Cybersecurity Workshop in Uttar Pradesh | Uttar Pradesh | 14 Nov 2024

Why in News?

Recently, the National e-Governance Division (NeGD) of Ministry of Electronics and IT (MeitY) in collaboration with the Government of Uttar Pradesh, organised a two-day Cybersecurity Workshop in Lucknow.

Key Points

- **Cybersecurity Training Program by NeGD:**
  - NeGD's Cybersecurity Training Program, part of the **State Capacity Building Scheme,** is designed to strengthen cybersecurity resilience among state government officials.
  - The program equips **Chief Information Security Officers (CISOs) a**nd Deputy CISOs with critical skills to handle and mitigate cyber risks effectively.
    - The NeGD was **established in 2009** by the **Ministry of Electronics & Information Technolog**y as an Independent Business Division under the Digital India Corporation.
    - Its aim was to **facilitate and catalyze the implementation of the Digital India Program** across Ministries and State Governments.
  - **Objective:**
    - **Cybersecurity Awareness:** Increase understanding of cybersecurity issues, cyber threats, and e-governance frameworks.
    - **Cyber Resilience and Artificial Intelligence (AI):** Enhance participants' knowledge of the **Cyber Resilience Ecosystem** and the role of AI in cybersecurity.
    - **Cyber Suraksha Kendra**: Educate on the importance of Cyber Suraksha Kendra for protecting state-level **e-governance** systems.
    - **Data and Application Security:** Provide insights into data protection (Digital Personal Data Protection Act, 2023) application security, and endpoint security.
    - **Crisis Managemen**t: Train participants in developing Cyber Crisis Management Plans (CCMP) for effective incident response.
    - **Identity and Access Management:** Address challenges in identity and access management to secure government digital systems.
- **State Capacity-Building Scheme:**
  - NeGD, under MeitY, has **launched a series of capacity-building workshops** for state leaders, CISOs, and officials across the nation.
  - These workshops provide **practical training and best practices for managing cyber threats,** adopting secure IT frameworks, and strengthening digital governance.
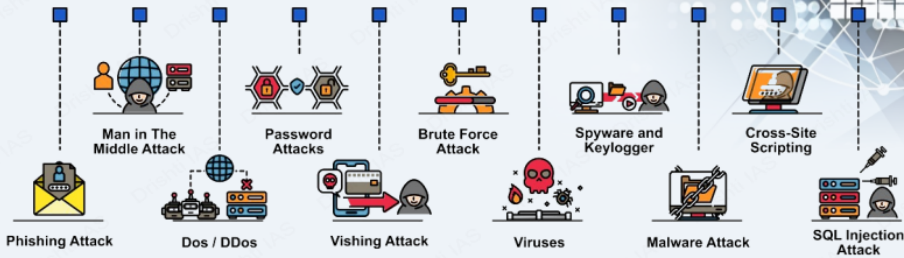
Digital Personal Data Protection Act, 2023

- It aims to **protect the digital personal data of individuals in India** and regulate the collection, storage, processing, and sharing of such data.
- **Key features**:
  - Establishes a **Data Protection Board of India** to enforce compliance.
  - Requires **explicit consent** for data collection and processing.
  - **Mandates data fiduciaries** to implement reasonable security safeguards.

CYBER SECURITY

Cybersecurity refers to any technology, measure, or practice for preventing cyberattacks or mitigating their impact.

CYBER SECURITY ATTACKS

- Man in The Middle Attack
- Password Attacks
- Brute Force Attack
- Spyware and Keylogger
- Cross-Site Scripting
- Phishing Attack
- Dos / DDos
- Vishing Attack
- Viruses
- Malware Attack
- SQL Injection Attack

'Crime in India' Report 2022 (NCRB) highlighted 24.4% surge in cybercrimes in India since 2021.

Common Cybersecurity Myths

- Strong passwords alone are adequate protection
- Major cybersecurity risks are well-known
- All cyberattack vectors are contained
- Cybercriminals don't attack small businesses

Cyber Warfare

- Digital attacks to disrupt vital computer systems, to inflict damage, death, and destruction.

CYBER THREAT ACTORS

CYBER THREAT ACTOR	MOTIVATION
NATION-STATES	GEOPOLITICAL
CYBERCRIMINALS	PROFIT
HACKTIVISTS	IDEOLOGICAL
TERRORIST GROUPS	IDEOLOGICAL VIOLENCE
THRILL-SEEKERS	SATISFACTION
INSIDER THREATS	DISCONTENT

Types of Cybersecurity

- Critical infrastructure security (Robust access controls)
- Network security (Deploying firewalls)
- Application security (Code reviews)
- Cloud Security (Tokenization)
- Information security (Data masking)

Recent Major Cyber Attacks

- WannaCry Ransomware Attack (2017)
- Cambridge Analytica Data Breach (2018)
- Financial data of 9M+ cardholders, including SBI, leaked (2022)

Regulations & Initiatives

- **International:**
  - UN Group of Governmental Experts (GGE) on Advancing Responsible State Behaviour in Cyberspace
  - NATO's Cooperative Cyber Defense Centre of Excellence (CCDCOE)
  - Budapest Convention on Cybercrime, 2001 (India not a signatory)
- **India:**
  - IT Act, 2000 (Sections 43, 66, 66B, 66C, 66D)
  - National Cyber Security Policy, 2013
  - National Cyber Security Strategy 2020
  - Cyber Surakshit Bharat Initiative
  - Indian Cyber Crime Coordination Centre (I4C)
  - Computer Emergency Response Team-India (CERT-In)

Steps Needed for Cyber Security

- Network Security
- Malware Protection
- Incident Management
- User Education and Awareness
- Secure Configuration
- Managing User Privileges
- Information Risk Management Regime

Drishti IAS

PDF Refernece URL: https://www.drishtiias.com/statepcs/15-11-2024/uttar-pradesh/print