# Certificate course in Cyber Security :- Threates and Prevention

## HAND BOOK




**Contact Details : Department of Defence and Strategic Studies**

**Web-page :** https://avpsthalner.org/wp-content/uplode/2020/02/admission-form.pdf

**E-mail:** kgjgavit.20@rediffmail.com

**Contact: 02563-285629 Mb.no. 9421527981**

## Program Objectives

The exposure of the students to Cyber Security program at Graduate level should lead to the following: -

(a) Learn the foundations of Cyber security and threat landscape.

(b) To develop students with the technical knowledge and skills needed to protect and defend against cyber threats.

(c) To expose students to governance, regulatory, legal, economic, environmental, social and ethical contexts of cyber security.

(d) To expose students to responsible use of online social media networks.

(e) To systematically educate the necessity to understand the impact of cyber crimes and threats with solutions in a global and societal context.

(f) To select suitable ethical principles and commit to professional responsibilities and human values and contribute value and wealth for the benefit of the society.

## Program Specific Outcomes –

Upon completion of the certificate program, students will be able to:-

(a) Analyse and evaluate the cyber security risks.

(b) Analyse and evaluate existing legal framework and laws on cyber security.

(c) Analyse and evaluate the importance of personal data its privacy and security.

(d) Analyse and evaluate the security aspects of social media platforms and ethical aspects associated with use of social media.

(e) Increase awareness about cyber-attack and safety against cyber-frauds.

(f) Take measures for self-cyber-protection as well as societal cyber-protection.

## About Course

As we live in the 21st century, we know that there is no alternative without computers and social media. Smartphone and computers the internet has changed the idea of communication. Due to lack of security, various cyber-crimes have emerged in the past decade. Cybercrime is an evolving form of transnational crime. The main function of cyber security is to protect networks, computers, programs from unauthorized access and loss. Maximum number of users are not aware of the risks and share their information unknowingly and their lack of knowledge makes them vulnerable to cyber-attacks. So cyber security is the main concern in today's world of computing. It is a general term covering crimes like credit card fraud, bank robbery, illegal downloading, industrial espionage, child pornography, child abduction through chat rooms, scams, cyber terrorism, creation and distribution of viruses, spam etc.

The main purpose of social networking sites is to connect people and organizations. Social media has introduces significant change in the way people communicate. Social networking sites bring out a specific concern related to privacy and security of the user. As the internet usage has increased in India, cyber-crimes have also increased respectively. Cyber-crimes are registered under three broad heads in India, the Indian Penal Code (IPC), the IT Act and other State Level Legislations (SLL). The cases registered under the IT Act include India is among the few countries that have strict laws to combat cybercrime. The IT Act, 2000 (Information Technology Act, 2000) has been enacted.

As growing popularity of the Social Networking Sites these have become a prime target for cyber-crimes and attacks. So be careful when disclosing your ID number, net banking account number, your ID number, password, credit or debit

password number or your personal information while using the Internet. Safety measures should be taken while shopping online. Along with the positive use of the Internet, misuse by miscreants can shake the life of the common man, the order of the nation, the economy. We are starting this educational program to shed light on the scope of this cyber crime, the security to be taken about it, A cyber-attack is an exploitation of computer systems and networks. It uses malicious code to alter computer code, logic or data and lead to cybercrimes, such as information and identity theft. So that students should be introduced to these cyber security certificate courses.

The syllabus should incorporate all the essential elements of cyber security so that the students learn understand the concept of cyber security as a whole. The syllabus should have sufficient depth so that even students from the non-technical streams can develop a complete picture of cyber security.

People, Process and Technology are the important pillars of the Cyber security, as to how, effectively the aspects related to these components fit into the curriculum considering the cyber threat landscape forms part of the content structuring and syllabus formation. With this backdrop, the following aspects, as tabulated below, have been taken into consideration in the syllabus formation: -

Course Coordinator
(Dr. G. J. Gavit)

# Table of Contents

# Chapter 1.
## Introduction to Cyber Security

The internet was born around 1960‟s where its access was limited to few scientist, researchers and the defence only. Internet user base have evolved expontinanlty. Initially the computer crime was only confined to making a physical damage to the computer and related infrastructure. Around 1980‟s the trend changed from causing the physical damaging to computers to making a computer malfunction using a malicious code called virus. In 1996, when internet was launched for the public, it immediately became popular among the masses and they slowly became dependent on it to an extent that it has changed their lifestyle. The focus of the computer crime shifted from merely damaging the computer or destroying or manipulating data for personal benefit to financial crime. These computer attacks are increasing at a rapid pase. Every second around 25 computers became victim to cyber attack and around 800 million individuals are affected.

The term cyber crime is used to describe a unlawful activity in which computer or computing devices such as smart phones, tablets, Personal Digital Assistants(PDAs), etc. which are stand alone or a part of a network are used as a tool or/and target of criminal activity.

**Cyber security definition:-**

1. Cyber security is the application of technologies, processes, and controls to protect systems, networks, programs, devices and data from cyber attacks.
2. It aims to reduce the risk of cyber attacks and protect against the unauthorized exploitation of systems, networks, and technologies.

3. Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack.
4. Illegal activities committed using electronic devices over cyberspace constitute cyber crime.
5. Cyber Crime is any criminal activity that involves a computer, networked, device or a network.

The first comprehensive published work Security Controls for Computer Systems which became the foundation in the field of cyber security was a technical report commonly called the Ware Report. This report, published in 1970, was the result of a study carried out by a task force on computer security organized by the department of defence of United States of America. The report concluded that a comprehensive security of a computer system requires a combination of hardware, software, communications, physical, personnel and administrative controls. The first computer program (also the first non-self-replicating benign virus in history) that could move across a network was written in 1971, leaving a message trail (I am the creeper, catch me if you can) behind wherever it went. The program was called the Creeper. The first example of an antivirus program (it performed the same functions that an antivirus does today) was written in the year 1973 called the Reaper, which chased and deleted the Creeper.

The three basic principles for cyber security and are still widely used benchmarks to evaluate the effectiveness of a cyber security system.

**Confidentiality :-**

The confidential information and data should be prevented from reaching the wrong hands. Confidentiality deals with the access, operation, and disclosure of system elements.

