threatcop
Security Starts with People

CYBER JAAGROOKTA (AWARENESS) DIWAS

COMPREHENSIVE IMPLEMENTATION PLAN

Introduction

Owing to the rapid rate of digitization and a massive increase in the use of ICT (Information and Communication Technology) devices and networks, the state of cybersecurity in India has significantly destabilized over the last few years. The consistently increasing number of internet users in India has led to a significant rise in cybercrime as well. To decrease this swiftly rising rate of cybercrime in India, **the Ministry of Home Affairs (MHA) has launched the initiative of Cyber Jaagrookta (Awareness) Diwas**. So, read on to learn more about the what, who, and when and of this initiative.

What is Cyber Jaagrookta (Awareness) Diwas All About?

With a belief that generating sustained awareness among the public is the best way to prevent cybercrimes, **the MHA and RBI have requested all Indian states and union territories to observe Cyber Jaagrookta Diwas on the first Wednesday of every month**. Commenced from **April 2022 onwards**, all the concerned **organizations under the Ministry have been requested to prepare an Annual Action Plan** in this regard. This action plan should put special emphasis on equipping employees with the knowledge and skills needed to deal with cyber attacks.

Who Has to Observe Cyber Jaagrookta (Awareness) Diwas?

All the schools, colleges, universities, Panchayati Raj Institutions (PRIs), municipalities, offices, branches/sections, and Public Sector Undertakings (PSUs) under the ministry are requested to observe Cyber Jaagrookta (Awareness) Diwas every month.

When is Cyber Jaagrookta (Awareness) Diwas Celebrated?

All the concerned organizations and institutions under the ministry will celebrate Cyber Jaagrookta (Awareness) Diwas on the **first Wednesday of every month during the period of 11 am to 12 noon** (tentatively)

How is Cyber Jaagrookta (Awareness) Diwas Celebrated?

All the concerned organizations are requested to observe Cyber Jaagrookta (Awareness) Diwas by generating cybersecurity awareness through **seminars, workshops, quiz competitions, interactive sessions, case studies, creative sessions and best practices**. Conducted on the same day and time every month, these sessions should shed light on the basic protocols of cyber hygiene.

Why is Cyber Jaagrookta (Awareness) Diwas Necessary?

In India, cyber attacks on PSUs, critical infrastructure and other government organizations have increased on a significant scale:

01 A major Indian oil PSU suffered a cyber attack disrupting its operations in Assam and received **a ransom demand of ₹57 crores**

02 In 2021, a suspected **Pakistani group launched phishing attacks on India's Critical Infrastructure PSUs** from the telecom, power and finance sectors

03 CERT-In reported a total of **11.5 lakh and 12.1 lakh cybersecurity incidents during 2020 and 2021** (up to October) respectively
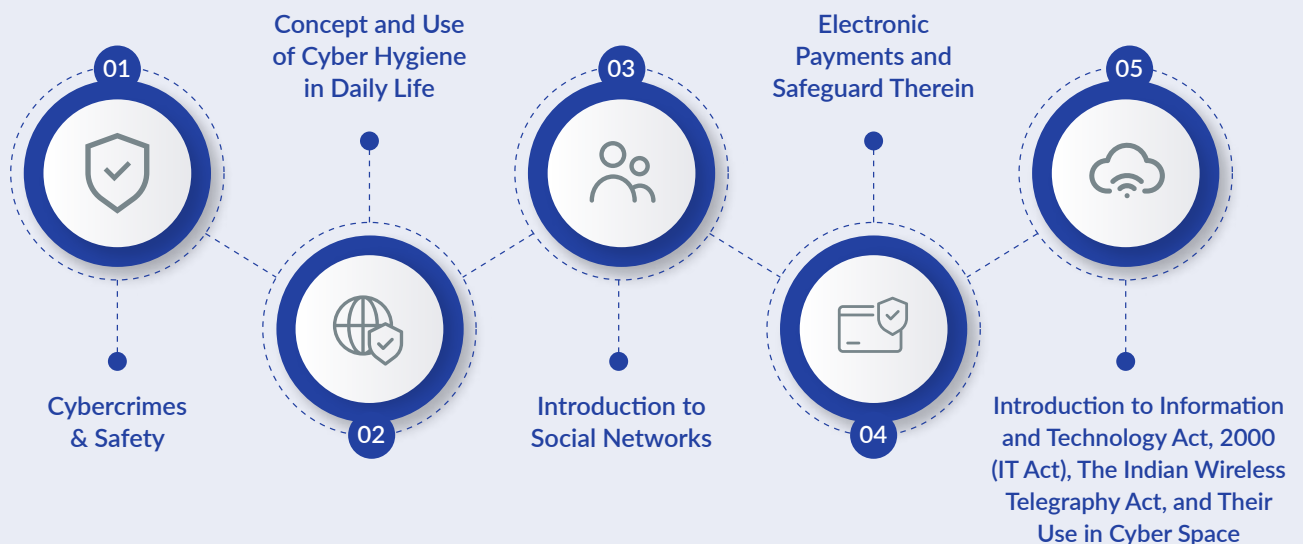
04 Of these, **54,314 and 32,736 incidents involved various government organizations** in 2020 and 2021 (up to October) respectively

