CYBERSECURITY CENTRE of EXCELLENCE
A joint initiative of DSCI & Government of Telangana

DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

ADVISORY FOR LAW ENFORCEMENT AGENCIES

- by the Data Security Centre of India (DSCI) along with the Cybersecurity Centre of Excellence (CCoE), Hyderabad.

Table of Contents

Background

Amid the rapidly growing Coronavirus (COVID-19) pandemic, countries are facing multifaceted challenges ranging from executing all measures to break the COVID-19 chain, and contain the disease spread by enforcing lockdowns while delivering health and essential services to its citizens and flatten the curve.

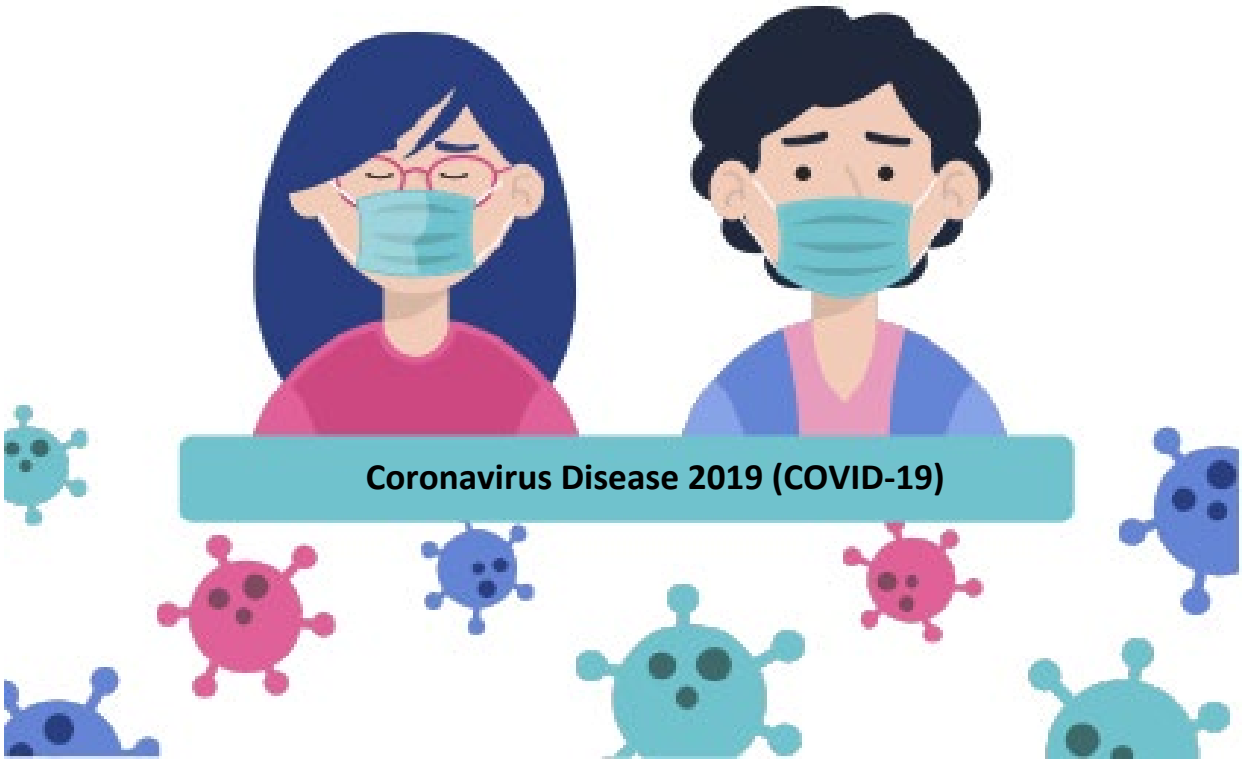
While we highly appreciate the efforts of our medical and healthcare professionals who are working at the forefront, putting their lives on line to save others; we deeply acknowledge the role of law enforcement agencies, who are standing beside them to administer social distancing and considerably mitigate the risks of further disease spread.

