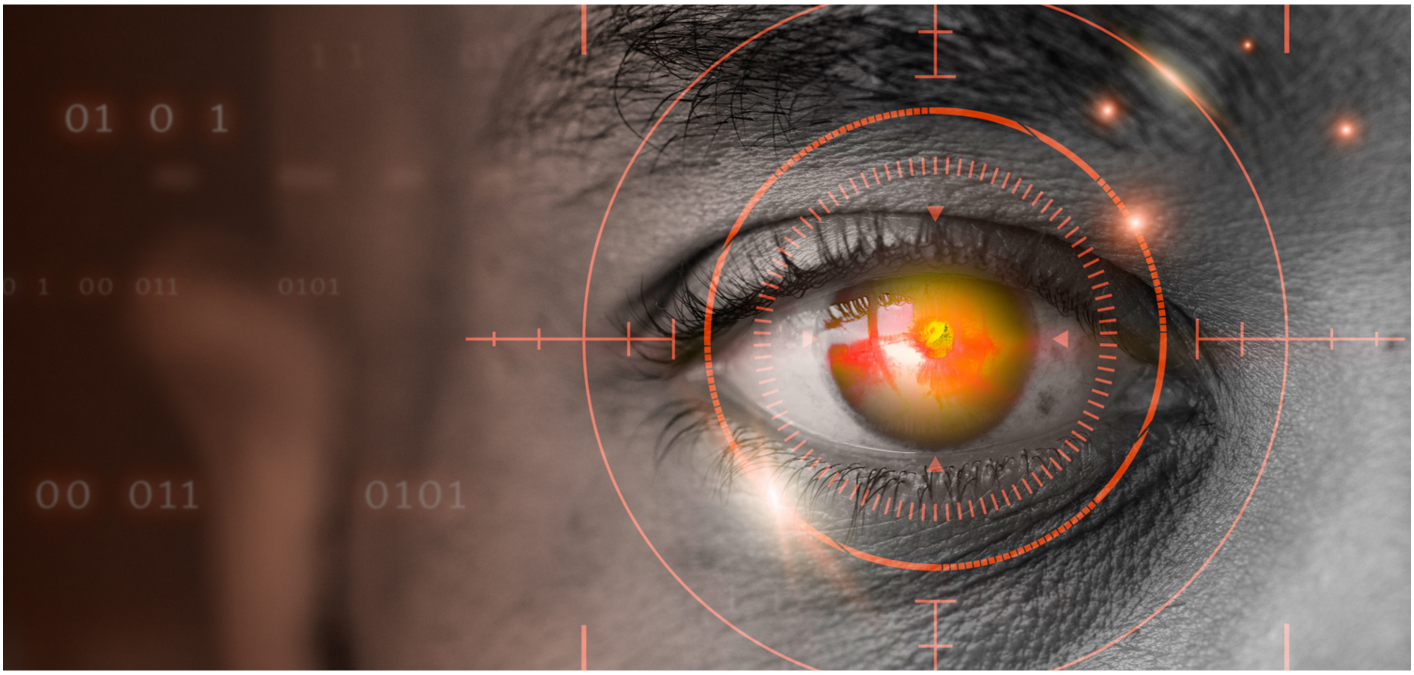
INDIA FUTURE FOUNDATION

INDIA FUTURE FOUNDATION

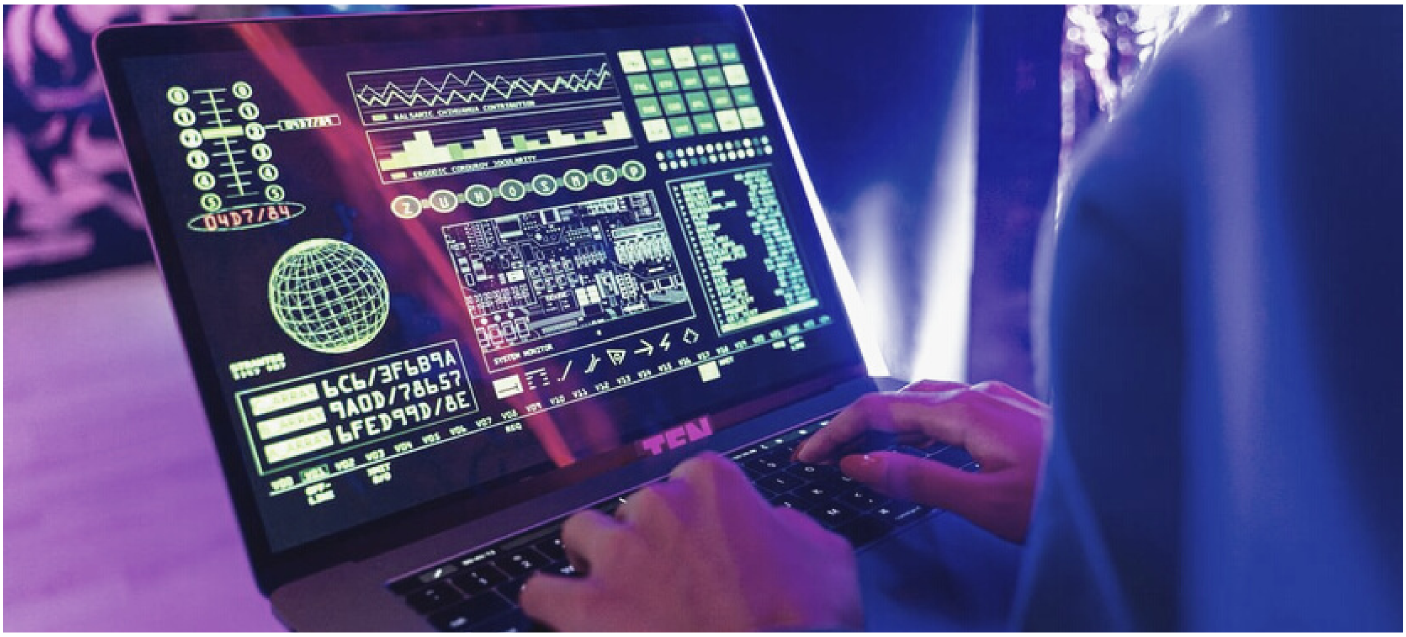
Freedom of Expression, Trust and Safety on Internet



PROJECT PEGASUS: PRIVACY UNDER CYBER ATTACK?

The forgotten Greek mythology winged horse - "Pegasus" resurfaced in the form of surveillance spyware. The mass surveillance project is the product of Israel's NSO Group Technologies. Through a collaborative effort by the Paris-based non-profit Forbidden Stories, Amnesty International, and 17 media organizations from 10 countries reveals that the Pegasus spyware is used to spy on politicians, journalists, and activists. The revelation is attributed to a leaked list of 50,000 phone numbers across 45 countries. NSO group claims that it counts only "vetted" governments among its clients. In the early versions of Pegasus, it used spear-phishing techniques to snoop into the target's phone.

OTHER STORIES INSIDE THIS ISSUE:



The current version of Pegasus is more dangerous as it involves "zero-click" techniques in which the target need not do anything or take any action but still can get infected by the spyware. In 2019, WhatsApp released a statement that Pegasus can infect phones via WhatsApp calls even if the calls are not answered. Pegasus used such zero-day exploits in Android and Apple phones to get into the target's phones. Once inside the phone, it escalates its privileges to root and obtains complete control of the device. It establishes a connection with the command-and-control centres and starts transmitting data of the target. Pegasus can turn the phone into a spying device with root privileges and turn the camera and microphones without the target's knowledge.

The NSO group claims it works with 60 clients in 40 countries. The leaked database includes 300 Indian phone numbers from the media houses like The Wire, The Hindu, Hindustan Times, politicians, journalists, and activists. Amnesty International released a detailed forensics report on the Pegasus spyware. Researchers at Amnesty International developed a tool – "Mobile Verification Toolkit" to find forensic traces that can help identify if the Pegasus spyware targeted your phone.

Source: https://www.indiatoday.in/world/story/decoded-nso-pegasus-spyware-greek-meaning-india-mexico-saudi-uae-1831122-2021-07-22

KASEYA RANSOMWARE ATTACK – THE BIGGEST RANSOMWARE ATTACK ON RECORD

The Kaseya, a US-based IT solutions developer for MSPs and enterprise clients, became a victim of a ransomware attack. The ransomware attack is already called the biggest ransomware attack on record as hackers demand 70 million dollars. The attack affects 800 to 1500 businesses globally. The Russian hacker group REvil claimed responsibility for the ransomware attack.

