

प्रधान महालेखाकार (लेखापरीक्षा - II) का कार्यालय, केरल, तिरुवनंतपुरम
OFFICE OF THE PRINCIPAL ACCOUNTANT GENERAL (AUDIT - II),
KERALA, THIRUVANANTHAPURAM

सं. लेप. II/प्रशा./I/निमलेप विविध/33-1/2022-23/

No. Au. II/Admn/I/CAG Misc/33-1/2022-23/

दि. 20.07.2022

परिपत्र/CIRCULAR NO.11

सीडैक, हैदराबाद द्वारा दि.22.07.2022 को सुबह 10.30 से दोपहर 12.30 तक और दो पहर 2.30 से शाम 4.30 तक साइबर सेक्यूरिटी बेसिक्स पर एक वेबिनार आयोजित किया जाएगा। वेबिनार का उद्देश्य आईटी/आईसीटी पर्यावरण में साइबर सुरक्षा संबंधी खतरों के नुकसान के संबंध में पदाधिकारियों को संवेदनशील बनाना और साइबर स्वच्छता पहलुओं का परिचय देना है।

कार्यक्रम में भाग लेने के लिए पदाधिकारियों को निम्न लिंक में दि. 21.07.2022 तक अपना पंजीकरण करवाना है।

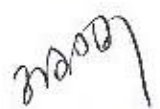
विस्तृत पाठ्यक्रम रूपरेखा एतद्वारा संलग्न किया जाता है। सभी पदाधिकारियों को वेबिनार में भाग लेने के लिए प्रोत्साहित किया जाता है।

A Webinar on Cyber Security Basics will be conducted by CDAC, Hyderabad on 22 July 2022 from 10.30 am to 12.30 pm and 2.30 pm to 4.30 pm. The Webinar is aimed at sensitizing the officials about the pitfalls of cyber security related threats in IT/ICT environment and introduction of cyber hygiene aspects.

In order to participate in the programme, the officials are required to get themselves registered at the following link by 21 July 2022.

<https://www.iseapmu.in/gct/>

Detailed course outline is attached herewith. All officials are encouraged to attend the Webinar.


वरिष्ठ लेखापरीक्षा अधिकारी / प्रशासन
Sr.Audit Officer/Admn.

सेवा में To

- 1 सूचनापट्ट / Notice Board
- 2 मुख्य कार्यालय के सभी अनुभाग / All Sections in Main office
- 3 शाखा कार्यालय, तृशर / Branch office, Thrissur

Generic Online Training Course on Cyber Security

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

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 Practices (<https://www.infosecawareness.in/cybhyg>) can be useful for Government officials at all levels register and access the course.

Eligibility criteria

- Government Employees who are actively using IT/ICT devices in personal as well as organizational context

Outcomes

- Participants will 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)

Duration: 6 hrs.

Mode of Delivery: Keeping in view the current pandemic situation, it is proposed 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 Practices 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 can appear for dynamic quiz(es) and get themselves certified.

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

Detailed course outline is given below:

Sl. No	Name of the Module
1.	Information Security @ Organizational level This module gives a brief overview of various threats and challenges an organisation can face and the importance of Awareness training for all employees about information security practices. <ul style="list-style-type: none">• Types of various threats• How organizational staff may be targeted• Methodologies and adware