Topics Covered under

Cyber Jaagrookta (Awareness) Diwas

The sessions conducted on Cyber Jaagrookta (Awareness) Diwas can cover a wide range of cybersecurity-related topics, which can be divided into five categories, as follows:

01

Cybercrimes & Safety

02

Concept and Use of Cyber Hygiene in Daily Life

03

Introduction to Social Networks

04

Electronic Payments and Safeguard Therein

05

Introduction to Information and Technology Act, 2000 (IT Act), The Indian Wireless Telegraphy Act, and Their Use in Cyber Space

The Internet Crime Report by the FBI revealed that India is ranked 3rd in the world among the top 20 countries being victimized by cyber crimes.
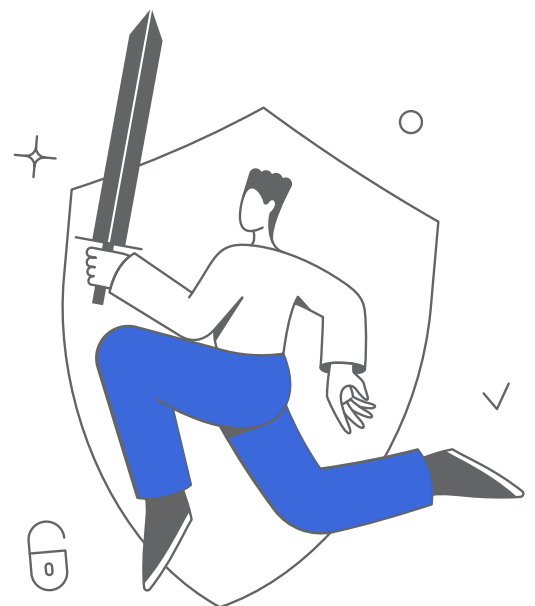
Cybercrimes & Safety

› Introduction to cybercrimes

› Kinds of cybercrimes: phishing, identify theft, cyber stalking, cyber obscenity, computer vandalism, ransomware, identity theft

› Spotting fake apps and fake news on social media and the internet (fake email messages, fake post, fake whatsapp messages, fake customer care/toll-free numbers, fake jobs)

› Internet ethics, internet addiction, ATM scams, online shopping threats, lottery emails/SMS, debit/credit card fraud, email security, mobile phone security

› Mobile apps security, USB storage device security

› Mobile connectivity security attacks (Bluetooth, Wi-Fi, Mobile as USB)

› Preventive measures to be taken in cyber space, reporting of cyber crime

› Forgery and fraud from mobile devices

› Cyber risk associated with varied online activities and protection therefrom

› Work on different digital platforms safely

› Online cybercrimes against women and impersonation scams

› Safety in online financial transactions
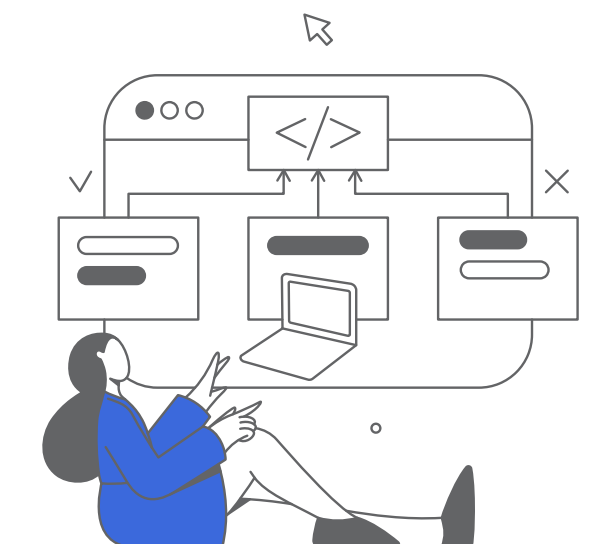
Security risks are reduced by 70% when businesses invest in cybersecurity awareness training!