Attackers leveraged a vulnerability in Kaseya VSA software, and researchers believe that the attack is triggered via an authentication bypass zero-day vulnerability present in the web interface of the VSA software. This vulnerability allowed the attackers to gain access to the VSA server.

The REvil group offered a universal decryption key for a ransom of 70 million dollars in the bitcoin currency. U.S Senators and politicians hugely blamed cryptocurrency technology for the increasing ransomware attacks. On 26th July 2021, Kaseya announced a decryption key for its clients to recover encrypted data by the ransomware attack. The firm denied paying the 70 million dollars ransom to the REvil group directly or indirectly through a third party.

BIDEN GOVERNMENT PUSHES FOR STRONGER CYBERSECURITY POSTURE

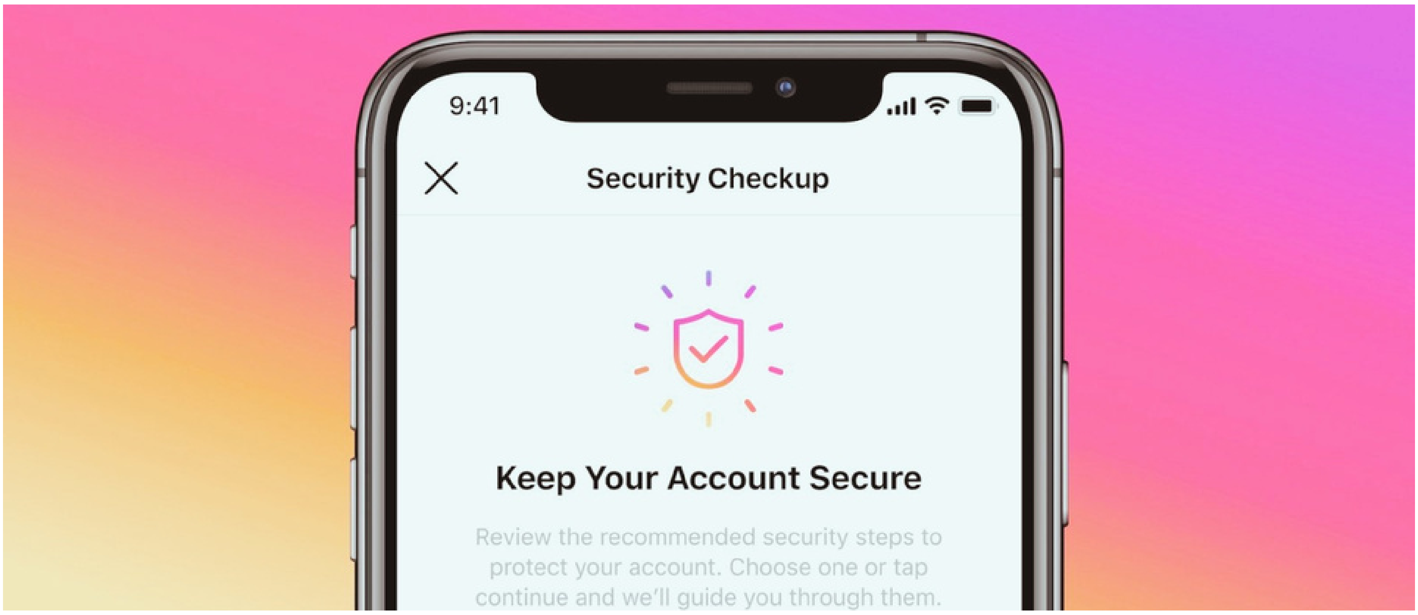
The White House released a memo for ransomware attacks urging Corporate Executives and Business Leaders to immediately convene their leadership teams to discuss ransomware threats and review corporate security posture and business continuity plans. The threats of ransomware attacks are serious as cybercriminals shift to disrupt core operations rather than steal the data. The memo states that the U.S. government's efforts to disrupt ransomware networks, work with international partners to hold countries accountable that harbours ransomware attacks and actors, develop policies towards ransom payments.

