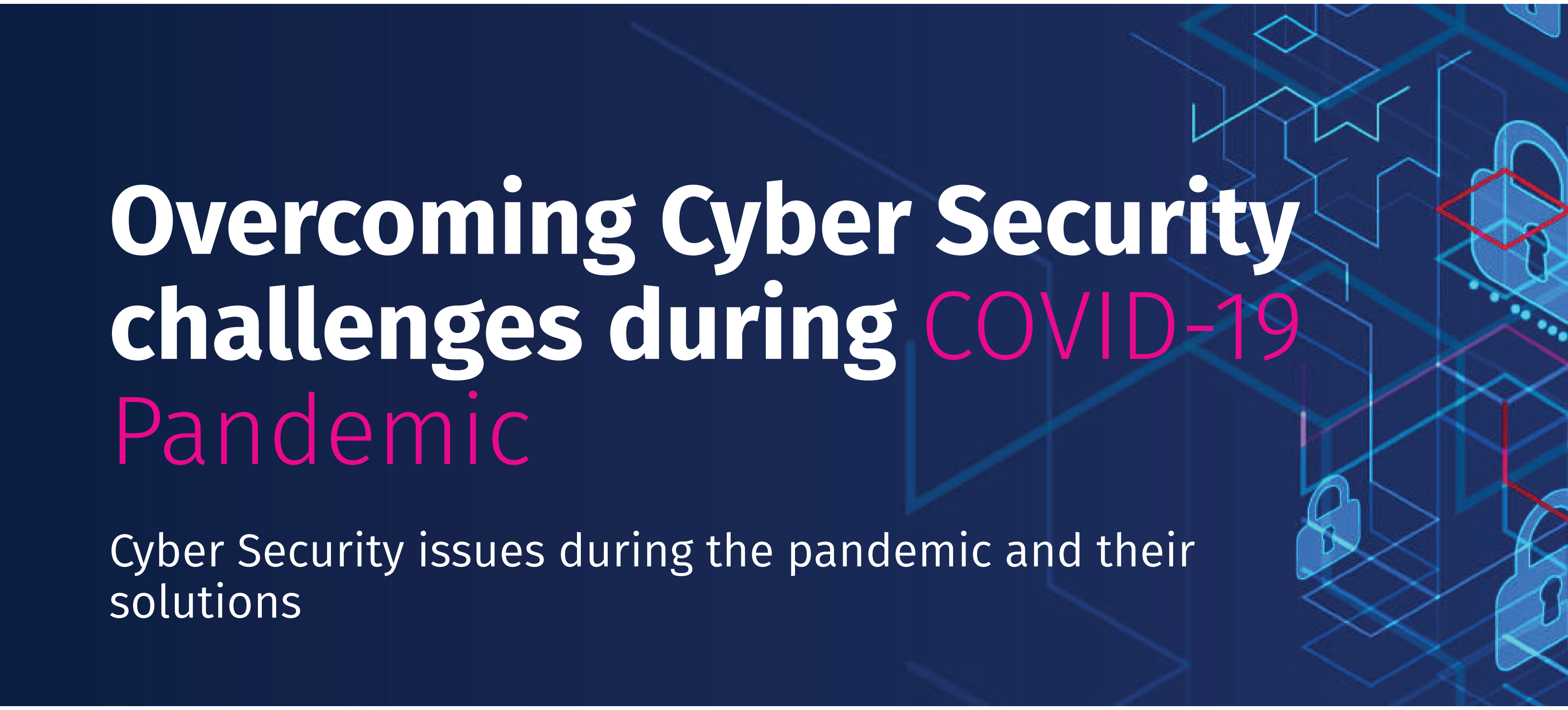


Overcoming Cyber Security challenges during COVID-19 Pandemic

Cyber Security issues during the pandemic and their solutions

Edited by **MOHAN DAS VISWAM**

Remedies for cyber security challenges cannot be uncertain as they pose a serious threat in all sectors such as governance, health care, finance, and transport. Just as the corona virus can be kept away by simple steps like social distancing and the use of masks and sanitizers, cyber threats amid the pandemic can be overcome by keeping cyber hygiene and following the best practices.

