cyber security -

syber security is the protection of internet connecting syst including software & hardware & data from cyber attack.

Data

It is made up of two words, one is syber & other is security.

- Syber is related to the technology which contain system, network & programs or data where as security related to the protectⁿ which include system security network security & applicatⁿ & infor security
- It is the body of technology process & practices design to protect network devices programs & data from attack, then thief damage modification or unotharise ogcess
- It may also be refer to as information technology security
- We can also define syber security as the set of principles & practices design to protect our computing resource & online information against threat
- Due to the heavy dependancy on computer in a modern industry that store & transmit abundance & essential information about the people, syber security is a critical fuⁿ & needed insurance of many business.

Q. Why is cyber security important -

We live in a digital era which understand that our private ~~in~~ inforᵐ is more vulnerable than ever before

- We all live in a world which is Network together from internet banking to government infrastructure where, data is stored on computer & other devices

- A portion of that data can be sensitive informatⁿ Weather that fanantial data personal informatⁿ or other types of data for which unalberise dcess could have negative consequence.
- Cyber attack is now an international concern & has given many other security attacks could denger the globle echonomy
- Organization transmit sensitive data accross network & to other device in the course of doing business & cybes security describle to protect that information & the system used to process or store it
- As the volume of cyber attack grows companies & Organizatⁿ espacially those that deep informatⁿ relatod to national security help or eatl fainantial records need to take steps protect their sensitive business at personal inform.

Types of attack

1) Phishing -

It is the act of aquire privak or sensilive data like username password & credit card delails for purpose of frod activities

- Phishing is usually done by sending image to user which require user to pul or enter personal data such as credit card No or social security No
- This information is hansmitted to the hacker & utilize for frod purpose.
- Phishing typically carried out by email spoofing or instant massege or phone calls etc.
- Some criminal do phishing by sending email or creating Wabepage that are design to collect an online bankdetails

credit card or other login information
iv) because of this image & wabepage look & fill like trusted email & wabepage

Phishing Technique-
i) Phone phishing -
- In phone phishing the phisher make the call to user & ask the user to dial the No
- The purpose is to get personal information of the bank account through the phone.
ii) Instant messaging -
- It is the method in which user recieve message with a link directing him/her to Phising website
iii) Key loggers -
- Key loggers refers to the malware used to identifing input from the keyboard & this informatn is send to the hacker to hack the password or other information.
iv) Trojen Host.
- It is invisible hackers trying to login into your user account to collect informatn through the local machine
v) Phishing through search engine -
- Some phishing involve search engin where user is directed to product site. which may occur lowcost product or service.
- When the user tries to by the product by entering ers credit card details then this detail are collected by phishing Website
vi) Email Phishing -
Some phisher send email to user & unable the user

to enter it's sensitive data to make frod.

ii] Identity theft (चोरी) -

- It is the one of the most serious frod as it involve stealing money & obtaining other benifits through the use of false identity.
- It is the act of pretending to be someone else by using someone else identity i.e. haa order items online under false name & pay using someone else credit card informat^{n} or by the debiting another person account-filligal migradion, terirism & blackmail are obtain may possible by means of identity theft

* 3) Credit card frod / Theft -

- Credit card or debit card ford is a frod is from a identity theft that involves an unathorised taking of another credit card information for the purpose of charging purches to the account or removing fonds from it

1) Lost and stolen Gard Frod -

- This occurs When your card is physically stole or lost & then used by criminal to make unathorised charges on your account.

2) Account takeover -

- When card holder gives personal infor mation such as Rome addess name, mother name etc. to hacker, then contact the card holders banks & report the lost card & change of address & obtain a new card as soon to be victim- name

3) Counterfeit Card-
- When a card is clone (copy) from another & then used to make purches

4) Frod Application-
- When hackers use another person name & informat" to applay for an oblain a credit card

5) Never received-
- When new or replacement card is stolen from the E-mail, never reaching it's rightfull owner.

* Hacking -
- Computer hacking is When someone modifies computer hardwere of softwere in way that alter original intent.
- People who hack computer are known as hackers.
- A hacker is a person who find weakness in computer system or network to gain access.
- hackers are usually skill computer programer with knowledge computer security for most hackers, hacking gives them the opportunity to use their problem solving skill & chance to show of there abilities
- Most of them do not ~~wh~~ wish to harm others.

Spoofing :- (धोखा)
- The Word spoof means Hoax, Thick or receive.
- In It Word spoofing refers tricks deceving computer system or computer user.
- This is typically done by, hiding once identity or fecking the identity of another user on internal

- Spoofing can take place on the internet in several diff Waves
- One common method is through email.
- Email spoofing involve sending message from email address or fecking o the Email address of another use
- Most Email server have security features that prevent anathorised user from sending message
- However, spammers obtain some spam message from their own SMTP.
- It is possible to receive Email from an address that is not an actual address of the person sending message
- Another way of spoofing take place on the internet Via IP spoofing.
- This involve masking the Ip address of certain Computer system by hiding or fecking computers Ip address
- Flood attack occur when the system receive to much traffic for the server to buffer, causing they to slowdown & eventially stop.
- It is defaull for other system to determine where the Computer is transmitting data because of IP Spoofing mask is difficult to trap of source of transmission.
- It is obtain to used in denial of service (dos) attack that overload service.server.
- This may cause the server to either crash for become on responsive to legitimate request.
- Software Security system have be develop that can identity of Dos attack & lock there transmission.

* Denial of Service [DOS] -

- A Dos attack is an attack to shutdown the machine or network making it inaccessible to it's intend users.
- The Dos attack privent legilimet user [i.e employee member or account holder] of the service or resource they accepted
- Vigteams of the Dos attack after target web server of high profile organization such as banking media, companies or Gore & tread organization or other security loss.
- They can cost the target person or victim a great deal of time & money.
- There are two general methods of Dos attack
  1) flodding service 2) crashing service.
- flodd attack occure when the system ressive to much traffic for the server to Buffer, causing they to slow down & eventially stop.
- A Dos attack can also distroy programming & files in affected Computer system.
- In some cases Dos attack have forced to websik access by millions of people to temporary stock.

* Cyber Security Goals -

The objective of cybersecurity is to protect informa from being stolen compromised to attacked. cybersecurity can be measured by at least one of three goals
1) Protect & Confidentiality of data.
2) Preserve the integrity of data.
3) Promote the availability of data for authorized users.