GOVERNMENT OF INDIA

MINISTRY OF INFORMATION AND BROADCASTING

LOK SABHA

UNSTARRED QUESTION NO. 5508

(TO BE ANSWERED ON 05.04.2022)

HACKING OF WEBSITES

5508 Shri A. RAJA:

Will the Minister of INFORMATION AND BROADCASTING be pleased to state:

a) The details of the hacking of Twitter/e-mail/ Government websites pertaining to Government accounts and Government offices also including VVIPs/VIPs during the last five years;

b) The details of action taken so far in each case; and

c) The steps being taken by the Government to protect such websites and prevent from hacking in future?

ANSWER

THE MINISTER OF INFORMATION AND BROADCASTING; AND MINISTER OF YOUTH AFFAIRS & SPORTS
[SHRI ANURAG SINGH THAKUR]

(a) & (b): As per the information received from Ministry of Electronics And Information Technology (MeitY), Indian Computer Emergency Response Team (CERT-In), reported to and tracked a total number of 175, 114, 61, 77, 186 and 28 Twitter/e-mail/ Government websites pertaining to Government accounts and Government offices which were hacked during the year 2017, 2018, 2019, 2020, 2021 and 2022 (upto February) respectively.

On observing compromise of websites/email/Twitter accounts, CERT-In notifies the affected entities along with remedial actions to be taken. CERT-In coordinates incident response measures with affected entities, service providers, sectoral Computer Security Incident Response Teams (CSIRTs) as well as Law Enforcement Agencies.

(c): The Government has interalia taken following measures to enhance the cyber security posture and prevent cyber-attacks:-

i. **Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis to ensure safe usage of digital technologies. CERT-In has issued 68 advisories for organizations and users for data security and mitigating fraudulent activities.**

ii. **Security tips have been published for users to secure their Desktops, mobile/smart phones and preventing phishing attacks.**

iii. **CERT-In is operating an automated cyber threat exchange platform for proactively collecting, analyzing and sharing tailored alerts with organizations across sectors for proactive threat mitigation actions by them.**

iv. **CERT-In has formulated a Cyber Crisis Management Plan for countering cyber attacks and cyber terrorism for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors.**

v. **All the government websites and applications are audited with respect to cyber security prior to their hosting. The auditing of the websites and applications is conducted on a regular basis after hosting also.**

vi. **CSD, MeitY conducts deep dive training on cyber security for Chief Information Security Officers (CISOs) and frontline IT officials from Central/State Governments, Public Sector Undertakings (PSUs), PSU Banks and Government organisations in collaboration with industry consortium in Public Private Partnership (PPP) mode to enable them to deal with challenges of cyber security.**

vii. **CERT-In has set up the National Cyber Coordination Centre (NCCC) to generate necessary situational awareness of existing and potential cyber security threats. Phase-I of NCCC is operational.**

****