The memo reiterates the critical responsibility of private sectors to protect against cyber threats and recognise that ransomware attackers can target any company. The White House memo lists five best practices that organisations can implement and make rapid progress on risk management:

1. Backup your data, system images, and configurations, regularly test them, and keep the backups offline
2. Update and patch systems promptly
3. Test your incident response plan
4. Check your security team's work
5. Segment your networks

On 28th July 2021, the Biden Administration released a fact sheet and announced President Biden signed a new executive order - "Improving Cybersecurity for Critical Infrastructure Control Systems" aimed to protect the critical infrastructure against cyber attacks.

INSTAGRAM LAUNCHES SECURITY CHECKUP TO HELP PEOPLE KEEP THEIR ACCOUNTS SAFE



Keep Your Account Secure

Review the recommended security steps to protect your account. Choose one or tap continue and we'll guide you through them.

Instagram introduced a new Security Checkup feature to help people keep their Instagram accounts safe and secure. This feature will guide people whose accounts may be compromised by hackers and will guide them with appropriate steps to recover their accounts securely.

Additionally, Instagram listed a few other best practices that everyone can take to make their accounts more secure. Below are the recommendations:

- Enable two-factor authentication: Instagram urged users to enable two-factor authentication as an extra layer of protection.
- Instagram urged users to update their phone numbers and email to recover the account if their accounts got compromised.
- Instagram claims to see a rise in malicious account messaging to try and access sensitive information like account passwords in the name of Instagram. Instagram confirmed that it will never send a Direct Message (DM) to people.

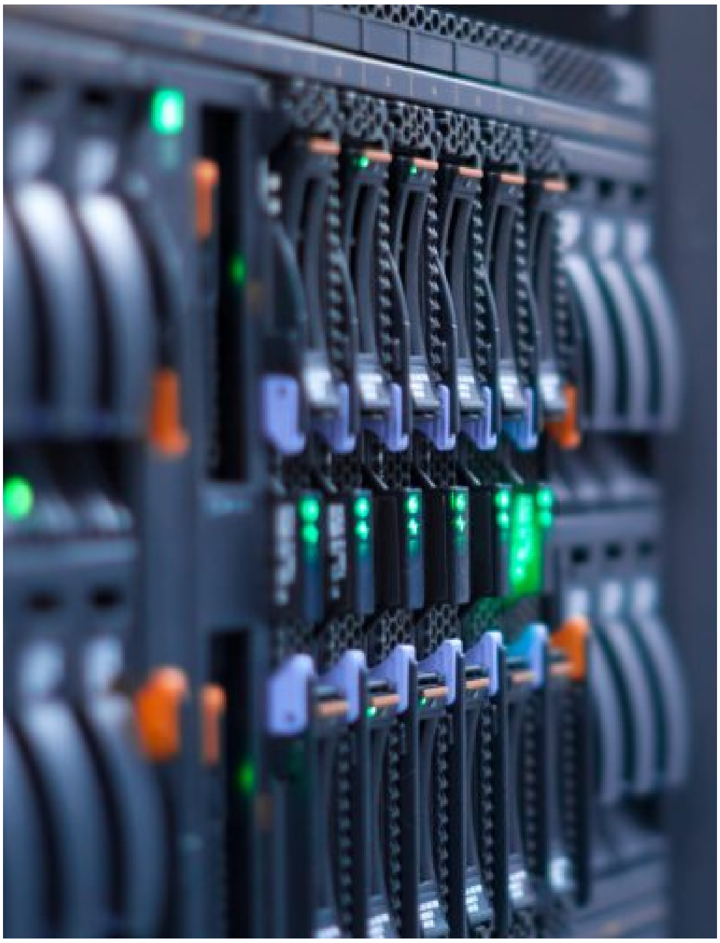
- Users can report inappropriate content from the post or visit the account and report directly from the profile.

- Set up login requests to receive an alert when someone tries to log in. These alerts will inform about the device and location from which one is attempting to log in.

Source: https://about.instagram.com/blog/announcements/keeping-instagram-safe-and-secure

MICROSOFT'S INCOMPLETE PATCH ALLOWS REMOTE CODE EXECUTION

The PrintNightmare is a printing-related vulnerability first discovered on Windows 7. Microsoft confirmed that this vulnerability existed in all of their operating systems above Windows 7, including Windows 10 as well. This vulnerability enables an attacker to run commands as an administrator, a direct vector of local privilege escalation (LPE). In simple terms, An attacker can add users with administrator rights, view all files, remove any file, and can potentially add a backdoor to the infected system.



