Online Training of Government Personnel of Union Ministries/ Departments in Cyber Security

Ministry of Electronics & IT (MeitY) is conducting following two types of Cyber Security training Courses for officers of Central Government Ministries/Departments:

  i. Generic Online Training in Cyber Security (Awareness training) of about 6-8 hrs duration for all the officers/staff of Government of India

  ii. Online Foundation Training (Advance Level) in Cyber Security for technically qualified or with requisite aptitude in cyber security / lT.

The first batches for both Generic as well as advanced online training have started on 2nd December 2020 and 7th December 2020 respectively. CDAC, Hyderabad is the implementing agency for both the training programmes. The whole progarmme for the training of government officials is proposed to be completed within next six months.

2.   The salient features of the Generic Online Training Course on Cyber Security (Basic Course) and the Online Foundation Course on Cyber Security (Advanced Level Course) are as under:

S. No.	Category	Generic Online Training Course on Cyber Security	Online Foundation Course on Cyber Security
		Basic training in cyber security	**Advanced training in cyber security**
1.	Objective	To sensitize a larger pool of Government personnel about the pitfall of cyber security related threats in IT/ICT environment and introduce cyber hygiene aspects	To harmonize the cyber security knowledge and skills amongst the identified personnel with 'technical aptitude' across the Ministries /Departments and equip them to acquire basic understanding of cyber risks, policies/ procedures/laws, enable protective measures such as scheduling security audits, facilitate incident reporting & escalation of issues, etc.
2.	Mode of Delivery	Keeping in view the current pandemic situation, it has been decided to use IT systems to deliver the programme in online mode through: • Webinars organized by experts on Cyber Security Awareness for Officers; Duration – 4 hrs. • Providing online awareness content on Cyber Hygiene for government officials for self-paced learning interspersed with quizzes, other awareness content, etc. of at least 2 hrs.duration. After completion of self-paced learning, the candidates have the	Keeping in view the current pandemic situation, it has been decided to use IT systems to deliver the programme in online mode through: • Virtual Instructor Led Training (VILT) through experts covering various topics of cyber security interspersed with case studies, assignments, hands-on using Virtual Training Environment (VTE)/ e-labs (duration 40 hrs.), etc. • The course has access to self-paced learning material of around 20 hrs. duration

S. No.		Generic Online Training Course on Cyber Security	Online Foundation Course on Cyber Security
	Category	**Basic training in cyber security**	**Advanced training in cyber security**
		option to appear for dynamic quiz(es) and get themselves certified.	• Entire course is completed in one week duration
3.	Broad Components (course structure)	• Information Security @ Organizational level, Cyber ethics and cyber offences • Data security, password security and email security • Mobile security, mobile app security and social engineering attacks • Social networking security and secured financial transactions	• Cyber Security basics for IT/ICT environment (10 Hours) • Information Security Policies, Procedures and Guidelines; (15 Hours) • System and Network security concepts; (20 Hours) • Information security audit and assessments including various cyber security threats, incident response(15 Hours)
4.	Target Audience	• For half day Webinar on Cyber Security Awareness - Around 100 personnel from each Ministry/Department • The on-line self-paced content on Cyber Hygiene is useful for Government officials at all levels.	• Around 10 personnel with technical aptitude from each Ministry/Department
5.	Eligibility Criteria	Government Employees who are actively using IT/ICT devices in personal as well as organizational context.	• Nominated personnel may preferably possess technical qualifications, such as B.Tech/B.E./M.Tech, M.Sc/ B.Sc/ Diploma/ Industry certificationsetc. or have an aptitude for technology. • They may have understanding of IT/ICT concepts like computer and network fundamentals, digital devices, hand-on experience in using IT/ICT tools and applications, etc.
6.	Delivery mechanism	• Targeted Webinars for up to a maximum of 1000 participants per webinar. • All the participants who attend the programme and who complete self-paced learning, etc. and thereafter clear the dynamic quiz are awarded a certificate.	• Training programme for around 10 participants from each Ministry/ Department; up to a maximum of 60 participants per batch. • All the participants who attend the programme regularly, submit assignment(s), complete hands-on exercises, etc are awarded with a certificate of participation. • After completion of training programme, all the participants

S. No.		Generic Online Training Course on Cyber Security	Online Foundation Course on Cyber Security
	Category	Basic training in cyber security	Advanced training in cyber security
			are provided with an access to an online remotely proctored assessment examination which is kept open for duration of say 2-months after the date of completion of training. All the candidates who are able to score more than 50% in this online examination are awarded with a certificate of completion. Further, the meritorious candidates are provided suitable avenues to pursue higher-level/ specialized training in cyber security through reputed institutions of higher learning like IISc, Bangalore, IITs, NITs, IIITs, etc. • For effective implementation of initiative of such a scale & scope, collaborative use of expertise & resources of MeitY & its organization viz. CERT-In, NIC, C-DAC, NIELIT, ERNET, STQC have been utilized.
7.	Expected Outcome	The participants get exposure on some of the common threats, which can emerge from phishing, misuse of passwords, financial frauds, use of social media, etc. and provided a general awareness on best practices to safeguard digital devices and manage security & privacy aspects (both, in the individual as well as the organizational context)	The Participants get an overview of the foundational aspects necessary to understand the cyber security posture of an organization.
8.	Value addition	• Access to supplementary awareness resources, blogs, relevant videos, multilingual content, etc. from time to time through email, Whatsapp groups, mobile app, etc. • The participants are provided with future handholding support through emails etc	• Access is provided to special talks by renowned experts in the area of cyber security from academia, industry, Seniorbureaucrats, etc • The trained personnel are provided with future handholding support.

3.   The initiative will create an ecosystem for capacity building/ training of Government personnel in cyber security and thereby provide support to formation of suitable structure with a

dedicated team in each Ministry/Department who would be able to support the respective CISOs in discharging their envisaged roles & responsibilities. It is also aiming to sensitize the larger set of Government officials at all levels about potential cyber related risks and measures to safeguard individual & organizational security & privacy.

4.   The initiative will empower individual Ministries/Departments to put in place requisite capabilities in the area of cyber security as well as create a homogeneous group well equipped to appreciate cyber security issues & challenges and also manage cyber threats and vulnerabilities through a MeitY supported system for training, re-training, up-skilling, etc.

******