India top fifth sextortion countries

Part of: GS-III- Internal security Cyber crime (PT-MAINS-PERSONALITY TEST)

As per a report by SophosLab, India is among the top 10 countries from where the sextortion spam emails originate. Researchers from the British cybersecurity firm Sophos traced the origin of millions of sextortion spam emails sent between September 2019 and February 2020 to conclude that India is among the top 10 sextortion mail source countries.

Being the source of 3.73 per cent of all sextortion emails, India is placed at fifth position preceded by Vietnam at the top (7.01 per cent), Brazil at second (5.89 per cent), Argentina at third (4.76 per cent), and Korea at fourth (4.76 per cent).

What is sextortion?

Sextortion is a widely used form of spam attack where cybercriminals extort money by claiming to have receiver’s compromising pictures or evidence of their sexual activity. The attacker threatens to share such pieces of evidence with the receiver’s friends and family unless they pay ransom money.

Sextortion email is not different from any other phishing. It’s more of a subcategory of ransomware emails. It includes malware that can hack the system upon accepting or activating the link.

The National Cyber Security Policy (NCSP) 2013 is a policy framework by the Department of Information Technology (DeitY) under the Ministry of Communications and Information Technology (MoCIT). It underscores the need for the creation of a secure computing environment and generating adequate trust in online systems and networks.

National Cyber Security Policy 2013 Objectives

- To create a secure cyber ecosystem and build adequate confidence in IT systems and transactions.
- To strengthen the regulatory framework for ensuring secure cyber ecosystem.
- To create and enhance mechanisms for monitoring and resolving cyber security threats.
- To enhance the protection and resilience of the nation’s critical information infrastructure.
- To create a workforce of five lakh specialists in cyber security over the next five years.

Key Highlights of National Cyber Security Policy 2013

- To meet with the various objectives of the cyber security policy, here are the strategy that will be put in place.
- Policy aims at creating a national level nodal agency that will co-ordinate all matters related to cyber security in the country.
- It will encourage organizations to develop their own security policies as per international best practices.
- The policy will ensure that all organizations earmark a specific budget to implement their security initiatives.
- Policy plans to offer various schemes and incentives to ensure that proactive actions are taken for security compliance.
- To create an assurance framework, policy will create conformity assessment and certification.
cyber security best practices, standards and guidelines

- Policy aims at encouraging open standards that facilitate interoperability and data exchange among IT products and services.
- A legal framework will be created to address cyber security challenges arising out of technological developments in cyber space.
- The policy also plans to enforce a periodic audit and evaluation of adequacy and effectiveness of Information infrastructure in India. The policy will create mechanisms to get early warnings in case of security threats, vulnerability management and response to the security threats thereof.

A 24X7 operational national level computer emergency response team (CERT-in) will function as an umbrella organization that will handle all communication and coordination in dealing with cyber crisis situations.

- To secure e-governance services, policy will take various steps like encouraging wider usage of Public Key Infrastructure (PKI) standards in communications and engagement of expert security professionals to assist in e-governance.
- The policy will encourage and mandate use of tested, validated and certified IT products in all areas.
- The policy also plans to undertake and invest in various R&D programs in areas of national cyber security.