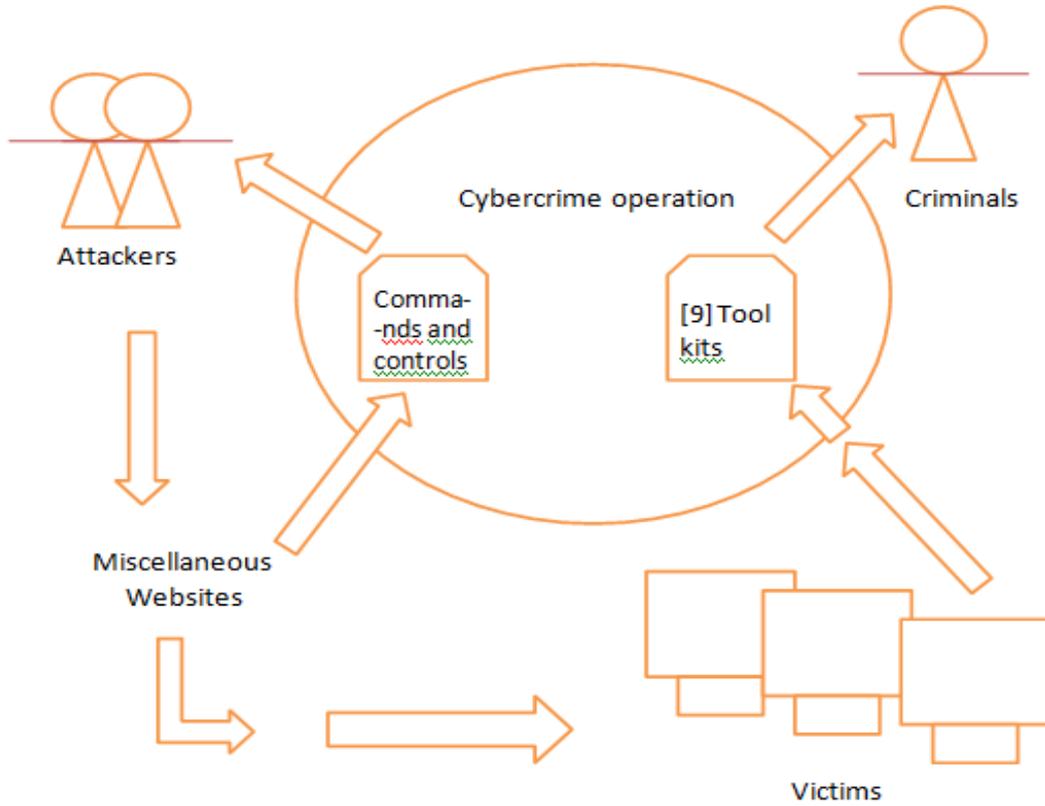


Fig.1 Demonstration of cyber attack

The above diagram simply explains that how the hackers does their work and how the simple and innocent people got indulge in their illegal and unethical works and may also get looted in many cases.