**Integrity :-**

The information and data should not be corrupted or edited by a third party without authorization. Integrity deals with the modification, manipulation, and destruction of system elements.

**Availability :-**

The information and data should be available all the time and adaptive recovery mechanisms should be established to restore the system and the services provided by the system. Availability deals with the presence, accessibility, readiness,

Cyber security proper began in 1972 with a research project on ARPANET (The Advanced Research Projects Agency Network), a precursor to the internet. Researcher Bob Thomas created a computer program called Creeper that could move across ARPANET's network, leaving a breadcrumb trail wherever it went. The 1980s brought an increase in high-profile attacks, including those at National CSS, AT&T, and Los Alamos National Laboratory. Despite this, in 1986, German hacker Marcus Hess used an internet gateway in Berkeley, CA, to piggyback onto the ARPANET. He hacked 400 military computers, including mainframes at the Pentagon, intending to sell information to the KGB.

1987 was the birth year of commercial antivirus, although there are competing claims for the innovator of the first antivirus product.

Stuxnet found in the year 2010 was the first weaponized malware program, and one of the first instances where cyber attacks were used in espionage. Stuxnet spread using an infected removable drive such as a USB flash drive. The best cyber security defense for a system is to know and reduce the current and future Cyber security risks to the system.

**Layers of Cyber Security:-**

1: Mission Critical Assets**:-** This is the data you need to protect

2: Data Security**:-**Data security controls protect the storage and transfer of data.

3: Application Security**:-**Applications security controls protect access to an application, an application's access to your mission critical assets, and the internal security of the application.

4: Endpoint Security: - Endpoint security controls protect the connection between devices and the network.

5: Network Security: - Network security controls protect an organization's network and prevent unauthorized access of the network.

6: Perimeter Security: - Perimeter security controls include both the physical and digital security methodologies that protect the business overall.

7: The Human Layer: - Humans are the weakest link in any cyber security posture. Human security controls include phishing simulations and access management controls that protect mission critical assets from a wide variety of human threats, including cyber criminals, malicious insiders, and negligent users.

**********

# Chapter.2
# Cyber crime and Cyber law

The Information and Technology (IT) Act, 2000 contains various provisions dealing with cybercrimes in India. With 'police' and 'public order' being in the State List, the primary obligation to check crime and create the necessary cyber infrastructure lies with States. At the same time, with the IT Act and major laws being central legislations, the central government is no less responsible to evolve uniform statutory procedures for the enforcement agencies.

## Classification of Cyber Crimes:-

The cyber criminal could be internal or external to the organization facing the cyber attack. Based on this fact, the cyber crime could be categorized into two types:

### (1) Insider Attack: -

An attack to the network or the computer system by some person with authorized system access is known as insider attack. It is generally performed by dissatisfied or unhappy inside employees or contractors. The motive of the insider attack could be revenge or greed. It is comparatively easy for an insider to perform a cyber attack as he is well aware of the policies, processes, IT architecture and wellness of the security system. Therefore it is comparatively easy for a insider attacker to steel sensitive information, crash the network etc.

### (2) External Attack: -

When the attacker is either hired by an insider or an external entity to the organization, it is known as external attack. The organization which is a victim of cyber attack not only faces financial loss but also the loss of reputation. Since the attacker is external to the organization, so these attackers usually scan and gathering information. External attacks can be traced out by carefully analyzing these firewall logs. Also, Intrusion Detection Systems are installed to keep an eye on external attacks.

Cyber crimes have turned out to be a low-investment, low-risk business with huge returns. Now-a-days these structured crimes are performed are highly organized. There is a perfect hierarchical organizational setup like formal

organizations and some of them have reached a level in technical capabilities at par with those of developed nation. They are targeting large financial organizations, defence and nuclear establishments and they are also into online drugs trading.

**Malware and its type:** -

Adware It is a special type of malware which is used for forced advertising. They either redirect the page to some advertising page or pop-up an additional page which promotes some product or event. These adware are financially supported by the organizations whose products are advertised.

1. **Spyware :** -

It is a special type of which is installed in the target computer with or without the user permission and is designed to steal sensitive information from the target machine. Spywares may be of various types; It can keeps track of the cookies of the host computer, it can act as a key loggers to sniff the banking passwords and sensitive information, etc.

2. **Browser :** -

Hijacking software There is some malicious software which are downloaded along with the free software offered over the internet and installed in the host computer without the knowledge of the user. This software modifies the browsers setting and redirect links to other unintentional sites.

3. **Virus :** -

A virus is a malicious code written to damage/harm the host computer by deleting or appending a file, slow down the performance of the computer, format the host machine, etc. It can be spread via email attachment, pen drives, digital images, e-greeting, audio or video clips, etc. A virus may be present in a computer but it cannot activate itself without the human intervention.

4. **Worms :** -

They are a class of virus which can replicate themselves. They are different from the virus by the fact that they does not require human intervention to travel over the network and spread from the infected machine to the whole network. Worms can spread either through network, using the loopholes of the Operating System or via email.

5. **Trojan Horse :** -

Trojan horse is a malicious code that is installed in the host machine by pretending to be useful software. It not only damages the host computer by manipulating the data but also it creates a backdoor in the host computer so that it could be controlled by a remote computer. The computers of this network which are infected by malicious code are known as zombies.

**Kinds of cyber crime :** -

Given below are some types of cybercrimes in India that have affected internet users and the cases are recurring. A quick read of types of cybercrime with examples can help understand the context.

**1. Cyber Stalking :** -

It is an act of stalking, harassing or threatening someone using Internet/computer as a medium. This is often done to defame a person and use email, social network, instant messenger, web-posting, etc. as a using Internet as a medium as it offers anonymity. The behavior includes false accusations, threats, sexual exploitation to minors, monitoring, etc.

**2. Child Pornography :** -

It is an act of possessing image or video of a minor (under 18), engaged in sexual conduct.

**3. Software Piracy :** -

Piracy is an illegal reproduction and distribution for personal use or business. It comes under crime related to IPR infringement. Some of the other crimes under IPR infringement are: download of songs, downloading movies, etc.

**4. Cyber Terrorism :** -

It is defined as the use of computer resources to intimidate or coerce government, the civilian population or any segment thereof in furtherance of political or social objectives.

