

# Era of Cyber Security

Khalid Arshad Parkar<sup>1</sup> Sejali Butala<sup>2</sup>

<sup>1,2</sup>Department of Computer Science Engineering

<sup>1,2</sup>ICS College KHED, India

**Abstract**— Cyber security is an important part of information and communication technology. Securing private information and privacy of a user is becoming challenging day by day. Cyber-crime is increasing day by day. Many big companies and public sectors are taking many measures to protect private information and preventing the cyber-crime. This paper focus on various cyber-crime and its prevention. It also focus on difficulty face by public sector and private companies.

**Keywords:** Common Cyber-attack, prevention of Cyber-attack, Cyber-attack on big companies

## I. INTRODUCTION

In today’s world a user is able to send and receive data in the form of audio, video, pdf, etc just by the click of a button but did a user think how securely the data is transferred or not? Today internet is the fastest growing infrastructure in the world. Due to increase in the technology the Cybercrimes increases because of the loop hole I the system or the server. The cybercrime is done by a hacker to steal the critical information of a company or to steal a private information. Today 60% of the transaction are done online and it’s increasing.

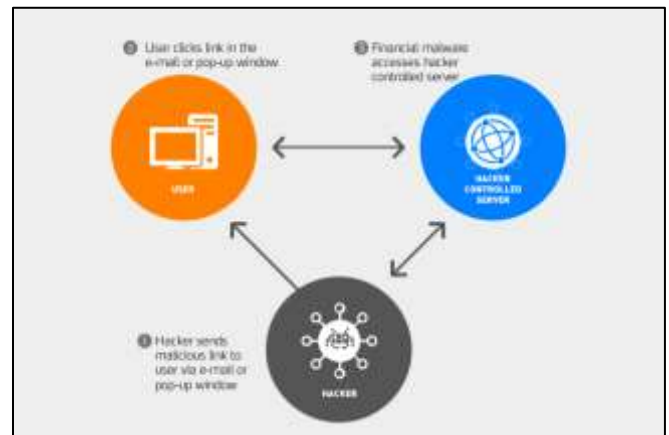
Many it sectors like banking, cloud, mobile internet need a tough cyber security to protect the private information. A server or a company hold very important information of a private sector or an information on a person of the security must be strong. Every nation enhancing their cyber security to protect the critical information and making the internet safer place. Every nation started to develop their new services and policy to protect internet user from cyber scam.

A discount offer link (fraud e-mail) is a common technique used by a hacker to wipe out money from the user account. The cyber-attack can be prevented by cyber security. Cyber security helps securing the private data, information. Computer systems from unauthorized digital access. There are multiple ways to enable cyber security. Cyber-attack are done depending the kind of network user connected to and cyber-attack user prone to.

## II. COMMON CYBER ATTACK

### A. Malware Attack

This attack are done through downloading any suspicious attachment online by certain malicious viruses amended with the attachment

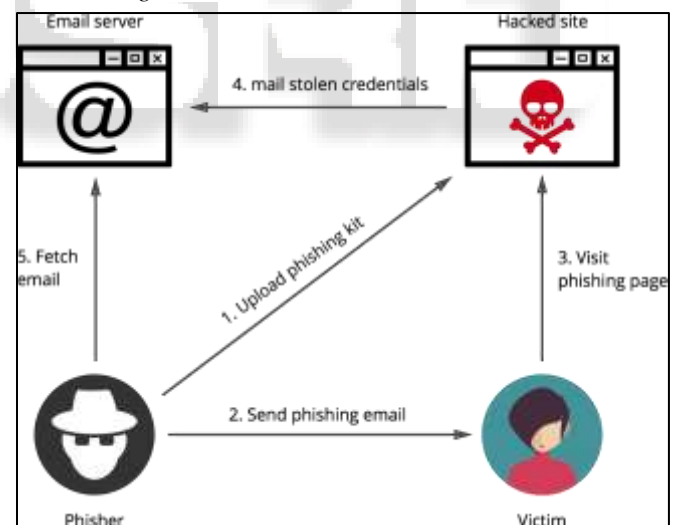


For example: Trojan, adware, remote access, spyware, rootkit, virus worm, keylogger.