As Coronavirus is continuously causing widespread disruption, the Law Enforcement Agencies (LEAs) confront a major challenge of controlling the spread of the disease and maintain law & order whilst safeguarding their own health as they are more prone to get infected, working at the ground level.

As LEAs hold the first line of defense to ensure precautionary measures enforced by the Government, DSCI has prepared a detailed guide for Law Enforcement Agencies which consists of two parts. The first part is a consolidation of safety tips that will help minimize infection risks while ensuring the police remain safe on/off duty. The second part of the advisory focuses on Digital Forensics safety, ensuring Cyber Security best practices for LEA departments, and cybercrime awareness.

About COVID-19

- **Coronavirus disease 2019 (COVID-19)** is caus
- It is a respiratory illness that spreads fro started in China, but it has now spread all countries, including India.
- Cases reported indicate that the symptoms as 14 days after exposure to the virus that c **19).**
- As of now, there is no specific antiviral tr



DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

Basic Guidelines - Protecting Yourself from Exposure

- **Maintain a distance of at least 3 feet/1 meter**
- **Wash your hands with soap and water for at least 20 seconds**
- **Practise proper hand hygiene**
- **Do not touch your face, especially with unwashed hands**
- **If soap and water are not readily available and illicit drugs are NOT suspected to be present, use an alcohol-based hand sanitizer with at least 60% alcohol**
- **When possible, ensure only trained personnel wearing appropriate personal protective equipment (PPE) come in contact with COVID-19 suspected individuals**

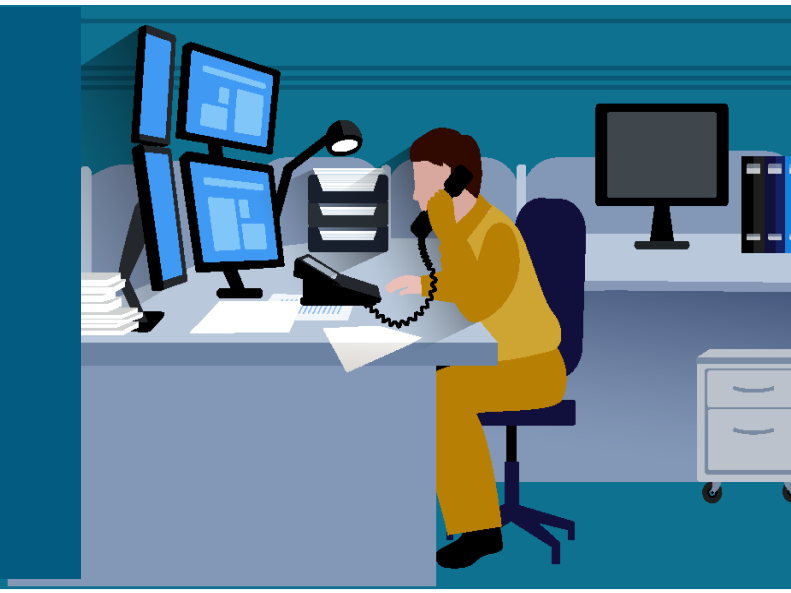
Recommended Personal Protective Equipment (PPE)

Remember Personal Protective Equipment (PPE) protects you and others only if you know how to use and dispose it properly. Therefore, impart caution and ensure to use provided PPE:

- Face Shield and goggles
- Wear masks, preferably triple layer medical mask or N-95 respirator mask
- Gloves
- Coveralls/Gowns when working in proximity of within 1 meter of suspect/confirmed COVID-19 cases or their secretions
- Head & Shoe covers

Dispose all contaminated PPE as per guidelines.