**5. Phishing :** -

The purpose of phishing is identity theft and the personal information like username, password, and credit card number etc. may be used to steal money from user account. If a telephone is used as a medium for identity theft, it is known as Vishing (voice phishing). Another form of phishing is Smishing, in which sms is used to lure customers.

**6. Computer Vandalism : -**

It is an act of physical destroying computing resources using physical force or malicious code.

**7. Cyber Squatting : -**

It is an act of reserving the domain names of someone else's trademark with intent to sell it afterwards to the organization who is the owner of the trademark at a higher price.

**********

# Chapter 3
## Social Media Overview and Security

These days, many internet clients consistently visit a large number of social site to continue connecting with their companions, share their thoughts, photographs, recordings and talk about even about their everyday life. In 1971 where two PCs were sitting ideal alongside each other. In 1987 Bulletin Board System exchanged information over telephone lines with different clients and of late around the same year the main copies of early web programs were conveyed through Usenet. Geocities was the primary social site established in 1994. In 1997, the America on Line (AOL) Instant Messenger was lunched. In 2003, My Space was lunched and in the next years numerous other social networking like Face book in 2004, Twitter in 2006 and so forth. There are such a large number of social networking destinations and social media locales that there is even search engine for them. These social sites have constructive and negative effects; such huge numbers of peoples waste most of their time on utilizing these sites, which brings about losing their employments or universities or even their normal social lives and families! Numerous others post copyrighted materials without authorizations, pornographic or banned contents.

In the now days The Internet, sorry to say, offers too many ways to the virtual criminals and gives many ability to hack accounts on social network websites and the right now, there are large numbers of malicious series of programs that objective to get the data from the social sites. Usually, users commit numerous risks and errors when utilizing social networks services, for example, utilizing unapproved programs, misuse of corporate PCs, unapproved

physical and network access, misuse of passwords and exchange touchy data between their work and computers when working at homes

**Security Issues on Social Media Network site:-**

As the growth of social networking sites has brought various benefits it also has brought various security concerns. It also provides a vulnerable platform to be exploited by the attackers. Some issues associated are as follows.

**1) Misusing Identity:** -

The attacker impersonate identity of any user results in misusing identity The attackers attack through the applications in which they ask for granting permission for accessing the information provided in Social Networking Sites. When a user allows doing so, they will gain access to all the information and that information can be misused without the knowledge of the user.

**2) Threats from using 3rd Party Applications:-**

These applications seek permission from the user to access personal information for all the various games and apps. The user grants the app a certain level of permission concerning user's information. And some of these applications which are playing at the foreground may download a malware on the user's computer or phone without their consent.

**3) Trusting Social Networking Sites Operators:-**

The contents that user uploads or posts on social networking sites, the information is available with the networking operators. The operators can save account data even after deletion.

**4) Viruses, Phishing Attacks and Malwares:-**

Viruses and malware often find their way onto your computer through those annoying ads. After gaining access to the network, the attacker can access or steal confidential data by spreading spam mails.

**5) Legal Issues:-**

Posting contents that is offensive to any individual or community or country. There are legal risks associated with the use of social networking sites like leaking confidential information on sites or invading on someone's privacy.

**6) Tracking Users:-**

It can cause physical security concerns for the user, as the third parties may access the roaming information of the user by collecting the real time update on user's location.

**7) Privacy of Data:-**

Users share their information on social networking sites and can cause privacy braches unless proper security measures are applied.

Social Networking Sites which has the privacy security setting discusses the tools which available to make the account more secure. Like Facebook's privacy settings where the privacy basics are subdivided as-

**1) Who-can-see-my-stuff:-** This is priority setting for the Facebook users where the user can limit the audience who can see the posts from the user. Public posts should be avoided for security

**2) Login-Alerts:-** This setting allows the user to get a notification when anyone logs into their account from an unrecognized device or browser.

**3) Third-party-authenticator:-** This is the new setting added to the Facebook which enables to generate Facebook security code to authenticate any third party app

**4) How others interact with the user:-** This helps user to manage how other people's activity affect the user's profile. And the user can manage tags, 'unfriend' or 'block' someone.

# Chapter 4
# E – Commerce and Digital Payments

Sharing business information, maintaining business relationships and conducting business transactions using computers connected to telecommunication network is called E-Commerce.

**Advantages Of E-commerce** -:

- Buying/selling a variety of goods and services from one's home or business Anywhere, anytime transaction
- Can look for lowest cost for specific goods or service
- Businesses can reach out to worldwide clients
- can establish business partnerships
- Order processing cost reduced
- Electronic funds transfer faster
- Supply chain management is simpler, faster, and cheaper using ecommerce
- Can order from several vendors and monitor supplies.
- Production schedule and inventory of an organization can be inspected by cooperating supplier who can in-turn schedule their work.

**Disadvantages Of E-commerce** -:

- Electronic data interchange using EDI is expensive for small businesses
- Security of internet is not very good
- viruses, hacker attacks can paralyse
- e-commerce Privacy of e-transactions is not guaranteed
- E-commerce de-personalizes shopping

**Threats of E-commerce -:**

- Hackers attempting to steal customer information or disrupt the site
- A server containing customer information is stolen.
- Imposters can mirror your ecommerce site to steal customer money
- Authorized administrators/users of an ecommerce website downloading hidden active content that attacks the ecommerce system.
- A disaffected employee disrupting the ecommerce system.
- It is also worth considering where potential threats to your ecommerce site might come from, as identifying potential threats will help you to protect your site. Consider:
- Who may want to access your ecommerce site to cause disruption or steal data; for example competitors, ex-employees, etc.
- What level of expertise a potential hacker may possess; if you are a small company that would not be likely to be considered a target for hackers then expensive, complex security may not be needed.

**Modes of Digital Payment :-**

• Banking Cards (Credit, Debit, Stored value/prepaid) Used in conjunction with PoS machines, ATMs, Online

• Unified Payment Interface (UPI) – authenticates the identity of the user like a debit card does using the phone as a tool instead of a separate card – Smart phone & bank account

• e-Wallets – a type of electronic card which is used for transactions made online through a computer or a smart-phone – Utility of e-wallet is same as a credit or debit card – Make paperless money transaction easier.