The PrintNightmare vulnerability is quite dangerous because the service Print Spooler is enabled by default, so an attacker need not need to enable it. In June, Microsoft came out with a patch for this issue. Unfortunately, Microsoft only released a patch for the Remote Code Execution vulnerability and not for the Local Privilege Escalation vulnerability. However, the official statement from Microsoft mentioned that the issue is completely fixed. Responding to the statement, security researchers published the exploit to the vulnerabilities. Although the exploits are taken down but they were posted for quite a while.

Source: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

ILLEGAL WILDLIFE TRADE ON SURFACE AND DARK WEB

The darknet is the part of the internet, which is not indexed by search engines like Google. This separate “internet” can only be accessed by special browsing software, like the “Tor Browser”. The TOR Browser connects the user to the TOR network. The TOR network is a network designed with anonymity as the primary goal to protect the privacy of its users. Traffic on the TOR network is highly encrypted to preserve the identity of the sender and the receiver of data.

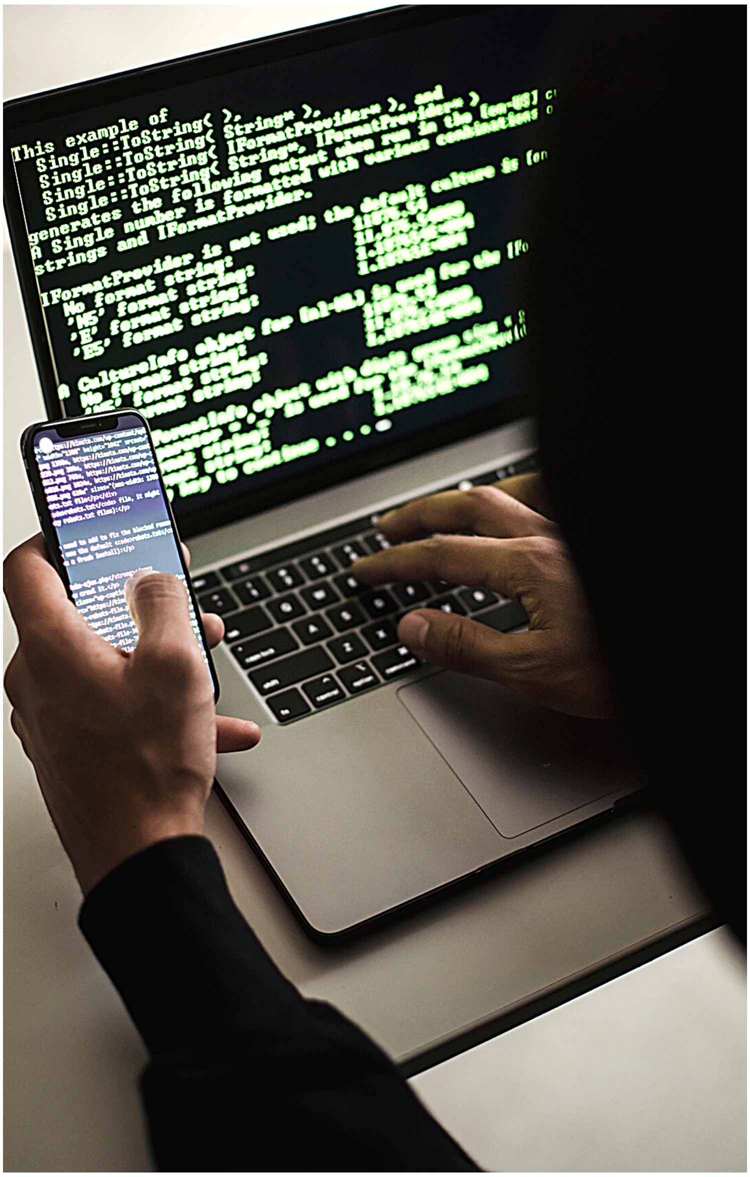
While this is promising in terms of security and privacy, malicious actors use this technology to earn profit by providing services that are considered illegal. One of such services is the Illegal Wildlife Trade markets. Biodiversity loss is currently one of the greatest global risks. There are traces of marketplaces on the dark web that enables users to trade in Wildlife products. As far as the illegal wildlife trade goes, offenders use the surface web for that purpose as well. Websites like eBay are known to host such products. In 2005, close to 9,000 ads were posted on the clear web relating to the wildlife trade. Most of these products are derived from ivory. Other than ivory products, live animals are put for sale like a Gorilla sells for over $9,000.