- Pensar

🌐 Concept and Use of Cyber Hygiene in Daily Life

› Browser security, desktop security, UPI security, juice jacking, Google map security, OTP fraud

› IoT security, Wi-Fi security, spotting fake apps on social media and internet (fake email messages, fake post, fake whatsapp messages, fake customer care/toll free numbers, fake jobs)

› Internet ethics, internet addiction, ATM scams, online shopping threats, lottery emails/SMS, loan frauds

› How to avoid social engineering attacks, debit/credit card fraud, email security, mobile phone security, mobile apps security, USB storage device security, data security

› Mobile connectivity security attacks (Bluetooth, Wi-Fi), mobile as USB, broadband internet security

› Preventive measures to be taken in cyberspace, reporting of cyber crime

- -

👥 Introduction to Social Networks

› Social network and its contents like blogs

› Safe and proper use of social networks, inappropriate content on social networks

› Flagging and reporting of inappropriate content

- -

💳 Electronic Payments and Safeguard Therein

› Concept of e-payments, ATM and tele banking

› Immediate payment systems, Mobile money transfer and e-wallets

› Unified Payment Interface (UPI)

› Cybercrimes in electronic payments

› KYC: Concept, cases, and safeguards

Introduction to Information and Technology Act, 2000 (IT Act), The Indian Wireless Telegraphy Act, and Their Use in Cyber Space

› Concepts as defined in the IT Act and the Indian Wireless Telegraphy Act

› Communication devices

› Computer, cybersecurity, data security

› Secure systems

› Basic concepts of blockchain, 5G, IoT, Ai, drones, etc.

'Cyber Star' Recognition By The Ministries

Under this Cyber Jaagrookta (Awareness) Diwas initiative, the Ministry may acknowledge 5-10 employees every year who have made exceptional contributions in generating awareness against cybercrime at their own level. This will serve to motivate them and inspire their tireless efforts towards fostering a cyber-safe environment. The Ministries may also recognize sections/officials as "**Cyber Star**'' of the month.

ThreatCop LMS

ThreatCop is a security awareness training tool that comes with an integrated Learning Management System (LMS) to help your employees become cyber aware and empower them to defend themselves against social engineering attacks. Our **ThreatCop LMS consists of more than 2000 pieces of informative and interesting cybersecurity content** including newsletters, advisories, videos, posters, infographics and more.

With the help of our meticulously curated content, imparting security awareness and educating individuals to become significantly easier and more effective. Several big and small organizations around the world have employed ThreatCop LMS to generate cybersecurity awareness amongst their employees and improve the level of cyber hygiene in their workspace.
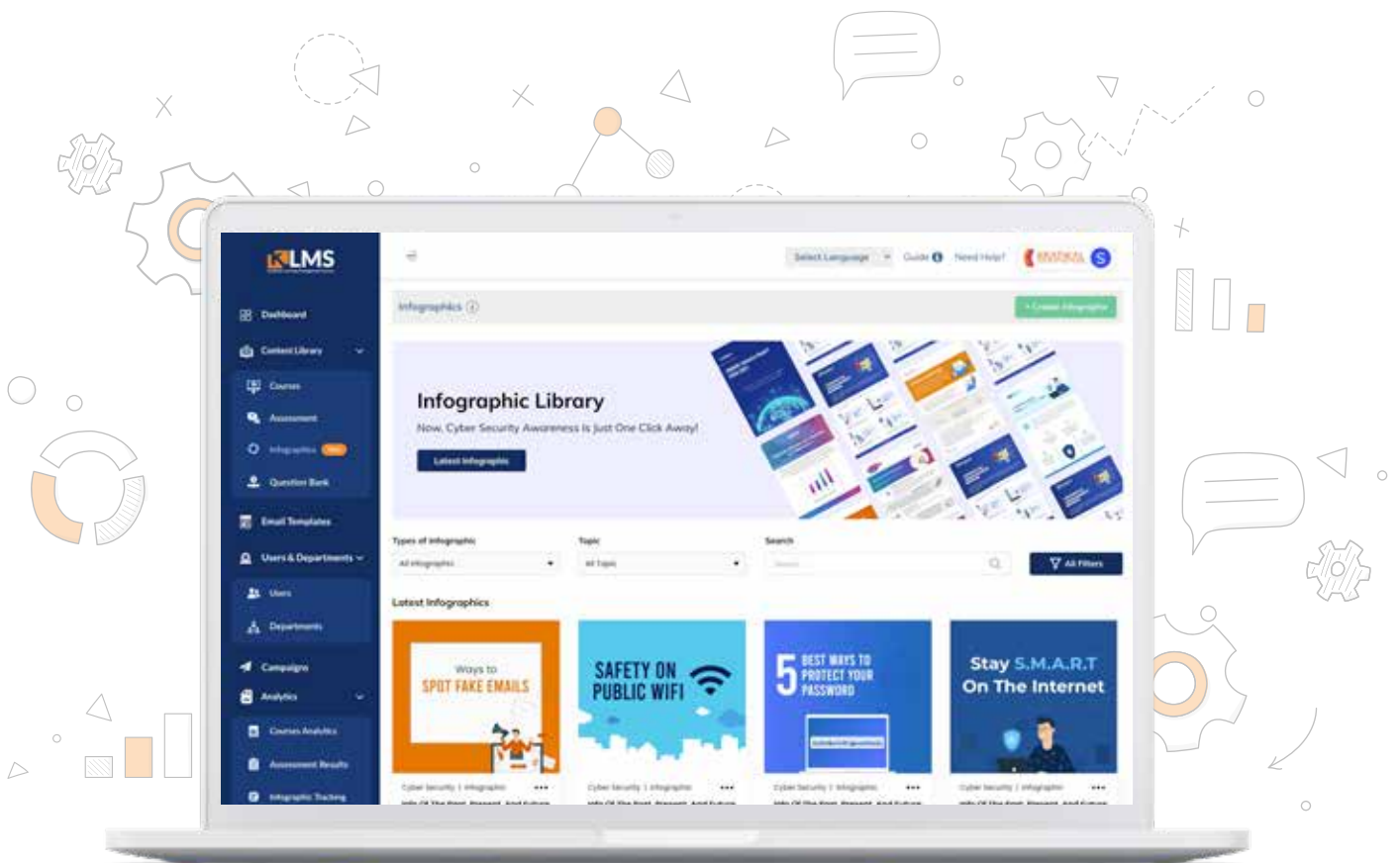
Wallpaper

