APRIL 2020

BUILDING RESILIENCE AGAINST CYBER ATTACKS DURING COVID-19 CRISIS

PREPARED BY:

NATIONAL CRITICAL INFORMATION INFRASTRUCTURE PROTECTION CENTRE

ADDRESS:

BLOCK III, OLD JNU CAMPUS, NEW DELHI-110067, INDIA

MISSION COVID-19

Mission

To identify Threat Actors active during COVID-19 outbreak all over the world. These include those who are targeting Critical Information Infrastructure of India.

Vision

Safe and Secure Cyber Space for Critical Information Infrastucture of India.

Values

Information collection, analysis and dissemination from & to all Stakeholders in time-bound manner.

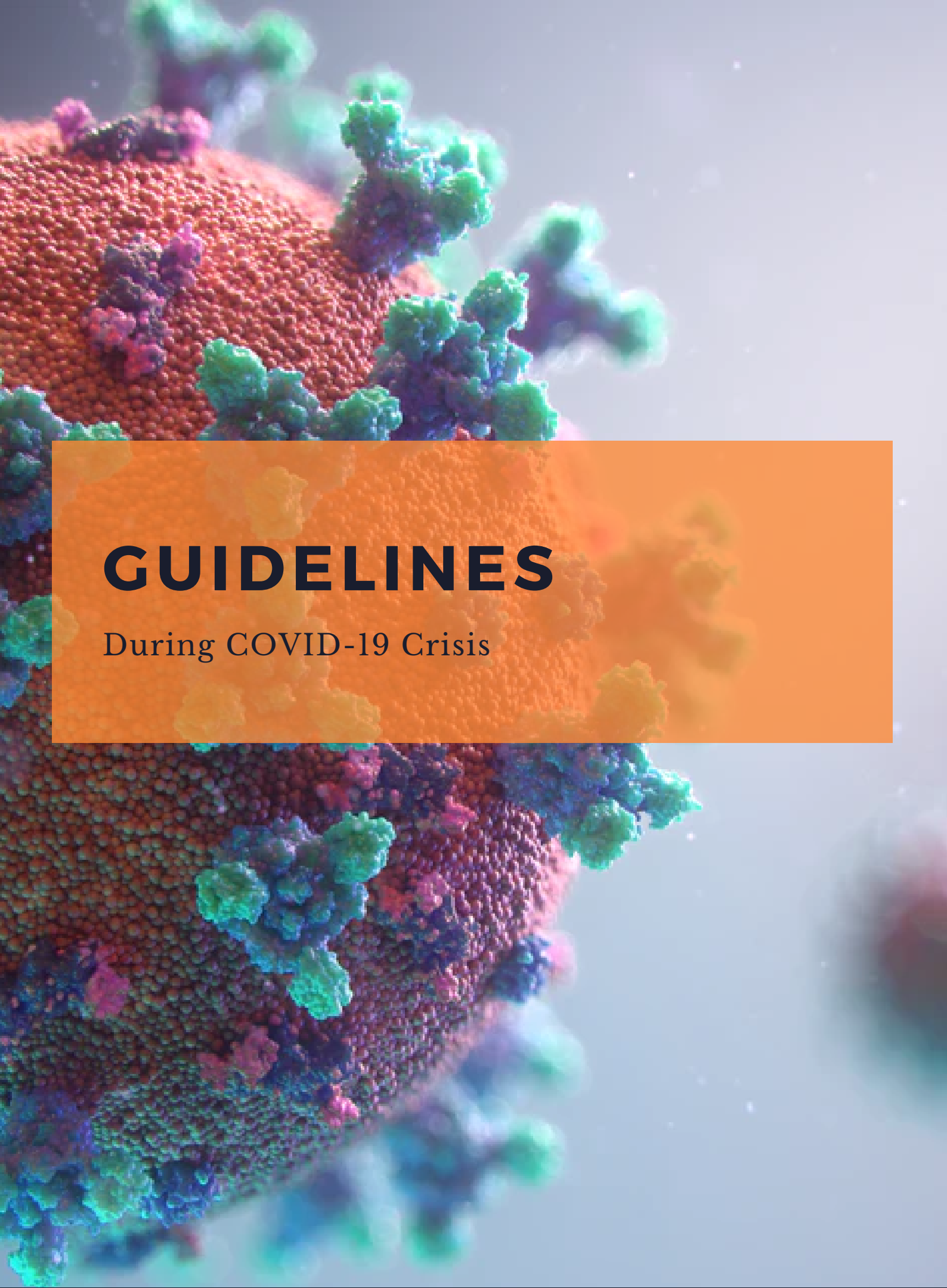
COVID-19 THREAT LANDSCAPE

Social Engineering

- Links to live tracking map and Mobile Apps
- Email attachments with malicious docs
- Donations for COVID-19
- IT fraud for credential harvesting (VISHING)
- Business Email Compromise / impersonation

Remote Access

- RDP and VPN credentials brute force
- SOHO Devices
- Invitation to fake VC/RAT application urls



GUIDELINES

During COVID-19 Crisis

purpose

To support IT & IS teams in protection of the organisation's critical assets and to get productivity from their remotely working staff/ employees and contractors.

GUIDANCE TO LEADERSHIP AND MANAGERS

Identify all business critical functions of the organisation/ critical e-governance and service delivery functions of the Govt, which have to be operational during the lock down. Choose only what is essential but everything that is essential.

Assess how these critical functions can be delivered by on-site and remote workers. What are the controls in place and how do these controls protect the applications and data from large scale cyber attacks on confidentiality, integrity and availability.

Carry out risk assessment – enable work vs cyber threats, business continuity and cyber crisis management plans. Focus on employee awareness training.