• Unstructured Supplementary Service Data (USSD) – Mobile banking for feature phones – Offered through a National Unified USSD Platform (NUUP) on a short code *99#.

• AADHAR Enabled Payments – Allows bank-to-bank transaction at PoS (Micro ATM) with the help of Banking Correspondent

**DOs & DON'Ts**

**• DOs –:**

- Password protect the mobile phone / device.
- It is recommended to set the maximum number of incorrect password submissions no more than three.
- Choose a strong password to keep the account and data safe.
- Review the account statements frequently to check for any unauthorized transactions.
- Change the PIN regularly.
- Report a lost or stolen phone / device immediately to the service provider and law enforcement authorities.

**DON'Ts –:**

- Never give the PIN or confidential information over the phone or internet. Never share these details with anyone.
- Don't click on links embedded in emails/social networking sites claiming to be from the bank or financial institutions.
- Don't transfer funds without due validation of the recipient, as funds once transferred cannot be reversed.
- Don't store sensitive information such as credit card details, mobile banking password and user ID in a separate folder on your phone.

- Don’t forget to inform the bank of changes in the mobile number to ensure that SMS notifications are not sent to someone else.
- Never reveal or write down PINs or retain any email or paper communication from the bank with regard to the PIN or password.
- Be cautious while accepting offers such as caller tunes or dialer tunes or open/download emails or attachments from known or unknown sources.
- Be cautious while using Bluetooth in public places as someone may access the confidential data/information. Similarly with using public Wi-Fi.

**Some online fraud related online network site:-**

- **CVV/OTP Sharing Fraud :-**

Cyber criminals posing themselves as bank /RBI officials call people and tell them that their ATM card has been blocked or their KYC (Know Your Customer) is not updated or their Aadhaar is not linked to their bank account & hence their account will be blocked. Then on the pretext of updating the KYC/linking bank account to Aadhaar or for resuming the services of ATM card/activation of new ATM card asks for details related to victim’s bank account like ATM card number, CVV number, OTP etc. After these details are shared by victim, money is siphoned off from the victim’s bank account.

- **UPI Phishing Fraud :-**

On the pretext of helping in banking related issues, fraudsters ask victims to forward an alphanumeric link to a particular number (depending upon the bank associated with the victim) from their registered mobile number. Once it is done, cyber criminals install the UPI wallet of the victim (using Wi-Fi) bypassing the SIM binding process onto their own mobile phone, thus gaining access to the victim’s bank accounts linked to the registered mobile number.

FRAUD BY REQUEST MONEY QR CODE/LINK ON GOOGLE PAY/PHONEPE/PAYTM

- **Fraud by Request Money QR Code/Link on Google Pay/Phonepe/Paytm :-**

Cyber fraudsters send debit links or QR codes to victims to scan and receive money in their bank accounts through Google Pay/PhonePe/Paytm. But instead of receiving money, it actually gets debited from the victim's account as fraudsters actually send a request money QR code/link.

- **Fraud Using Google Docs App**

Apps for online forms like Google Docs etc. are widely used to collect data. Fraudsters take advantage of such applications and misguide the victim to fill or submit his/her confidential bank related data like ATM number, UPI PIN, password etc. As soon as they fill up the form and submit their data, it is directly transferred to the creator of the form.

- **Fraud Using OLX / e-commerce :-**

Cyber fraudster uses the e-commerce platforms like Olx/Quikr/Facebook for giving fake advertisements to sell commodity at lucrative prices. When someone intends to buy, cyber fraudster asks for advance payment in the form of packaging/transportation/registration charges etc. Buyer pays the money believing him/her to be a real seller and the fraudster disappears with the money. Frauds are also committed by cyber criminals posing themselves as buyers to real sellers. In this modus operandi, cyber criminals get the seller's account debited on the pretext of paying advance money by sending request money link/QR code instead of the credit link/QR code.

- **Fraud through Fake Cash back Offers :-**

Fraudsters lure victims by offering cash back offers from Phone Pe/Google Pay etc. and request the victims to click on a request money link or scan a QR code to avail the same. Once the link is clicked or QR code is scanned, money is debited

from the victim's bank account instead of being credited as he enters MPIN or UPI PIN.

- **Fraud using Fake Social Media Account :-**

Fraudsters target accounts on popular social media platforms like Facebook and Instagram. They commit fraud by creating a similar fake account of the target profile and requesting his/her friends for instant money transfer citing some medical emergency etc. Target profile's friends transfer the money considering him/her as his/her friend. By the time the target profile comes to know of it, many of his friends become victims of the fraud. Similar fraud is also committed by hacking the target account.

- **Sextortion On FACEBOOK :-**

Live video chat is done on Facebook via Messenger by cyber criminals posing as female. Cyber criminals convince the victim for video call in compromising positions, following which fraudsters take screenshots of the same or do screen recording of the video call. Cyber criminals then threaten the victim to circulate the photographs/videos in compromising positions on various online platforms, if the demanded money is not paid.

- **Harassment through Fake Social Media Profiles :-**

Cyber criminals morph the photographs of the victim which they get from social media and upload it on social media platforms. After that they demand money to remove the morphed pictures from social media. Victim falls prey to the trap and transfers the money.

- **Cyber Bullying on Social Media :-**

Cyber bullying is bullying with the use of digital technologies. It can take place on social media, messaging platforms, gaming platforms etc. It is a sort of repeated behavior, aimed at scaring, angering or shaming those who are

targeted. Examples include: spreading lies about or posting embarrassing photos of someone on social media, sending hurtful messages or threats via messaging platforms, impersonating someone and sending mean messages to others on his/her behalf.

- **Lottery Fraud / Nigerian Fraud :-**

Cyber fraudsters send e-mails/SMSs informing the recipient (victim) that he/she has won a lottery/prize worth millions of rupees/dollars and the recipient only needs to click on the link sent on their e-mail/mobile phone or to tell how they want to receive the prize money. However, on responding positively, the recipient is asked to pay money in the name of registration/shipment/service charges, GST etc. one after the other for releasing the prize money. This way the recipient keeps on paying the fraudsters until he/she realizes the fraud. The fraudsters were initially mainly from Nigeria and hence the terminology.