C.J. Antony
Dy. Director General
antony@nic.in

The year 2020 started with a lot of cheer and fanfare, reminiscent of the year 2000 that had ushered in this century and the millennium. But the euphoria was cut short with the news about a deadly virus spreading fast in China and other parts of the world. Sooner than later the first case in India was reported on 30th January and since then cases have been soaring. Governments at various levels took precautionary measures and initiated awareness programmes to contain the pandemic. Jantha curfew was observed across the Nation on 22nd March followed by the countrywide lock-down. Migrant workers and expatriates returned home in large numbers due to loss of livelihood. With the scientists still clueless on a possible solution, the end is nowhere in sight.

Turning Crisis to Opportunity

Corona Virus Disease (COVID-19) has thrown the world as a whole and nations in particular into an unprecedented crisis. The situation was challenging to the governments, corporates as well as individuals in terms of economy, social life, and even the very survival of human beings. Converting the crisis to an opportunity, governments across the country have opened new spheres in eGovernance. As a result, digital transformation that could not be achieved in the last six years was achieved in the last six months. What was hitherto considered to be The Normal was replaced by a New Normal. But this digital revolution was not without challenges - it has increased the scope for cyber-attacks. The increased use of cyber platform during the pandemic has widened the attack surface.

Cyber Security Challenges During Pandemic

Security challenges are always a fellow traveller of any crisis. Security takes a back seat during a shortage of key resources such as time, manpower and money. The pandemic called for the rolling out of voluminous hardware and software in a very short span of time. Often there was little time to harden the hardware and secure the software. More work needed to be carried out by the same or even less manpower. Delays in approval and transfer of funds created financial constraints in various spheres.

The pandemic confined a large number of people in their homes with their social life almost completely crippled. With the television initially telecasting only the repeat entertainment programmes, apart from the virus news, of course, the internet was the only source of entertainment for most people. Fear of salary cuts and layoffs due to the worsening economic conditions was looming large. As a result, the human mind started wandering - or remained idle - and negative emotions often influenced their behaviour. Casual browsing increased and attackers started exploiting this curiosity, confusion, fear, and boredom of the victims leading to large-scale phishing attacks.

Phishing in troubled Pandemic

Phishing is a fraudulent attempt to obtain sensitive information by disguising it as a trustworthy entity in electronic communication. More than 90% of data breaches start with spear-phishing attacks. In the current scenario where real-time

information about the disease is highly sought after, cybercriminals have been found to leverage online search terms by placing links to websites distributing malware as results of web search and social media. According to the report of a leading security OEM over one lakh new domains containing words like 'covid', 'virus', and 'corona' have been registered in the early weeks of the pandemic. Needless to say, a vast majority of these sites may be malicious and users need to be extra cautious while accessing them.

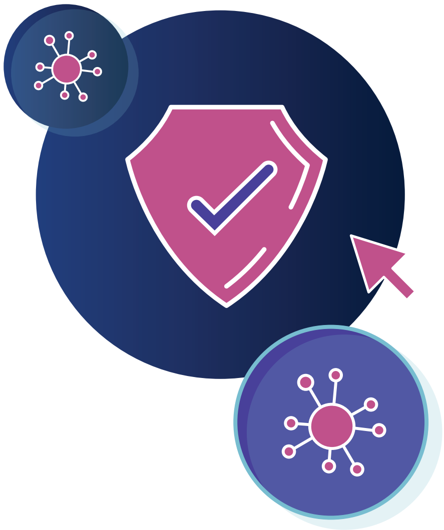
There are no fool-proof ways to avoid phishing attacks. Awareness needs to be created among users to stick to trusted sites for any information and apply due diligence before clicking any link. Keeping the browsers up-to-date with anti-phishing features, using antivirus software with website filtering, better password habits combined with multi-factor authentication are the other best practices against phishing attacks.