For more information: https://www.mohfw.gov.in/pdf/GuidelinesonrationaluseofPersonalProtectiveEquipment.pdf



Indoor areas including office spaces:

- Office spaces, including conference rooms should be cleaned every evening after office hours or early in the morning before the rooms are occupied
- If the contact surface is visibly dirty, it should be cleaned with soap and water prior to disinfection
- Prior to cleaning, the worker should wear disposable rubber boots, gloves (heavy duty), and a triple layer mask

Outdoor areas:

- Outdoor areas have less risk than indoor areas due to air currents and exposure to sunlight
- Cleaning and disinfection efforts should be targeted to frequently touched/contaminated surfaces

Toilet area:

- Sanitary workers must use a separate set of cleaning equipment for toilets (mops, nylon scrubber) and a separate set for sink and commode
- They should always wear disposable protective gloves while cleaning a toilet

For more information:
https://www.mohfw.gov.in/pdf/Guidelinesondisinfectionofcommonpublicplacesincludingoffices.pdf

Police while On/Off Duty

Police On-Duty:

- Avoid touching your eyes, nose and mouth with unwashed hands
- Avoid close contact with people who are sick
- Wash your hands with soap and water for at least 20 seconds or use a sanitizer with minimum 60% alcohol, if you must touch suspected individuals or objects
- Stay home if you are feeling sick
- Clean and disinfect frequently touched objects and surfaces

Police when leaving for Home:

- Sanitize Waist Belts/Whistle Chord/Stick/Cane/Cap and any other accessories from your uniform/equipment that's frequently touched
- Change your uniform at the end of shift while still at the station/office or immediately after returning home prior interacting with family members
- Visually practice good hygiene and isolation, thereby imparting model behaviour for children and elderly at home. Reinforce it as routine to help minimize children anxiety during isolation.

Police at Home:

- Identify a separate area to quarantine sick household members
- Limit close contact with others as much as possible
- Clean and disinfect frequently touched objects and surfaces in your home
- Avoid sharing your personal items with other family members

Police Vehicles:

- Duty driver should be made aware of basic hygiene protocol while on duty
- Sanitize the steering wheel, gear shift, door handles, ignition keys, etc. frequently
- Reduce the number of people in police vehicles
- Outdoor air should be allowed as much as possible for proper ventilation
- Air-conditioned vehicles should be run in non-recirculation mode
- Special care to be taken for isolation while transporting prisoners to jails

Dealing with COVID-19 Positive/Suspects

Close contact during Apprehension

- Exercise additional care while dealing with suspected/infected individuals by mandatorily wearing PPE
- Clean and disinfect Waist Belts/Whistle Chord/Stick/Cane/Cap and any other accessories from your uniform prior to reuse using a household cleaning spray or wipe
- Even though uniform may not appear contaminated, still follow standard operating procedures for containing and laundering clothes
- Follow standard operating procedures for containment and disposal of any used PPE

Dealing with Digital Assets

- The staff involved in taking over the digital assets (mobile phones, etc.) belonging to COVID-19 positive/suspects should ensure he/she doesn't touch anyone without proper precautions
- The forensic examiner at different state and central forensics laboratories/police investigation laboratories should mandatorily wear PPE while conducting any analysis
- The number of forensics analysts working in the laboratory must be reduced based on the actual requirement
- The devices subjected for examination must be sanitized
- The laboratory seating arrangement must be rearranged keeping in view the safe distance
- There should be an abundant supply of hand sanitizers, working gloves, masks, etc., in the laboratory
- Visitors (jurisdictional police officers, senior police officers & others) to the cyber forensic laboratory should mandatorily wear masks and use sanitizers
- Equipment at the cyber forensic lab must be disinfected frequently and the housekeeping staff involved should wear protective equipment

Police Leadership Decisions

Amid this crisis, Government, healthcare departments and key decision makers are continuously monitoring developments and amending plans such as lockdown extensions, changing the list of essential services, etc. to safeguard the public. Coordinate with national, state and local government agencies and clearly communicate with your staff about changing policies and procedures, and prepare staff on ground to implement required measures.

Also, train officers and external facing staff to be prepared with answering general queries such as travel restrictions, quarantine, isolation, personal safety measures and SOS facilities in case of an emergency. This will reduce panic in public and reassure faith on the fact that help is available.