	<ul style="list-style-type: none"> • Accepted use of behaviors towards Cyber Security • Organizational Intellectual properties and responsibilities • Securing information practices
2.	<p>Introduction to Internet fundamentals and Information security:</p> <p>This module gives an introduction to internet fundamentals and basic concepts of information security and its application. This module will help the learners to understand critical characteristics of information, importance of Information Security and Network security</p> <ul style="list-style-type: none"> • How internet works? And How internet is different from web? • Usage of internet and Privacy aspects of internet? • What is IP Address and what URL? • What is information security? • What are the information security threats? • Information security basic principles?
3.	<p>Password & Data security</p> <p>Considering that IT/ICT devices without proper security measures could lead to exploitation of system for illegal activities. This module gives a brief overview of various ways to securing digital devices used at home and office. Also it gives an insight to the importance of Password and data security, various measures to safeguard data and password, including safe ways of creating back up of important and sensitive data.</p> <ul style="list-style-type: none"> • What are Passwords? • What is the problem with passwords and how can passwords be cracked? • Passwords - Are they secure? • Why are passwords insecure, The solution - Two factor authentication • Multi factor Authentication - Challenges • What is Two Factor Authentication and what are the challenges associated with it?
4.	<p>Browser, email and Wi-Fi Security</p> <p>This module gives a synopsis of browsers, email and Wi-Fi security where the user can learn and understand types of browsers, its features. It also gives an in depth understanding on how to configure security settings of web browser, various risks involved while using browsers. It also gives an overview of the various types of cyber-attacks possible through email and Wi-Fi and how effectively one can recognize with the warning signs, the ways for checking the authenticity of emails and mitigation methods to safe guard from cyber attacks</p> <ul style="list-style-type: none"> • Why and how to Secure Web browser? • What is private/ incognito mode browsing? • What are the threats at browser level? • Guidelines for email Security? • What are the email threats and examples?
5.	<p>Social Engineering Techniques: Understanding Phishing, Vishing, Baiting, Smishing, etc.</p> <p>This Module will helps the learner to comprehend the various social engineering techniques like Phishing, Smishing and Vishing, Tools to identify Phishing websites, Tools to check the website is genuine or not, consequences, etc. It also gives an insight on recent reported scams.</p> <ul style="list-style-type: none"> • What are various social engineering attacks? • What is phishing, Vishing and Smishing? • How can we recognize social engineering attacks with examples? • What is Spear phishing and whaling?

	<ul style="list-style-type: none"> • Security measures against the social engineering methods? • Warning signs of the attacks?
6.	<p>Mobile and Mobile apps Security</p> <p>This module gives an overview measures for securing mobile and Apps that are used in daily life. It will impart learning about Mobile OS and Anti-virus, How your phone can be hacked, App downloads, permission and Privacy settings, and Mitigation methods to ensure security while using mobiles and Apps.</p> <ul style="list-style-type: none"> • Need for Mobile Security • Challenges of mobile security • Knowing the major security threats and mitigation • Know the permission given to the apps downloaded
7.	<p>Social Networking Security</p> <p>This Module gives the learner an understanding of basics of security measures while enjoying the benefits of social networking. This module covers, Social Networking and its types, Risks and challenges while using social networking including instant messaging. An insight to the security settings to be enabled while using the social networking sites to protect your identity and also on What to do and whom to contact when we are victims of Social Networking.</p> <ul style="list-style-type: none"> • What is social Networking? • What is difference between social media and social networking? • Advantages of social networking? • What are types of Social Networking? • What are risks and challenges? • What is the impact and effects of Social Networking? • Security measures for various social networking tools? • What are the various social networking threats and Security measures? • Social networking cases studies
8.	<p>Secured financial Transactions</p> <p>This Module gives an understanding about Online Banking, UPI Transactions, QR Code and online shopping. This gives and in depth knowledge on the security measures to be followed and the reporting mechanism to be known if you lose your money through online scams.</p> <ul style="list-style-type: none"> • What are digital Transactions? • What are the types of digital Transactions? • OTP Threats • Safety measures during online Transactions?

Self-paced learning, e-learning, other awareness content, etc.: Participants upon completing the course are encouraged to attend self-paced e-learning modules through an offline/e-learning mode to go through the concepts covered in Cyber Security Awareness Webinar. The e-learning courses contains modules on (a) Internet Fundamentals (b) Information Security (c) Computer Ethics (d) Cyber Crimes (e) Browser Security (f) Email Security (g) Social Networking (h) Social Engineering (i) Online Threats (J) Desktop Security (K) Mobile Security . All modules comprises of lecture notes, study material, related awareness videos, YouTube links, extra web resources, video lectures and quiz for each module.

After completion of self-paced learning, the candidates can appear for dynamic quiz(es) and get themselves certified.

Process for delivery of Generic Online Training Course on Cyber Security

Registration:

- All the participants would need to register @ www.isea.gov.in/get for attending the Generic Online Training Course on Cyber Security
- Registration will be accepted up to 1 pm, prior to the day of start of the programme
- Link for joining the session will be shared one day before the scheduled training programme, as per the details indicated during the registration
- Participants are requested to install CISCO WebEx Meeting prior to the session for better experience (<https://www.webex.com/downloads.html>)
- Participants can raise their queries in the chat box / Q&A section of the WebEx platform
- Resource person will address all the queries raised by the participants at end of the each session