Ensure IT &IS Teams are not overwhelmed by urgent but low priority IT support calls from employees. IT & IS Teams should focus on Critical aspects of business operations and business continuity.

Organise remote working awareness training for employees, if not done already.

purpose

To protect the organisation's critical assets and enable employees and contractors to work remotely.

GUIDANCE FOR IT/IS TEAM

Allow remote access to the organization's internal network strictly with MFA and through proxy servers.

Apply application whitelisting, block unused ports, turn off unused services, monitor network traffic to prevent suspicious activities.

Apply least privilege controls to applications.

Security update/patches for all devices firmware/application.

Closely monitor privileged users/ administrators of critical accounts. Track all CRUD (Create-Read-Update-Delete) activities in Identity and Access Management (IdAM), AAA servers, NAC etc.

Backup of all configurations, networks, systems, databases, user identity and access data etc. Specifically focus on resilience of backups against ransomware attacks.

Check that all stakeholders are clear on Business Continuity and Cyber Crisis Management Plans and the actions they need to take if BCP or CCMP is activated.

MANAGE EMAIL PHISHING RISKS

Enforce Multi-factor Authentication (MFA) to access business email.

Configure Spoof Protection Controls : Ensure spoofing controls such as Sender Policy Framework (SPF), Domain-based Message Authentication, Reporting, and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) are fully configured for mail-enabled domains with hard fail and reject policies, where applicable.

Validate Email Security Gateway Implementation: Scan and sanitize all emails and attachments from malicious content and embedded URLs. Block certain file attachment types automatically (e.g., .scr, .exe, .chm, etc.) along with implement automated email warning reminders for external email.

Block Macros in Microsoft Office Documents. Validate Web Proxy or URL Filtering Configurations.

Implement Strong Password Policies, ensure sufficient logging and alterting mechanism in place. Develop and operationalize Phishing Incident Response Playbook.

purpose

Take responsibility to protect the organisation's assets

GUIDANCE TO EMPLOYEES

Identify and secure devices to be used for remote working with latest versions, patches and updates of Anti-virus/ anti-malware , OS and other application like MS Office/Libre Office suite/ web browsers/ Acrobat PDF Reader/ web conferencing utilities like Skype/ Webex/ Zoom etc.

Strong password protection, Firewall, Drive Encryption of the device to be enabled.

Do not share devices with other family members, specially children for the duration of remote working from home. If sharing is unavoidable, log off from your account and let them access through their own login account, which has no administrative privileges and cannot install applications.

Ensure that web browser protection feature is enabled and active. This will flag unknown and risky websites.

Secure the Home Router by changing the Admin and WiFi passwords and use strong wifi protocol.

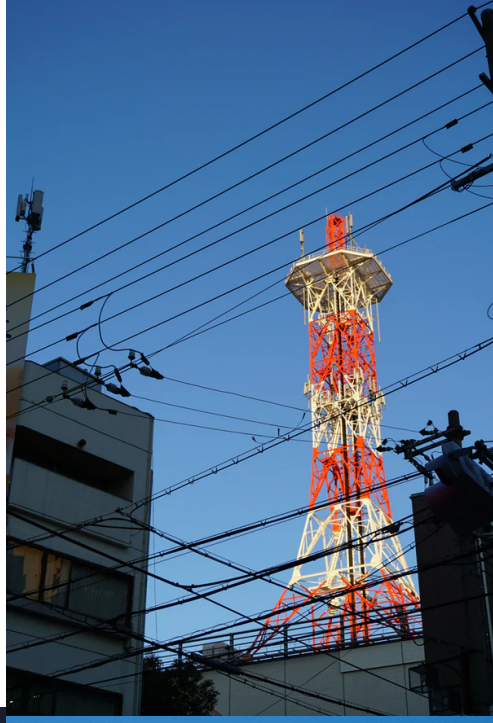
Actively participate in all employee awareness training programs and strictly follow the advisories and guidelines given by IT and IS teams.

TIME IS CRUCIAL

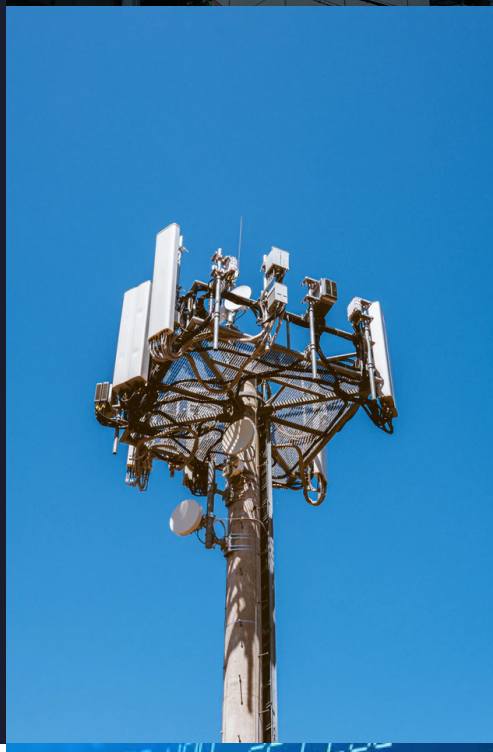
Situation is Ad-hoc but Learning is long term

Online Training and Awareness program is crucial for Employees and Management

Challenge is to support scaled up 'work-from-home' employees and access to Critical Informaiton in a Secure manner.



"Its our responsibility to protect Critical Information Infrastructure of India. We are prepared to defeat COVID-19 Cyber Threat together."



Best Practices

This document is intended to be shared with all NCIIPC Stakeholders to make them aware of ongoing Cyber Threats and Organisation Best Practices related to COVID-19 pandemic.

Feedback/Suggestions are welcome at helpdesk1@nciipc.gov.in