(B) Diagram to show the precautions from hacking / Security

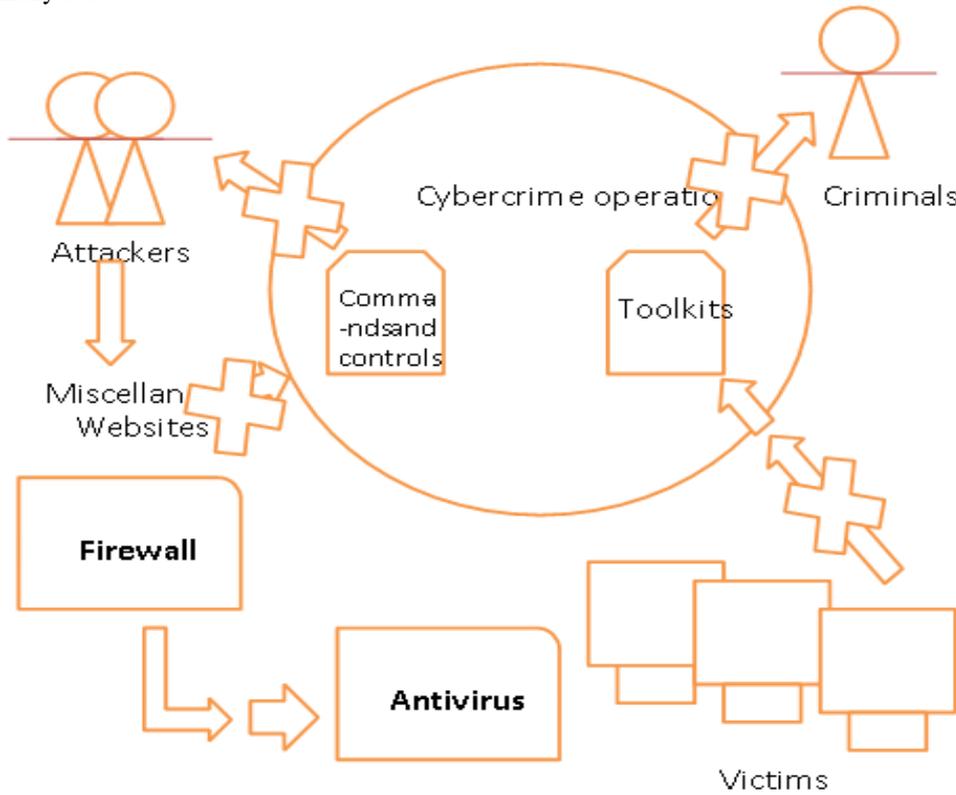


Fig. 2 Demonstration to secure from cyber attack

IV. TERMS NEED TO KNOW: -

Viruses: - The term virus may be defined as the piece of code or an infectious agent or any miscellaneous software which may affect the working.

Antivirus: - This is an anti-version of virus which may be explained as the piece of codes which are solely made and developed by the engineers for protecting the credentiality of the resources. System with all types of injurious and infected materials. It turns it on as the wall full of fire and protects the machine from any conscious mechanism.

Firewall: - This is another term which was developed by [10] Nir Zuk firstly with collaboration the other engineers which protect the

Trojan: -It is a malicious program which works by misleading the users for their pure intentions.

Key stroke login:- It is a smart infected or malicious software piece that works to copy or remember the keystrokes which user pushed while typing.

Back Door:-It is a term which is quite famous in the world of hackers as it may be defined as his entry without knowing any one.

Bot: -It is artificial and virtual human or a man built from codes who do simple actions but at higher rate.

DOS:-It stands for denial of services which means it make the services out of use for some couple of minutes.

Logic Bomb: - It is like a normal bomb but create destruction in the computer memory .The virus is speeded into the computer and this bomb triages itself if the conditions meet

Black hat: - These are the type of hackers who are involved in illegal hacking.

Botnet: -These are the computers or group of system who are controlled without their owners knowledge and used to send spam mails and messages.

Cracking: - This is a term used to define the cracking of those systems who have security enabled.

Doxing: - Doxing is defined as identifying and discovering the identities of other anonymous internet uses.

(C)Statistics in terms of Cyber-attacks held in last few years:

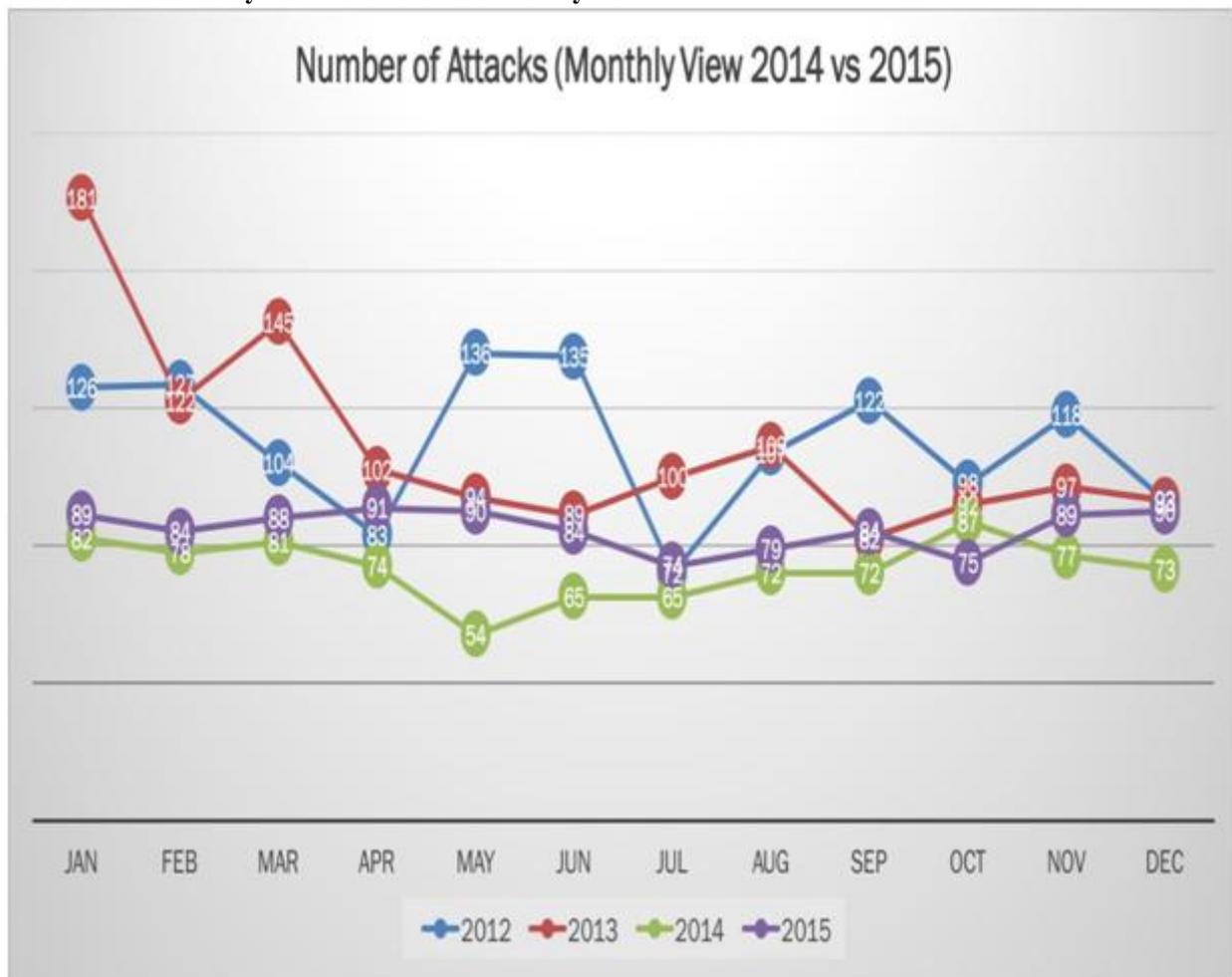


Fig.3 Numeric calculation of cyber-attacks [1]

According to the data cyber-attacks held in mentioned year was great and huge in the month of January of 2013 and found much depreciated and reduced in 2014 but if we look

(D)The attacks held in last year:-

towards the year 2012-13 we can easily calculate the alarming increment whereas in the month of May 2014 we can see how much threats and attacks are reduced.