Additionally, below points summarise few other important aspects to be followed:

- Encourage sick employees to take medical leave and stay at home
- Ensure adequate supply of Personal Protective Equipment to all ranks of police stations and other offices
- Impart training on proper wear, removal and disposal of PPE, along with its strict adoption as directed
- Avoid physical meetings, roll calls, briefing, etc. This can be done over call or using videoconferencing.
- Provision work from home for non-essential staff members, if feasible
- Encourage forming communication groups comprising of local health department, police officers and other emergency services at sub-divisional, divisional and zonal levels for seamless communication and quick response
- Designate Public Information Officers to disseminate public information in a timely manner
- Consider alternative staffing options like availing services of retired employees, volunteers, shared staffing from other government departments
- Reduce the number of suspects in police station lockups
- Ensure hospitals tied up under the government schemes attends the LEA staff without getting into detailed formalities
- Build LEA quarantine facility exclusively for police personnel at DCP office levels

Cybercrime & COVID-19

Cybercriminals are exploiting the current crisis by increasingly deploying a wide range of cyberattacks ranging from phishing attacks, unsolicited emails posing as advisories from government agencies, malware attached to mails, exploiting vulnerabilities in network devices, and to a greater extent, more sophisticated type of attacks such as ransomware.

While the corporate and business sector has been mainly targeted by cybercriminals, they might attack law enforcement establishments as well to disrupt law & order, and leak confidential police and criminal records. Therefore, it is important to ensure basic cyber security protocols for all staff who are at desk jobs and record keeping.

Cyber Security Best Practices for LEA Professionals

Secure your information

- Identify all critical information regarding your work and classify the information depending on its sensitivity
- Back up your files using a 3-2-1 backup rule; i.e., retain at least three separate copies of data on two different storage types, with at least one of those stored offline
- Reset all passwords for accessing emails, investigation case diaries and other administrative data. Avoid using common nomenclature for setting passwords, i.e., (first 3 characters of the unit + ABC + 1234).
- Enable continuous log monitoring and information access management
- Perform audits to check who all have administrative privileges to access computer systems and networks. Enforce strict policy to allow the least privilege to common users. Users should not be given administrative permissions unless it is absolutely necessary for carrying out their work.
- Check for any third-party access provided to police network to carry out any project, troubleshooting or implementing new solutions. Access may be disabled if it is not too critical at this time.
- Apply encryption wherever possible to ensure confidentiality and maintain the integrity of information

Training & Awareness

- Conduct security awareness training and educate your staff about ransomware attacks-short video/audio messages from the Police IT system admins may be circulated
- Train your staff to spot and report phishing emails containing malicious attachments and suspicious links
- Create train-the-trainer programs for expanding the awareness program

Software, Computer Systems & Network Security

- Employ a strong email filtering system to block spam and phishing emails
- Keep firewalls and antivirus fully operational and updated
- Identify computer systems still running on legacy operating systems like Windows XP for which there is no available support and isolate them from the network or upgrade
- Patch vulnerabilities and keep all your software updated
- Use complex passwords with strict password policy like 8 characters with a combination of alphanumeric and special characters (@#$%*)
- Enable multi-factor authentication on all user accounts
- Set up rigorous software restriction policies to block unauthorized programs from running at office systems
- Minimize the number of computer systems that are connected to public networks
- Provide restricted access to computer systems which store sensitive information
- Conduct periodic security assessments to identify security vulnerabilities of your website
- Revisit the physical security of restricted access rooms like police data centers and if required, enhance security

Cyber Security Breach Incident Handling

- Have a detailed contingency plan for handling any untoward cyber security breach incident. The plan should include the details of roles & responsibilities of individual staff members, action to be taken, reporting, etc.
- Documentation of procedures related to identification, collection acquisition and preservation of potential digital evidence during any cyber security breach incident should be very well documented
- Take help/guidance regarding handling of any such incident from the respective state/central special divisions like CERT-In, Cybercrime Police Station, Hi-Tech investigation cells, etc.