### B. Phishing Attack

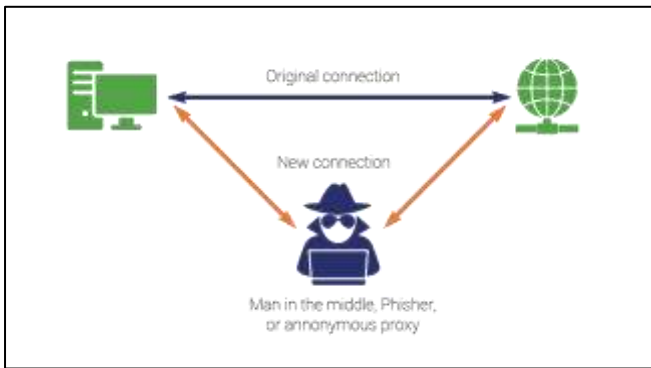
Phishing attack is done by the hacker, that usually send the fraud email, links which come from a legitimate source (e.g.: discount offer). This is done to install malware or to steal the sensitive data like credit, debit card information, login id, password info and personal info.

### C. Phishing Attack



### D. Man in the Middle Attack

In man in the middle attack the hacker get the access to the user computer by gaining access to the information path between user device and the website server. The hacker computer takes over IP address of the user computer by doing through communication line between user computer and the website is secretly intercepted. (This happens with unsecured Wi-Fi networks and also through malware)



Having a strong Wi-Fi mechanism in the user pc can prevent the man in the middle attack. The sudden slow internet connection can be a sign if man in the middle attack.

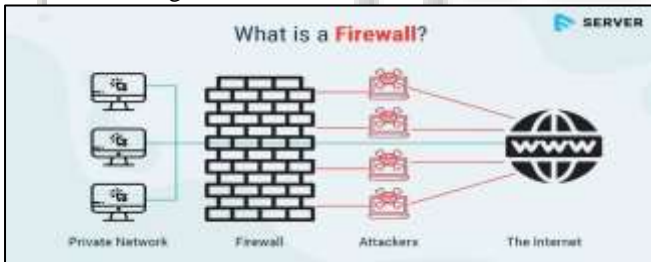
### E. Password Attack

This is one of the easiest way to hack the system. Here the user password could have been cracked by the common password [(1,2,3,4) (a,b,c,d) (0,0,0,0)]. The first common type is dictionary attack, most people use real words as a password, through the deaconry attack the hacker crack a common or real word. Guess and the offline cracking are also common in the password attack. Brutal force attack the most common and the easiest way to crack a password. The most common used password in 2020 is 1,1,1,1 and 0000. To secure the data from password cracking a user must have a better password.

## III. PREVENTION OF CYBER ATTACK

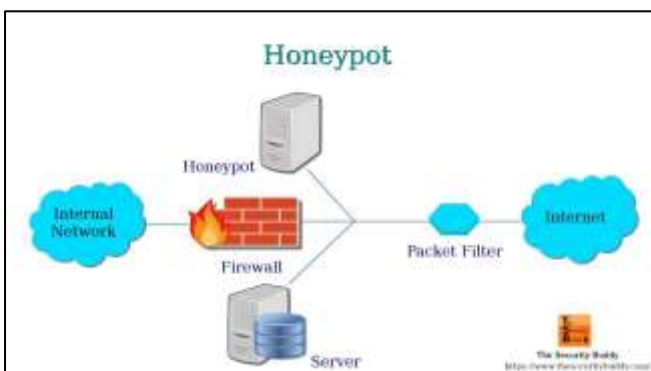
### A. Install a Firewall

It is a virtual wall between user computer and the internet. The firewall filters the incoming and the outgoing traffic from the user to safe guard the network connection.



The firewall is based on the security policies of the user. Firewall is the important to protect data from cyber-attacks.

### B. Honey Pots (Virtual Trap)



Just like the honey in the flower attracts the bees, the dummy computer system called honey pot are used to attract the attackers.

Due to honey pots the system looks vulnerable to deceive the attackers and this turns in the deface of the user real system and data.

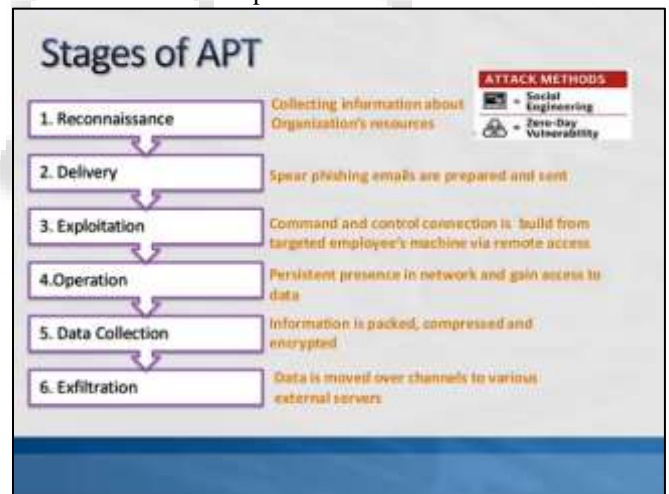
In the addition of the honey pots and the firewall the user must use unique password, antivirus software and avoid fake mails form unknown source.