On the clear web, eBay is the marketplace where these activities occur in the most significant numbers. eBay, in response, issued policies and rules that forbid any ads on their website of such nature. As for the dark web, many marketplaces support the illegal wildlife trade. On conducting a study, researchers found one result displaying a species of cactus, which is used as a hallucinogen, for sale on the AlphaBay market. There are possibly many marketplaces that are yet undiscovered or are only available with invite codes, as seen as a general trend in illegal dark web marketplaces.

WHEN CRYPTOCOIN MALWARE EVOLVES: LEMONDUCK MALWARE PUTS WINOWS AND LINUX SYSTEM AT RISK

An infamous crypto-mining malware evolved over the years from a cryptocurrency botnet to malware capable of stealing credentials, removing security controls, and spreading via phishing emails, exploits, Exchange Server vulnerabilities, and USB devices. LemonDuck is one of the few bot malware that targets both Windows and Linux systems.

In 2020, the malware used COVID-19-themed lures in email attacks. In 2021, the malware exploits newly patched Microsoft Exchange Server vulnerabilities to compromise unpatched systems. LemonDuck expanded its operations to the USA, Russia, China, Germany, the United Kingdom, India, Korea, Canada, France, and Vietnam.



Researchers found the malware to use automated tools to scan, detect, and exploit servers. "Once inside a system with an Outlook mailbox, as part of its normal exploitation behaviour, LemonDuck attempts to run a script that utilizes the credentials present on the device. The script instructs the mailbox to send copies of a phishing message with preset messages and attachments to all contacts."

Source: https://www.microsoft.com/security/blog/2021/07/22/when-coin-miners-evolve-part-1-exposing-lemonduck-and-lemoncat-modern-mining-malware-infrastructure/

KODI BOXES HIT REVENUES OF PAY TV AND OTT PLATFORMS

Piracy is a real issue we face today, where everything is available online. In the generation of the internet, the entertainment industry, too, is on the internet. Companies like Netflix and Amazon are prime examples of this industry. And piracy for them is one of the primary concerns. Kodi boxes these days are used to stream paid content from these platforms for free, which is technically illegal. Kodi is open-source media-playing software and can be used to play media like songs, movies, and videos. Kodi boxes offer all major Indian broadcasters content, including Star, Zee, Viacom18, Sony Pictures, ETV and SunTV. These boxes are available for sale on various e-commerce sites and wholesale or retail stores in Gujarat, Delhi, Uttar Pradesh and West Bengal.

What makes Kodi so reliable and exciting is the ease of use and customizability. Users can customize their Kodi media player however they'd like. Files do not have to be stored in the computer/storage to be played on the software as Kodi can download it from the internet. Nowadays, the Kodi software is embedded into Set-Top boxes and is called as Kodi-Boxes. So, a Kodi-Box is any TV set-top box in which the Kodi software is installed.

Digital piracy costs jobs and hurts businesses, and lose 10-25% of their annual revenues to piracy. More than 400 Indian channels are illegally streamed and impact Indian broadcasters' business.

Source: https://www.livemint.com/industry/media/tv-channels-battle-piracy-woes-11624960194388.html

PROTECT YOUR PRIVACY ON SOCIAL MEDIA

Would you consider yourself walking to a room full of people and broadcasting the details of your private life like health issues, your location, and opinions? The answer is no, but we do not think posting the same on social media platforms. Social media is a great place to connect, but the ramifications of sharing too much may impact your personal life and your professional life as well. One needs to understand what information social media platforms collect and how they are used.

Review the privacy setting for all your social media platforms, especially when there is a change in terms of service and privacy policy. Adjust the privacy settings as the default privacy setting may permit information sharing. Review the settings of who can tag you in their post and be selective with the audience. Block and report any inappropriate content on your feed.

INDIA FUTURE FOUNDATION

India Future Foundation

Phone: +91-1244045954, +91-9312580816
Email: helpline@indiafuturefoundation.com
BSMT, Building no. 2731 EP, Sector 57, Golf Course Ext. Road, Gurugram,
Haryana, India – 122003
www.indiafuturefoundation.com