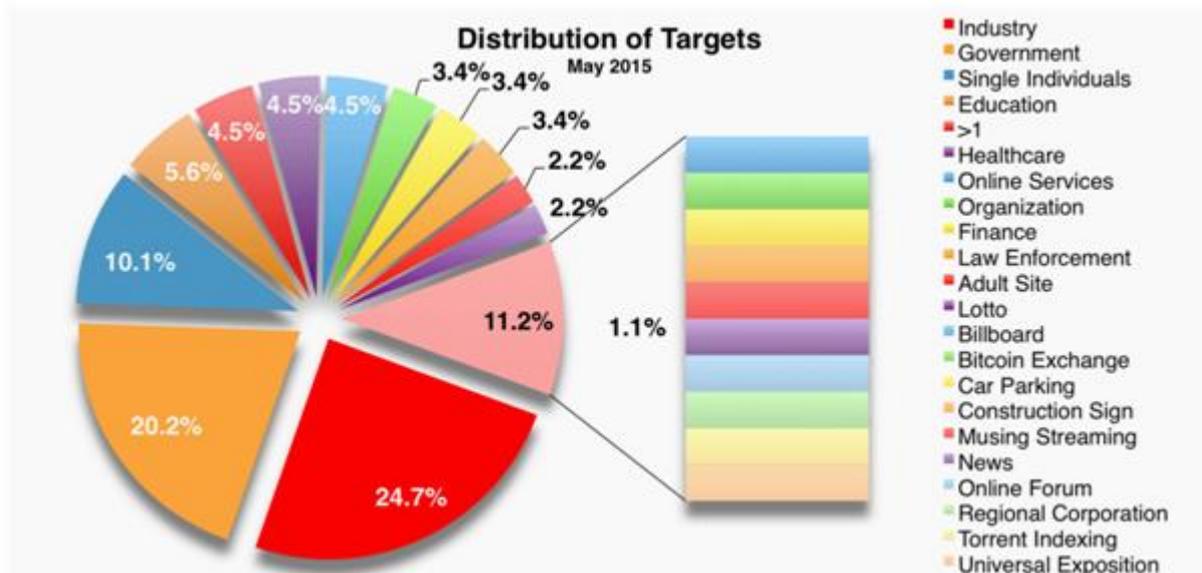


Fig. 4 Pie chart to show risk in different sector [2]

These are the small representation of the attacks which may be held in different sectors if the nation. we have different or verities of areas which help in developing the nation but with this fear they also sometimes tries to migrate from one Nation r country to another.

We all need to see the highly and intense requirement of the devices and the equipment’s which may help the nation and the industries to make them secure in the factor of cyber-crime and security.

(E)The graphical status of attacks in the same year and month:-

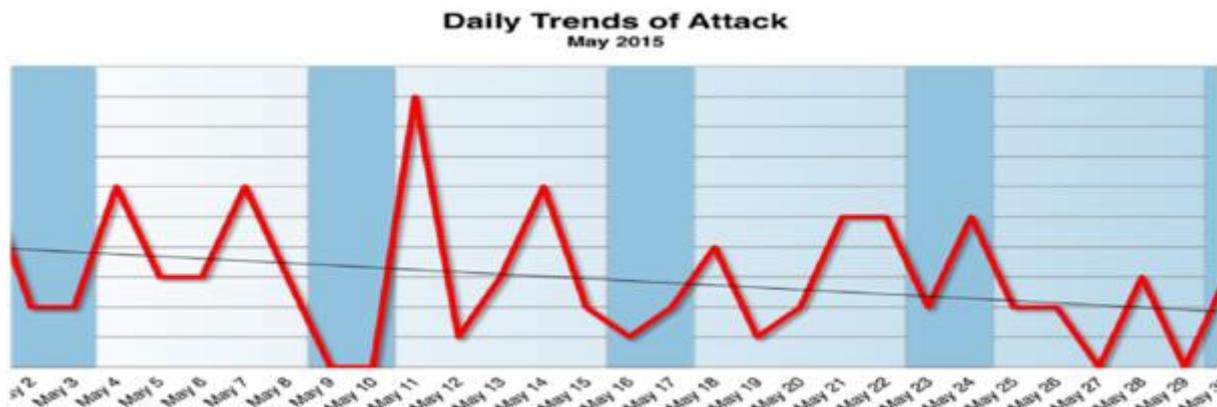


Fig.5 Month wise calculation of cyber-attacks [3]

This is a graphical representation showing how dangerous is to keep our data under or in computer resources like different apps andgadgets, as here we can see easily and normally the intention of attacks held in the month of May 2015 . The daily a dramatic changes in the attacks.

V. HOW TO SAVE OUR SELF

1. It is not a great challenge to save our data or resources and other private material in personal or an individual form but yes it is great challenge for those who owes an INDUSTRY or have a FIRM but not having the proper knowledge of protecting the resources.
2. In terms of securing the resources the best way of doing is to use personal owned and developed or personal paid and on demand developed antivirus to get rid of any type of theft and crime.
3. We can also make our crucial data in complete security with the help of personal cryptographer

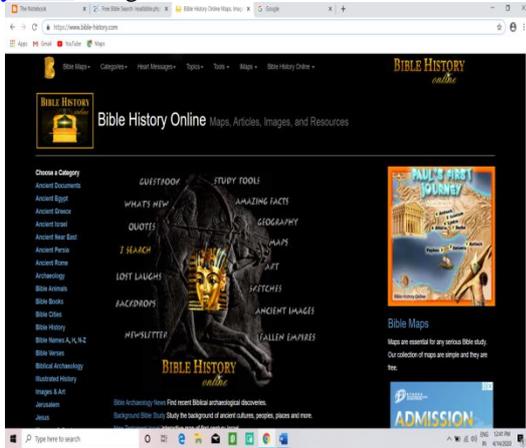
- and encoder so that the company or organizational data may get full and fledge security at priority
4. Companies are also needed to order and try to develop such types of devices which may control or check the security level of the organization or the firm in terms of data theft and security.
5. There is also need to know that the organization in some unexplainable cases they use some third party or unpaid or pirated or copied software’s and protecting kits which afterward captures a lot of funds .
6. Using anti malware and anti-Trojans and other sort of crucial software are needed at the first as without those the data of any company may got stolen quite Instantly.