- **Edited Google Customer Care Number Fraud :-**

Cyber fraudsters edit the customer care number of banks/airlines/food outlets/ecommerce entities etc. on Google page and customize it in such a manner that whenever someone searches on Google for the customer care number, the edited number of cyber criminals appears on top of the search results for that entity. Victim ends up calling the fraudsters instead of the real helpline numbers. The fraudsters portraying themselves as helpers actually give instructions to dupe the caller victim.

**********

# Chapter 5
# Digital Devices Security and Awareness

Mobile devices (i.e. cell phones laptops tablet) have become an indispensable part of our everyday life, since they fulfill the increasing users

- **Fraud using Screen Sharing Apps :-**

Cyber fraudsters on the pretext of aiding or citing the policy of a company guide the victim to install screen sharing apps like Quick Support/TeamViewer/AnyDesk etc. and thus get control of the victim's phone, thereby getting access to banking credentials like OTP/MPIN/username/password for internet banking etc. The fraudster then siphons off money from the victim's account using those credentials. By the time the victim realizes it, a lot of money is already siphoned off.

- **SIM Card Swapping Fraud**

It is a type of identity theft where cyber criminals manage to get a new SIM card issued for your registered mobile num ber through the Telecom Service Provider. With the help of the new SIM card, fraudsters get OTP & other confidential details required for financial transaction from your bank account.

- **ATM/DEBIT Card Cloning Fraud :-**

Each ATM/debit card has a magnetic strip in it containing confidential data. Cyber criminals use a skimmer machine to read this strip and capture the confidential data related to the card. Then they copy the data onto a blank card, which is used for fraudulent transactions. They use overlay devices/pin-hole camera/ spy camera or peep from behind in the queue to read ATM/Debit card PIN while it is being entered by the user on the ATM keypad/POS machines.

- **Computer or Device Hacking :-**

Hacking is the act of gaining access to a computer/device without legal authorization. Cyber criminal uses various methods for hacking a victim's computer/device such as infecting a computer/device by a virus or malware. Hacking may lead to data corruption/deletion or data loss or stealing of data

- **Mobile Application Fraud :-**

Mobile applications may be mediums of cyber-attacks, stealing of confidential data or mode of getting access to the controls of your phone/device. People download mobile applications from unknown sources ignoring security warnings. These applications may have viruses which pass sensitive information or give control of your phone/device to some outside agent, who gets access to your contacts, passwords, financial data etc. Several mobile applications from unknown sources ask for unnecessary permissions for access to your phone/device, which one grants without due diligence. Thus, these mobile applications can access a huge amount of personal information, photographs etc. from your phone/device.

**General Cyber Safety Tips**

- For Device/Computer Security
- Keep your antivirus and operating system updated at all times.
- Backup your sensitive/important data at regular intervals.
- Be careful while opening suspicious web links/URLs.
- Always scan external storage devices (e.g. USB) for viruses, while connecting to your device.
- To prevent unauthorized access to your device, consider activating your wireless router's MAC address filter to allow authorized devices only.

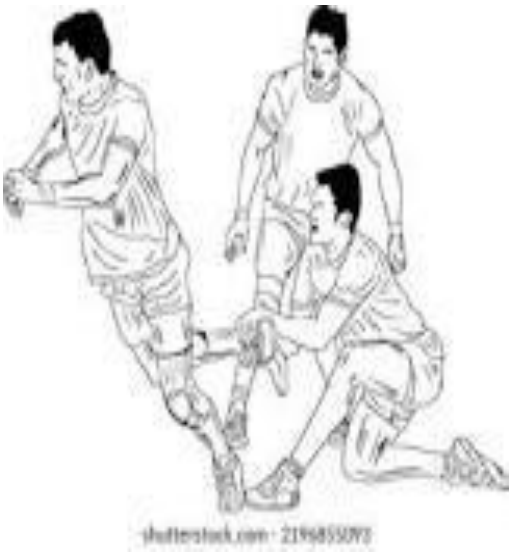
- Wireless router can screen the MAC addresses of all devices connected to it, and users can set their wireless network to accept connections only from devices with MAC addresses recognized by the router.
- Secure all your wireless access points with a strong password. Hackers usually scan for open access points and may misuse it to carry out unwanted activities. Log records may make you more vulnerable for such misuse.
- Merely deleting sensitive material is not sufficient, as it does not actually remove the data from your device. 'File Shredder Software' should be used to delete sensitive files on computers.
- Delete unwanted files or data from your computer device. It prevents unauthorized access to such data by others.
- Use 'Non-Administrator Account' privileges for login to the computer and avoid accessing with 'Administrator' privileges for day-to-day usage of computers.
- Make sure to install reputed mobile anti-virus protection to protect your mobile from prevalent cyber threats and also keep it updated.
- In case of loss or theft of your mobile device, immediately get your SIM deactivated and change passwords of all your accounts, which were configured on that mobile.
- Do not leave your phone unattended in public places and refrain from sharing your phone password/ pattern lock with anybody.
- Always enable a password on the home screen to restrict unauthorized access to your mobile phone. Configure your device to automatically lock beyond a particular duration.

- Always lock your computer before leaving your workplace to prevent unauthorized access. A user can lock one's computer by pressing 'Ctrl +Alt + Del' and choosing 'Lock this Computer' or "Window button+ L".
- Remove unnecessary programs or services from computer which are not required for day to day operation

**********

# A HAND BOOK ON KABADDI

**Simple Easy learning**





By Dr. Tejas R Sharma (Director of Physical Education)
Late Annsaheb P S Wadile Arts College, Thalner

## About the tutorial:

Kabaddi originated in India that teaches you a traditional way of self-defence. Another beauty of this game is that it needs neither costly playing equipment nor a big playground.

The basic purpose of this tutorial is to introduce the basic playing fundamentals and rules of kabaddi.

## Audience:

This tutorial is aimed at giving an overall knowledge to a person who does not know how to play kabaddi. Step by step illustration and guidance will help the beginner to build his fundamental pillars about this game successfully.

## Prerequisites:

You can have a good grasp upon the fundamentals of kabaddi from this small tutorial, if you have the passion and eagerness to play this game.