Common Cybercrime Scenarios

As cybercrimes are on the rise, criminals have come up with several innovative ways to con citizens. Several fake websites, portals and apps have mushroomed over the web promising medicines, treatment, factual information, donation links and dupe unsuspecting individuals of their money. The below mentioned scenarios would help the law enforcement agencies to be aware about the latest modus operandi adopted by cyber criminals. This information can also be used to warn the general public, companies and other organizations.

- Criminals pick up a topic that is contemporary and most discussed to craft phishing emails to steal credentials and financial account details. The number of 'spoofed' websites used for phishing to steal people's private credentials rose by 350% since January 2020. Emails and web links related to the pandemic are being sent claiming to be from health authorities, with the aim of tricking people into connecting to a specific webpage and login with their real email address and passwords. Scammers use the gathered information to access sensitive information and potentially use to steal their money.

  Recommendation: Phishing uses fraudulent email messages designed to impersonate a legitimate person or organization and trick the recipient into downloading malware laden attachments or reveal sensitive information, such as passwords, official data, bank account numbers, etc.

  Stay away from such attempts by closely checking the sender's address, never click on any suspicious email links and open attachments from unknown senders. Poor grammar, spelling mistakes and inconsistent formatting are other indicators to identify phishing emails.

- Fake COVID-19 mobile applications promising to notify the users as soon as any COVID-19 infected person comes in the vicinity.

  Recommendation: Never install any mobile application from untrusted sources.

- Criminals know that public institutions like hospitals, government organizations and all those engaged in COVID-19 rescue operations are soft targets since they are deeply involved in handling the current health emergency. They target those institutions through ransomware which can infect the computer system through malicious links or attachments, compromised credentials or through bugs in the system.

  Ransomware: Never click on any suspicious link. Ensure you have backed up all the critical data. Whenever there is a demand for ransom, reset the system with the most recent backup. Please remember: ***Paying ransom doesn't guarantee regaining access to data***

- ‘Work from Anywhere’ infrastructure is being heavily targeted along with attempts of identity theft and malicious payload delivery.

  Recommendation: Companies should set up VPN infrastructure and enable their employees to work from anywhere during the crisis

- Several fraudulent websites and e-commerce platforms have mushroomed on the Internet, promising to sell medicines that could either prevent or cure COVID-19, while some others are being fooled to transfer money in the name of delivering medical supplies.

  Recommendation: Stay away from such false claims as there is no treatment or vaccine available for Coronavirus until now. Care is being administered to relieve symptoms and manage pneumonia and respiratory failure by trained medical professionals at hospitals. Also, essentials services are open and running; purchase medicines from your local store or trusted online sellers only.

- State Bank of India (SBI) and the Press Information Bureau (PIB) have cautioned citizens of fake Unified Payments Interface (UPI) ID being circulated in the guise of PM CARES fund for fighting the coronavirus pandemic in the country.

  Recommendation: Always crosscheck all account details/UPI handles before making any donation at PM or CM relief funds. Ignore emails and messages with links urging for donations. Always initiate a donation from your end at official websites.

- Many instances of spreading misinformation in the form of false and unverified news regarding coronavirus on various Social Media platforms have come to the fore. Such posts can potentially lead to panic and terror among the common people.

  Recommendation: Stay away from false news or forwarded messages on Social Media. Always refer to mainstream media channels for news and check government approved sites such as https://www.mygov.in/covid-19 and https://www.mohfw.gov.in/ for Coronavirus related stats and updates.

DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

TOGETHER

WE SUPPORT YOU!

Data Security Council of India

3rd Floor, NASSCOM Campus, Plot No. 7-10, Sector 126,
Noida, UP -201303

dsci.connect
DSCI_Connect
www.dsci.in
dsci.connect
dscivideo
Data-Security-Council-of-India

#STOPCOVID-19