## IV. CYBER-ATTACK ON BIG COMPANIES

- Cyber attacker not just attack individual but also attack public sector (gov.) and private organization.
- Cyber-attack done in the public and private organization are more dangerous.
- This attack are done to tampering crucial data to gain profit or to sell crucial information on the dark web.
- The attackers stole the information of the private and public sector and upload the data to dark web, this is done by the opposition company to destroy the sectors.
- The attackers stole the business finance details, sensitive personal data, customer database, clint list, IT infrastructure

## V. ADVANCE PERSISTENT THREAT (APT)

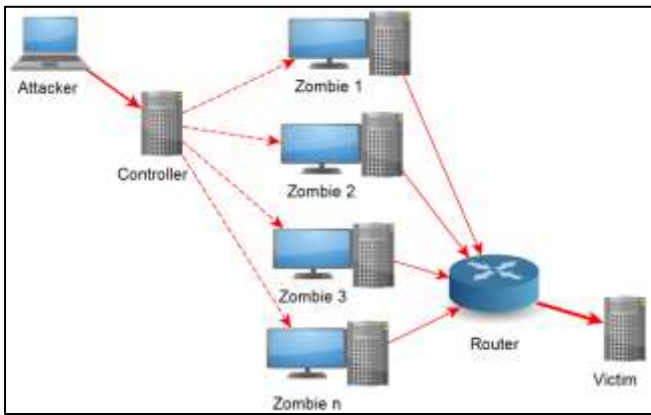
Big companies and public sectir organization face the advacw threate called advance persistent threat.



In these attack hackers gained access to network for prolonged period, in order to gain confidential information.

### A. Denial Service Attack

Hacker use multiple system to flood the network of the server which cause the leave of legitamtee service request It is also called as distributed denial of service

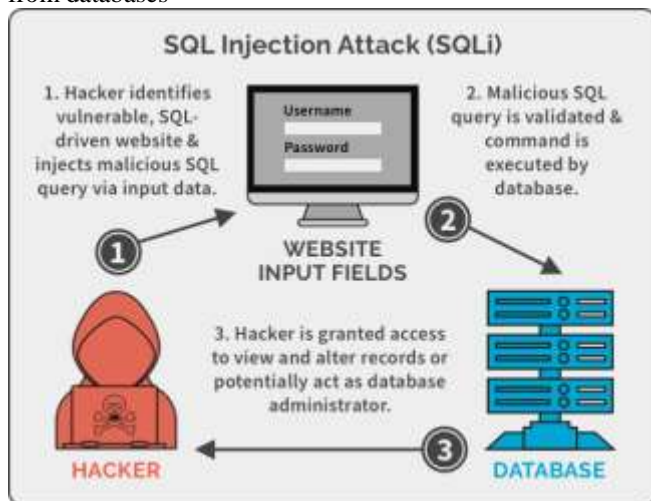


[3] [https://blog.netwrix.com/wp-content/uploads/2018/05/CA2\\_session\\_hijacking\\_2.png](https://blog.netwrix.com/wp-content/uploads/2018/05/CA2_session_hijacking_2.png)  
 [4] [https://elie.net/static/images/images/how-phishing-works/phishing\\_cycle.png](https://elie.net/static/images/images/how-phishing-works/phishing_cycle.png)  
 [5] <https://www.thesslstore.com/blog/wp-content/uploads/2018/11/man-in-the-middle-attack.png>

### B. SQL Injection Attack

A hacker manipulate a standard SQL query in database driven website

By this attack hacker can view, edit and delete tables from databases



### VI. CONCLUSION

- With the increase of the global digital data it is anticipated that cyber attackers will quadruple in the near future.
- Government agencies and big companies are the most of the target of the hackers.
- India Is the highest in the cyber-attack with the 80% of the share of respondent.
- To prevent the cyber-attack their India should present new internet policy.
- Companies should hire nest cyber security expert to prevent cyber-attacks.
- A big organization and public sector need a professional cyber security expert to prevent this type of attack.

### REFERENCES

[1] <https://www.researchgate.net/profile/Obinna-Igbe-2/publication/319901682/figure/fig1/AS:614307704352795@1523473778432/Elements-that-constitute-a-distributed-denial-of-service-attack.png>  
 [2] <https://heimdalsecurity.com/blog/wp-content/uploads/2014/07/typical-financial-attack.png>