Poster

Quiz

Video Training

Flyer

Sticker

How

How Exactly Can We help?

If you fall under the umbrella of the Ministry of Home Affairs, it's essential you understand everything there is to know about Cyber Jaagrookta (Awareness) Diwas. While the concept of spreading security awareness sounds simple and straightforward, creating and implementing an annual action plan (as directed by the MHA) can be a time-consuming and complicated process. Our ThreatCop LMS can help you streamline this process and comply with the guidelines issued by the government. Here's how!

Creation of Annual Action Plan

The Ministry of Home Affairs (MHA) has requested all the concerned organizations to come up with an Annual Action Plan for celebrating Cyber Jaagrookta Diwas on every first Wednesday of the month throughout the year. We will help you create a comprehensive and effective plan that will not only comply with the government guidelines but also gain your employees' attention and interest. Following is a basic prototype of the kind of Annual Action Plan we will prepare for you:

1st Wednesday (Every Month)	Category (As per the guidelines)	Category Name	Plan of Action on Suggested Units
1st Month	Category 1	Cyber Crimes and Safety	Video training + Quiz + Infographics + Stickers (Designs)
2nd Month	Category 2	Concept and Use of Cyber Hygiene in Daily Life	Case Study + Questionnaire + Wallpaper
3rd Month	Category 3	Introduction to Social Networks	Video training + Quiz + Screensaver
4th Month	Category 4	Electronic Payments and Safeguard Therein	Recorded Webinar + Quiz + Newsletter
5th Month	Category 3	Introduction to Information and Technology Act , 2000 (IT Act), The Indian Wireless Telegraphy Act, and Their Use in Cyber Space	Video Training + Quiz + Poster (Designs)
6th Month	Category 1	Cyber Crimes and Safety	Infographics + Quiz + 1st Simulation Attack
7th Month	Category 2	Concept and Use of Cyber Hygiene in Daily Life	Video training + Quiz + Screensaver
8th Month	Category 3	Introduction to Social Networks	Case Study + Questionnaire + Screensaver
9th Month	Category 4	Electronic Payments and Safeguard therein	Recorded Webinar + Quiz + Infographics
10th Month	Category 3	Introduction to Information and Technology Act , 2000 (IT Act), The Indian Wireless Telegraphy Act, and Their Use in Cyber Space	Video Training + Quiz + Newsletter
11th Month	Category 1	Cyber Crimes and Safety	Recorded Webinar + Poster (Designs)
12th Month	Category 2	Concept and Use of Cyber Hygiene in Daily Life	Gamified Assessment (ThreatCop Game) + Newsletter + 2nd Simulation Attack

Note:
The Annual Action plan will be customized according to the needs and environment of your organization to ensure smooth and hassle-free implementation.

Curation of Required Content

ThreatCop LMS will provide you with all the content pieces required to implement the decided-upon annual action plan. This includes everything from videos, infographics and posters to **quizzes, assessments, webinars and more**. The content will not only cover the topics suggested by the **MHA** but also be interesting enough to engage the audience. We'll make sure that you only receive the content relevant to your industry, domain and organizational structure.

Get in Touch
to Consult for Cyber Jaagrookta Diwas

Email us at sales@kratikal.com
Contact us at +91 9717792410, +91 8826990982

threatcop
Security Starts with People