# Table of Contents

# KABADDI – Overview

Kabaddi is a popular team sport, which needs skill and power, and conflates the characteristics of wrestling and rugby. It is originated in India 4000 years ago. It is widely played across the Indian subcontinent. Originally it was intended to develop self-defence. It is a simple and inexpensive game and does need a massive playground nor expensive equipment.

It is also known as the Game of the Masses because of its simplicity and public appeal. As it requires less expensive equipment, it is very popular in the developing nations. It is an out door sport, which is played on clay court, but synthetic surface indoors are being used now-a-days.

Kabaddi is known by various names, i.e., Chedugudu or Hu-Tu-Tu in southern India, Hadudu ( for Men) and Chu –Kit –Kit (for women) in eastern India, and Kabaddi in northern India. It is far more popular in the villages of Punjab, Tamil Nadu, Andhra Pradesh, Uttar Pradesh, Bihar, Maharashtra, Madhya Pradesh, and Gujarat.

## Objective

The main objective of this game is to grab points by raiding into the opponent's court and touching as many opponent players as possible without getting caught on a single breath. Each player, chanting “Kabaddi! Kabaddi! Kabaddi” enters into the opponent court and try to touch the defense players nearest to him, while the opponents make tactical coordinated efforts to catch that player.

## Team Size

Every team consists of 12 players, of which seven are on court, and five in reserve. The two teams fight for higher scores, alternating defence and offence. Participants from various countries form teams for major tournaments or championships conducted across the globe. Two teams compete with each other for higher scores, by touching or capturing the players of the opponent team.

## A Little History of Kabaddi

Tracing shows its existence since pre historic time. Earlier times it was used not only as an entertaining game but also was used to build physical strength and stamina needed to deal with the day to day work. They used it as a self-defensive tool. A hint about the existence of the game far behind from the pre historic time can be seen nowhere else but in great Hindu mythology Mahabharata, where Abhimanyu’s Chkrabyuha Trap and his defense against that was itself self-explanatory.

Even it is said that Arjuna was very good at this art. He used to go into the enemy’s wall to destroy them and used to come back unhurt. Gautama Buddha was also using this game as a means to know his inner strength and stamina and manuscripts say that through this game only he got his bride.

In the year 1918, Kabaddi was given national game status. All rules and regulations were also formulated in the same year but officially implemented after 1923 but it took quite a long time (1938) to be introduced into Indian Olympics

## Participating Countries

Since Kabaddi originated in India, the neighbouring countries could easily access it and learn the game. Over the years, Asian countries have dominated this game and they are considered to produce world's best players in Kabaddi.

Apart from India, millions of people from countries like Sri Lanka, Japan Bangladesh, Chinese, Taipei, Nepal, Malaysia, Afghanistan, Kambodia, Indonesia, Kyrgyzstan, Turkmenistan, Oman, South Korea, Thailand, Iran and Pakistan participate in Kabaddi. Most of these Asian countries also have their own Kabaddi Confederation bodies.

Kabaddi is gaining popularity in countries like Argentina, Sierra, Leone, Denmark, New Zealand, Canada, USA, Australia, England, Italy, Kenya, Norway, Scotland etc. and have also formed their Kabaddi federations. Countries like Australia, New Zealand, Canada and United States have also picked up the game and it is rapidly gaining popularity amongst the citizens.

# Kabaddi – Playing Environment

Kabaddi is a game of excess physical work. Apart from excessive physical work, it requires excess stamina and good tactics. You should know the way to get into other team's area and come back successfully without getting obstructed by your opponents. But before heading towards the game let's know the basic necessities that you will require to play this game.

## Necessary Requirements

### The Court

The court measures 12.5-meter length and 10 meter wide. A mid line is drawn in the court, splitting into two halves. The depth of the court is 1 foot in which sand is filled by removing mud.

### Dress Code

The game demands excessive physical work where one has to pull or push another. Therefore, excessive loose-fitting dresses are not allowed. Only a short and a vest is considered to be ideal. In some tournaments like the "Pro Kabbadi League", players are allowed to wear colored T-shirts to represent their team.

### Teams

Total numbers of player in each team is 12. Only 7 players are allowed in to the playing court. Rest 5 will be kept as reserved. During the game only the leader is allowed to give instructions to the other players in his team.

### Play Duration

The playing duration is different for different genre. For men's there will be two sections of play, each bearing a time line of 20 minutes. In women's and children's category of match the two sections and each half is of 15 minutes each. After the end of one session, the team is allowed to take a 5 minutes' break.

### Officials

There are different types of officials present in the game. Let's know about them in detail. Six officials are nominated to conduct a Kabaddi Match. Among them, two are umpires, one is a scorer, one is an assistant scorer and one is a referee.

- Referee: He has the power to warn, declare point against or Dis-qualify a participant from match. He has the authority to over-turn the decision given by umpire.
- Umpire: Generally, the decision of the umpire taken as final.
- Scorer: The scorer fills the scores data, timings, time-outs.
- Assistant Scorers: They record those players who are out and those who are survived.

# Kabaddi – How to Play?

## Marking of Lines

In the 12.5×10 meter playground, the outer lines, known as Boundary lines, are marked with colored sands. Playing areas are marked with one-meter space from each side of the 10 meters' boundary line.

To separate the territory of each team, a middle line is drawn in such a fashion that it divides the whole court in to two equal 6.5×8 metre sections. The position of baulk lines can clearly be seen from the above picture. They are positioned at a distance of 3.75 meters on the either side of the middle line. On the either side of the middle line, bonus lines are drawn which are present at a distance of 1 metre from it.

## Toss and Decide

Tossing of coin is done to determine which team will go first. Sometimes tossing is done with an unbiased dice also.

## Raiding

After winning the toss, the team takes turn and sends players, often known as raiders into opponent team's sections. The sole aim of the raider is to tag the members of the opposite team and run back into his team side. Each player he touches on the opponent's side gives his team one point.

- The team with the maximum score at the end is declared as winner.
- If a match end in a tie, then two 5 minutes durations are given.
- If the tie still exists after (20+20+5+5) 50 minutes of play, then the team that scored first will be declared the winner.

The raider needs to repeatedly yell the word "Kabaddi" soon after crossing the mid line and he needs to keep it yelling till he safely returns to his zone. It is worth noting that, under no circumstances the raider should stop yelling the word "Kabaddi". In case if he does so, he should return to his zone as soon as possible. This will yield no point to his team but will earn a point to his opponent team for successfully defending him.


