

INDIA LAUNCHES

CYBER

SWACHHTA KENDRA

WHY IN NEWS

Minister of Electronics and Information Technology (MeitY) launched Cyber Swachhta Kendra- Botnet Cleaning and Malware Analysis Centre for analysis of malware and botnets that affect networks and systems

ABOUT CYBER SWACHHTA KENDRA



Part of Digital India initiative under MeitY

Notify, enable cleaning and secure systems of end-users



Will work in coordination with the internet service providers (ISPs)

Will enhance awareness regarding botnet and malware infection along with measures to be taken to secure their devices



Systems will be scanned by the Computer Emergency Response Team (CERT-in) for free for users who register to the CSK website

NEED

Will promote start-ups in cyber-attack security



India is promoting Digital India, Go cashless campaign

There are half a billion people online, over 250 million smartphones, one billion mobile phones in the country



Cyber crime cases in the country registered under the IT Act surged nearly 300 percent between 2011 and 2014

ANNOUNCEMENTS AT THE LAUNCH OF CYBER SWACHHTA KENDRA



The National Cyber Coordination Centre to be operational by June 2017



Sectoral CERTs to be created, that would operate under CERT-In. CERTs are to be set up in the state level as well



Empower designated Forensic Labs to work as the certified authority to establish cyber-crime



10 more STQC (Standardisation Testing and Quality Certification) Testing Facilities to be set up. Testing fee for any start-up that comes up with a digital technology in the quest of cyber security, to be reduced by 50%

REASONS FOR INCREASING CYBER ATTACKS



Increased Penetration whereas awareness about the security features is inadequate



Borderless: The cyber world has no barriers of geography

India uses cheap smartphone which have low security features



Lack of coordination among agencies and departments involved in cyber space like CERT-In, NTRG, etc.



No national security architecture that can assess the nature of cyber threats and respond effectively



Local police is unaware of various provisions of IT Act, 2000 and also of IPC related to cyber crimes



lack of IT skilled manpower



BOTNET



Is a network of computers infected with malware without the user's knowledge and controlled by cybercriminals. They're typically used to send spam emails, transmit viruses and engage in other acts of cybercrime.

MALWARE



"Malware" is short for "malicious software" - computer programs designed to infiltrate and damage computers without the users consent.

TOOLS PROVIDED FOR FREE UNDER CSK ARE

AppSamvid: This is a whitelisting tool for the desktop



M Kavach: Special anti-virus tool for smart phones and tablets



Browser JSGuard: It helps to block malicious Java Script and HTML files while browsing the web



Free Bot Removal Tool: It's a Quick Heal partner tool



USB Pratirodh: It is a USB protector to help clean various external storage devices like USB(s), memory cards, external hard disks, etc



WHAT COULD BE DONE?



Implement measures suggested by National Cyber Security 2013

Immediate focus on increasing the trained workforce to manage the cyber security issues



India should build its own offensive team like China



R&D in cyber security in order to innovate technologies



Institutional measures such as setting up Indian Cyber Crime Coordination Centre, National Cyber Security Agency that can coordinate with various agencies



Concept of air gapping which isolate the critical infrastructures from the internet should be used



India can follow Tallinn Manual which is an academic work related to laws that apply to cyber-crimes which developed nations such as USA are following



coordination among all the stake holders vis-a-vis corporates, government, NGOs, etc. Recently Ground Zero Summit held to discuss the challenges in cyber security



India should persuade at global forum for depleting the use of cyber weapons similar to that of NSG