Work from Home

The culture of Work from Home (WFH) coupled with online meetings is going to be the long-lasting relic of the COVID-19. WFH has become a blessing in disguise for employees and employers alike. It provided the employees a safe workplace without any fear of infection at the comfort of their homes. The saving in time and expenses for travel enabled them to spend quality time with their families. The employers benefited from the continued availability of manpower often with extended working hours and saved the costs of power, rent, security, and the like. Ironically, the cybercriminals also benefitted, thanks to the security implications related to WFH culture!

All the major players in the Work from Home paradigms such as People, Process and Platform have security vulnerabilities associated with them. Utmost care must be taken to overcome these vulnerabilities forreaping the real benefits of the WFH system in the new normal. Organisations that suddenly shifted to WFH have become vulnerable on all these fronts and cyber attackers know this fact very well. The casua environment at home in contrast to the formal office atmosphere causes distractions and low alertness in employees, which are the key ingredients in the recipe for cyber-attacks. Psychological factors depending on family relations and vulnerabilities due to working at odd and extended hours also may cause security challenges.

During the time of crisis, there is an inherent tendency to bypass established processes and procedures. Policies and guidelines are often set aside for want of time, manpower and money. Other common security challenges in the process include granting temporary access and escalation of privilege to users and systems for the sake of convenience and sharing of user credentials with those in the office and contract workforce for executing urgent tasks. The remote desktop facility can be easily misused unless proper protocols and precautions are not followed.



Serious vulnerabilities exist at every point of the platform the employees use to Work from Home. The employees are primarily outside the protection of the secured perimeter of their organisations and the corporate data is being exchanged through unsecured channels, even without a Virtual Private Network (VPN). Employees use their personal devices such as desktops and laptops with outdated/ pirated operating systems and application software to perform office tasks. These devices are often without basic antivirus solution and are shared with other family members for online classes and gaming activities. The default names and easy-to-guess passwords of the home WiFi Networks is another matter of serious concern that can be addressed easily by following the best practices.

Online Meetings

Online meetings have saved the day in ensuring business continuity during the pandemic in all spheres of life like governance, academia, and healthcare. The daily routine of the employees is now governed by their professional (and personal) virtual meetings and the people have got accustomed to it. Shortage of time, know-how and finances have forced organisations to choose the platform for virtual meetings without considering the security aspects. While the 'Free Tools' has made the choice easy, large-scale usage, especially during the early days of lockdown, has made the matters worse.

Simple precautions can overcome the security challenges with online meetings to a large extent. Always ensure that important meetings are password protected to safeguard their privacy and confidentiality. Otherwise malicious users may join these meetings and overhear the conversations by keeping the camera off and mike muted. The use of host controls like Lobby and Room Locking to moderate meetings can keep the malicious elements at bay. Disable file transfer by default and beware of threat actors using the chat portion to spread malicious links. Always use the latest version of the software as the OEMs are releasing security fixes regularly. While the notice to the meeting can be circulated well in advance, sensitive information like meeting ID and password may be shared privately under short notice.

Conclusion

Various countries across the globe. While researchers are hopeful of an immediate remedy, the possibility of an affordable vaccine for large-scale roll-out across the world in near future is still uncertain. Remedies for cyber security challenges cannot be uncertain as they pose a serious threat in all sectors such as governance, health care, finance, and transport. Just as the corona virus can be kept away by simple steps like social distancing and the use of masks and sanitizers, cyber threats amid the pandemic can be overcome by keeping cyber hygiene and following the best practices. As citizens across the globe are getting accustomed to living with the corona virus, netizens should learn to live amidst cyber criminals by devising appropriate mechanisms to overcome attacks during and after the pandemic.

For further information, please contact:

C.J. Antony
Deputy Director General
National Informatics Centre
A-Block, CGO Complex, Lodhi Road -110003
NEW DELHI
Email: antony@nic.in, Phone: 011-24305166