**Raiding** should be done in proper order by the team. That means in a sequence, each team needs to send its all players to the opposite side. The opponent team can earn a point by not letting the raider return to his section.

## Defence

In case your team lose the toss, it will be raided by the other team. Then it is the responsibility of your team to stand in front and defend. You should not tag yourself by the raider. Doing such will fetch a point to the raider's team. To avoid yourself from being tagged, you should run as far as possible from the raider, till he becomes breathless of saying "Kabaddi".

If he tags you, wait till the raider becomes breathless and as soon as the raider stops saying kabaddi, grab him with your team mates before he touches the middle line. You cannot pull the cloths or hairs of the raider. Rather you can grab him only at his limb or torso.

Alteration between the raiding and defending goes on between the two teams for 20 minutes. After the end of first session players take 5-minute break. After that switching between the two teams take place to either side of the court. The team which gathers maximum point at the end of two sessions wins the match.

# Kabaddi – Game Tactics

Knowledge about the game is not enough. Physical force is just 50% of the basic need that a game demands; another 50% is the tactics required to use your physical force efficiently. So let's discuss about some necessary game tactics that you need.

## Raid Mechanisms

The attacking style is known as raid mechanism. One difficult thing in kabaddi is that the raider will be one, while the defender will be many. So the raider must have skilled tactics to tag the opponents and come back safely towards the middle line.

The whole game of kabaddi can be changed in couple of minutes with the help of few good raiders. Therefore, it is utmost necessary to understand the raiding mechanism very carefully. The raiding depends upon number of factors. Some of the important ones are:

- Entry
- Cant
- Footwork
- Settling path of attack
- Tactics
- Retreat

A right entry can give a raider a safe exit. The defenders always pre-plan about every move that a raider is going to make. The most important part for a raider is to judge it in advance and make a right entry. After the entry the raider must act quickly enough to finish it come back before he becomes breathless in doing can't.

After entering, the first step for the raider is to judge its defenders very well. He should also see the defenders outside the ring. That is because an ineffective raid may bring a strong defender into the ring and may make their defense stronger next time. He should also have the idea about the various strong defense moves of the players present in that ring. Knowledge of this will help him a lot in saving himself from being caught.

From time to time, the defenders change their system of play. The raider must be able to judge that and act accordingly. Their strategy will vary in accordance with the number of players they are having. For example, with 4 numbers of players they may approach the format of 2-2, 1-2-1 or 1-1-2. It is the raider who should be able to judge that one correctly to make his safe move towards the middle line.

Situations matter in the game of kabaddi to make your move as a raider. If your team needs to score point, then you have to tag any one of them to upbring your team into a safe zone otherwise; coming back into your zone without crossing the baulk line is a wise decision.

Presently **bonus line game** is in vogue. The bonus depends upon the number of antis that you have on the other side of your zone. If the number of antis are 6, then just by crossing the bonus line you can earn a point for your team. Otherwise, you

have to go deeper inside the zone to score.

## Cant

The most unique feature of kabaddi is its cant. Beginners often find themselves in difficult position in doing this. The rule says you have to chant the word "kabaddi" as soon as you enter the defending zone and should continue till you come back to your side by crossing the middle line. If the player fails in this at any moment during his raid, he will be out of the match. So indirectly the duration of cant can be used as an I-measurement tool of kabaddi.

## Entry

A raider can use right, left, or central zone for his entry into the court. However; his entry depends upon the following factors very strongly:

- The position of the raider at the time of his act as team's defence system.
- The direction of attacking side
- His moving direction

A player fighting for right corner should start with an anti-present in the right side and similarly for left and corner size. Starting of the cant should be made before entering to the defending zone. This is because if the raider makes any delay in the cant process after entering the defending zone, then under late cant penalty he may be debarred of the match.

## Footwork

The movement of the foot of the raider during his raid is most important. The footwork however depends upon the following factors:

- Position of the body
- Stance of the raider
- Speed with which he moves
- Agility
- Style of movement

The raider should bring speed in his movement during the raid. He should keep in his mind that the work should be finished as soon as possible as the loose of breath will lose the cant process and his team may get penalized. Footwork can be divided into four categories basically.

- Leading leg raid
- Natural method
- Reverse step raid
- Shuffling raid

## Necessary Skills

A man needs skills to have mastery upon techniques. There are broadly two categories of skills that a kabaddi player needs to learn are offensive skills and defensive skills. For example, during a raid, a raider must try to touch the antis with the maximum use of his limbs. It will make easy for him and for his team to score points. Some touches that are legal in kabaddi are;

- Foot touch
- Toe touch
- Thrust
- Squat leg
- Kicks
- Touching of hand through upper limbs

## Retreat

After the starting of the raid, until and unless the raider returns to the home zone safely, the raid is not accepted as successful. This is known as retreat. Before going to the opponent's zone, the raider must pre-plan his retreat.

No room for pursuit should be given by the raider to his antis. As soon as the raider comes back from the raiding, he should position himself in his team's defensive system. For example, if a player is supposed to defend his team at right corner, but if he returns from the raid by left corner, then the antis may attack quickly and the team's defensive system may jeopardize.

# Kabaddi – Governing Bodies

## All India Kabaddi Federation (AIKF)

To increase the popularity of kabaddi as a sport in India, All India Kabaddi Federation (AIKF), was founded in 1950. Since its establishment, the AIKF has been working towards improving the standards of the game. For this purpose, it conducts National level kabaddi championships regularly since 1952, as per the rules and regulations. The first men's national tournament was organized in Madras (Chennai) and the first women's national tournament was held in Calcutta (Kolkata).

## Amateur Kabaddi Federation of India (AKFI)

The Amateur Kabaddi Federation of India (AKFI) is the central institution to administrate and promote Kabaddi in India. It was established in 1973. Beside this, AKFI aims at improving the standard of the sport in the neighboring countries of India.

It also organizes international kabaddi tournaments for both men and women in India. Along with it sub-junior and junior nationals and zonal competitions are also organized to promote the game at the local level. Mr. Janardhan Singh Gehlot is the current AKFI President. He is also the president of the Asian Amateur Kabaddi Federation (AAKF) and the International Kabaddi Federation (IKF).