VI. RESULTS:

Hacking using SQL Injection

Step 1: Find a Vulnerable website through Google Dork.

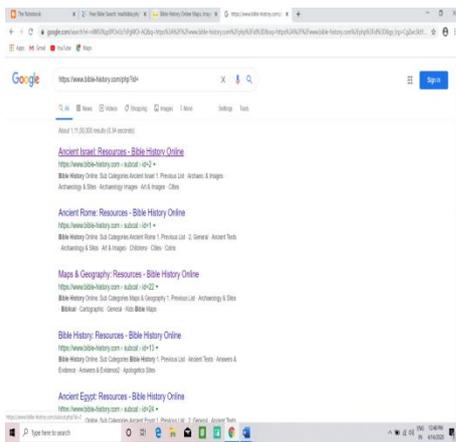
Step 2: This steps tells whether the website is SQL based or not. Here the testing is done on <https://www.bible-history.com/> using local host.



Step 2

Open new tab and type this line in google search box <https://www.bible-history.com/php?id=>

This command will illustrate how many pages are there in website. In case of the defined example, number of pages are 2.



Step 3:

To find number of columns we will use "ORDER BY" statement. Now remove the single quote and add order by n /*where n = 1, 1++*/so you keep incrementing the number(n) till you get an error

```
NO ERROR
http://www.bible-history.com/subcat.php?id=2
order by
ERROR : Query failed : Unknown column '2' in
'order clause'
```

This mean the number of column in this site is 1, different sites have different number of columns, ie yours maybe 10 or 11 or even 100 as the case may be. The above example shows hoe security is effected.

VII. CONCLUSION

Cyber-crime is an offence which is done by third party to effect the victim mentally, physically. The third party which effect the victim is the person who has a vast knowledge of computer and network he can be known as Hacker. Hacker can effect victims through miscellaneous websites or threats. The main aim of hacker is to steal personal and crucial information which can help them to harm the victim. The statistic shows that cyber-attacks were increased in the passing years, but as the companies get into the knowledge of threats the companies had started taking precaution which had reduced the attacks in the year upcoming. There are some ways to protect yourself from hacker is by: By developing personalized antiviruses. Encrypt the data so that company data get full fledge security from theft or crime. The companies should use devices which help them to control security level.

REFERENCES

1. Hackmageddon.com "Cyber Attacks" available at <http://www.hackmageddon.com/2015/05/19/1-15-may-2015cyber-attacks-timeline/> retrieved 03 oct 216
2. Wikipedia "UK Cyber security community" available at https://en.wikipedia.org/wiki/UK_cyber_security_community retrieved 10 oct 2016
3. **Abbreviations:-**
Serious talks:- The Important and the concerned talks and discussions held in any company or organization **[7]lineeloquence:-** Good in something or great power **[8]credentials:-** The rights and permissions with or given to someone .
4. **Toolkit:-** It is some set of special and top secret software's and codes which help the coder or programmer In their work.
5. **Nir Zuk:-**He is a man who firstly invented and got the section)
6. Idea of firewall (to know firewall refer **terms need to know**

AUTHORS PROFILE:



Dr. Shaveta Bhatia Head of Department, Computer Applications

Dr. Shaveta Bhatia has been awarded her Ph.D degree in Computer Applications. She has completed her Master in Computer Applications (MCA) from Kurukshetra University. She is having 17 years of academic and research experience. She is a member of various professional bodies like ACM, IAENG and CSI. She has participated in various National and International Conferences and actively involved in various projects. There are more than 40 publications to her credit in reputed National and International Journals and Conferences. She is also member of Editorial board of various highly index journals. Her specialized domains include Mobile Computing, Web Applications, Data Mining and Software Engineering and guiding research scholars in these areas.



Harshit Popli, Students of MCA(L)

Manav Rachna International Institute of Research and Studies



Mitali Jain, Students of MCA(L)

Manav Rachna International Institute of Research and Studies

