

● CYBER FRONTIERS

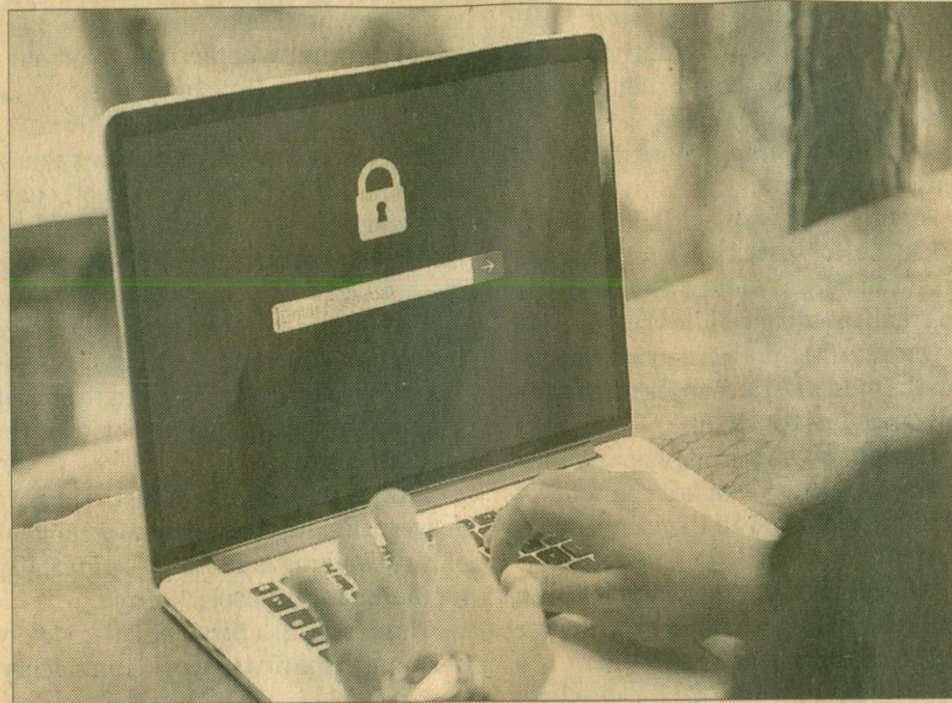
In pursuit of a safe cyberspace

NIC-CERT centre to prevent and predict cyber attacks on government utilities

SUDHIR CHOWDHARY

YOU ARE CONSTANTLY connected to the internet—chatting, checking emails, shopping, banking, using mobile wallets or updating your social media profile. But do you know that each time you go online, your computer or mobile device could be putting you and your personal information at risk. Even government agencies collect and hold massive amounts of personally identifiable information, creating valuable targets for cyber crime.

“As internet with its ever-expanding canvas of opportunities is touching the lives of people, it necessitates the requirement to up-scale the existing security infrastructure,” Ravi Shankar Prasad, minister of law & justice and electronics & IT, said while inaugurating the “NIC-CERT”, a set-up of National Informatics Centre, in New Delhi.



As part of its Digital India initiatives, the government has introduced many of its services online. Although this has made services very accessible to the citizens, it has also exposed them to the threats and vulnerabilities which are an inherent part of cyberspace, the minister said. He mentioned that in the re-

cent past, there has been an exponential growth in cyber attacks leading to concerns of data theft which led to the government drafting the Data Protection Act.

“NIC has been doing a remarkable job of securing the government cyberspace for a long time and by setting up the NIC-CERT,

they have taken their experience and expertise to the next level,” Prasad said. He emphasised that for responding to the cyber attacks of today, the government needs an agile and responsive ecosystem.

NIC-CERT has been set up with the objective of creating a comprehensive framework that integrates world-class security components and inbuilt threat intelligence for detection, prevention and incident response. Using the tools, the team will correlate events that would help in generating a canvas of the attack surface and identify the vulnerabilities and possible exploits. The gathered intelligence assimilated with the knowledge of the open web would give CERT the ability to prevent and predict attacks.

NIC's pan-India connectivity and reach is one of its key strengths, and this, coupled with its enhanced ability to detect and prevent attacks would collectively upscale the government's ability to protect its data. Setting up NIC-CERT, as per the minister, is MeitY's initiative under Digital India aimed at enhancing the security posture of NIC and the government, which will in turn lead to enhanced trust of the citizens as the services offered to them would be configured in a framework that is secure by design.

NIC-CERT will operate in close coordination and collaboration with sectoral CERT's and more so with Cert-in, the nodal agency with MeitY to deal with cyber security threats like hacking and phishing.