# Kabaddi – Tournaments

Many countries have their own organizing bodies and they conduct championships at national level to pick the best players who can represent their nation at the international level. Most of these international tournaments are conducted in Asian countries.

| TOURNAMENT | YEAR | WINNER |
|---|---|---|
| ASIAN GAMES | 1990, 1994, 1998, 2002, 2006, 2010, 2014 | INDIA |
| WORLD CUP | 2010, 2011, 2012, 2013, 2014 | INDIA |
| SAF GAMES | 2006, 2010 | INDIA |

## Pro Kabaddi League

Pro Kabaddi League (PKL) is a professional Kabaddi league of India. This tournament is played on the same format as that of Indian Premier League (IPL). The first edition of Pro Kabaddi League (PKL) started in 2014 with eight franchises. It consisted of players from all around the world. It is monitored by the Mr. Charu Sharma, Managing Director of Mashal Sports. This tournament is backed by the Amateur Kabaddi Federation of India (AKFI), Asian Kabaddi Federation (AKF) and International Kabaddi Federation (IKF).

# A HAND BOOK ON KABADDI

Date: 02-08-2019. Session: Morning.

Sports Department ( Kabaddi – Simple as Learning)

| Sr. No. | Name | Class | Sign |
|---|---|---|---|
| 1 | Shirsath Suraj Ashok | T.Y B.A. | |
| 2 | Shirsath Sidhharth Kailas | S.Y.B.A | |
| 3 | Dhangar Ankush Santosh | T.Y.B.A | |
| 4 | Khatik Sahil Jahar | T.Y.B.A | |
| 5 | Bakash Daga Koli | T.Y. BA | |
| 6 | Sonawane Akshay Vikram | T.Y.BA | |
| 7 | Ahire Rakesh mukesh | S.Y.B.A | |
| 8 | Baisane Aditya ishwar | S.Y.B.A. | |
| 9 | [illegible] | T.Y.BA | |
| 10 | [illegible] | T.Y.B.A | |
| 11 | hire Manoj | T.Y.B.A | |
| 12 | [illegible] | T.Y.B.A. | |
| 13 | Bhoi Ajay Bapu | S.Y.B.A | |
| 14 | Dhole Rohit dilip | S.Y.B.A | |
| 15 | Koli Chetan | T.Y.B.A | |
| 16 | Girase Ashwini | S.Y.B.A | |
| 17 | [illegible] | T.Y.B.A | |
| 18 | Koli Archana | S.Y.B.A | |
| 19 | [illegible] | T.Y.B.A | |
| 20 | Thorat Anil nandu | T.Y.B.A | |
| 21 | Koli Ganesh. | S.Y.B.A | |
| 22 | Wadile Radhika Parbat | F.Y.B.A. | |
| 23 | Shide Vijay Sanjay | F.Y.B.A | |
| 24 | Koli Lakhan | S.Y.B.A | |
| 25 | [illegible] | S.Y.B.A | |
| 26 | Savale Akshay | F.Y.B.A | |
| 27 | Savale Divya D. | F.Y.B.A | |
| 28 | [illegible] | S.Y.B.A | |
| 29 | Sonar Devyash. | F.Y.B.A | |
| 30 | Ishar Yogita | S.Y.B.A. | |

Principal
Late Annasaheb P.S.Wadile
Arts College, Thalner
Tal.Shirpur, Dist.Dhule

# Add on course – Cyber Security Threats and Prevention

Department of Defence and Strategic Studies
Faculty Name – Dr. G. J. Gavit
Session - Morning Date – 1/08/2021

## Attendance sheet

| Sr. No | Name of Students | Class | Signature |
|---|---|---|---|
| 1 | Baqul Rohil | T.Y.B.A | |
| 2 | Borasu tejaswini | S.Y.B.A | Borasu tejaswini |
| 3 | Bhangar Ankush | S.Y.B.A. | D.Ankush |
| 4 | Bhangar Dipak | F.Y.B.A. | D.Bhangar |
| 5 | Baisane Ashvani | T.Y.B.A | B.A.Y. |
| 6 | अहीरे पुष्पा | S.Y.B.A. | अहीरे पु. |
| 7 | बाग्डल दिपाली | S.Y.B.A | बो.दि. |
| 8 | Bhoi Mayur | T.Y.B.A | Bhoi |
| 9 | Patil Nikita | F.Y.B.A. | P.Nikita |
| 10 | Rajput Rupali | F.Y.B.A. | Rajput |
| 11 | वाघ नितीन प्रकाश | F.Y.B.A. | V.N.P. |
| 12 | कोळी ममता संतोष | S.Y.B.A. | koli.mamtas. |
| 13 | Chouk Lokesh G. | TYBA | C.L.G. |
| 14 | Patil Aarti sanjay | S.Y.B.A. | |
| 15 | शेख बाबुल | S.Y.B.A. | शेख बाबुल |
| 16 | वाडीले मिलींद | S.Y.B.A | V.Milind. |
| 17 | Chitte Sonal S. | TYBA | Chitte.S. |
| 18 | Koli Manisha V. | TYBA | KM.V. |
| 19 | Koli Anil S. | TYBA | Anil. |
| 20 | Koli Anil dada | F.Y.B.A. | koli A. |
| 21 | साई कविता | F.Y.B.A. | K.Bhoi |
| 22 | कोळी अपना | F.Y.B.A. | KO.Apana. |
| 23 | सोरे पंकज | F.Y.B.A. | पंकज सोरे. |
| 24 | Manore Sagar | TYBA | |
| 25 | Koli Vijay | F.Y.B.A. | Koli V. |
| 26 | Bhil Arjun | F.Y.B.A. | Bhil Arjun |
| 27 | Patil Swati | T.Y.B.A | Swati.P. |
| 28 | पावरा संजय | F.Y.B.A. | P.Sanjay |
| 29 | Patil Rajshri S. | TYBA | Raj... |
| 30 | वाडीले शितल | F.Y.B.A. | वा.शितल |

Principal
Late Annasaheb P.S.Wadile
Arts College, Thalner
Tal.Shirpur, Dist.Dhule