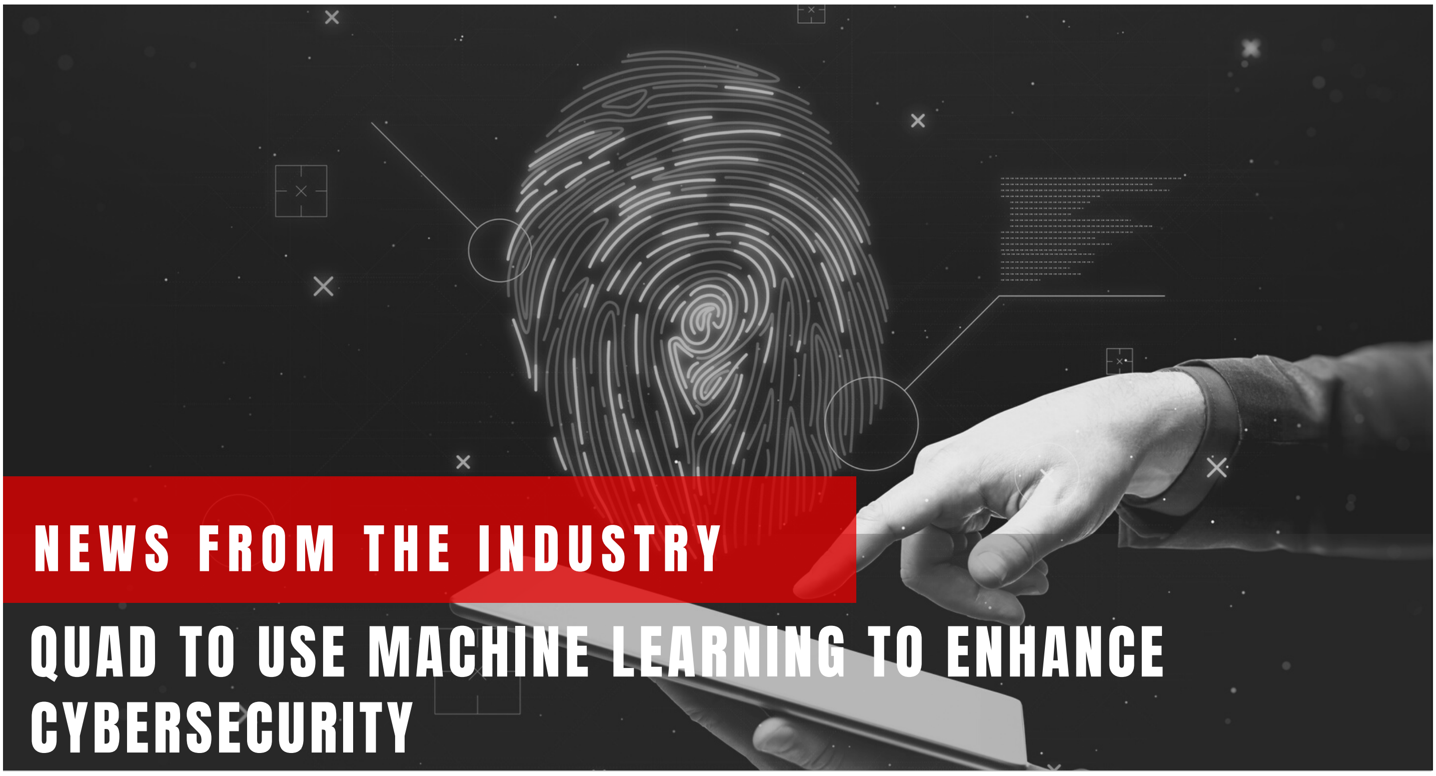
INDIA FUTURE FOUNDATION

Freedom of Expression, Trust and Safety on the Internet



NEWS FROM THE INDUSTRY

QUAD TO USE MACHINE LEARNING TO ENHANCE CYBERSECURITY

The Quad, an informal alliance between Australia, India, Japan and the US, has pledged to use advanced technologies, including machine learning, to enhance cybersecurity. At a recent meeting in New Delhi, the group reaffirmed its commitment to a free and open Indo-Pacific that is inclusive and resilient. In the longer term, the Quad aims to establish secure channels for computer emergency response teams and private sector threat information sharing, as well as to create a framework and methodology for ensuring supply chain security and resilience for information communication technologies and operational technology systems of critical sectors. These objectives will form part of the future work plan for the group.

Closer collaboration on machine learning research will enable better detection of network intrusions and improving cyber risk management of critical infrastructure. The framework for secure threat information sharing by computer emergency response teams and private sector entities will enable better real-time cooperation and assessments as cyber incidents arise. The

IN THIS NEWSLETTER

1. News from the Industry..01

2. Theme of the Month.........06

3. Our Events...............................07

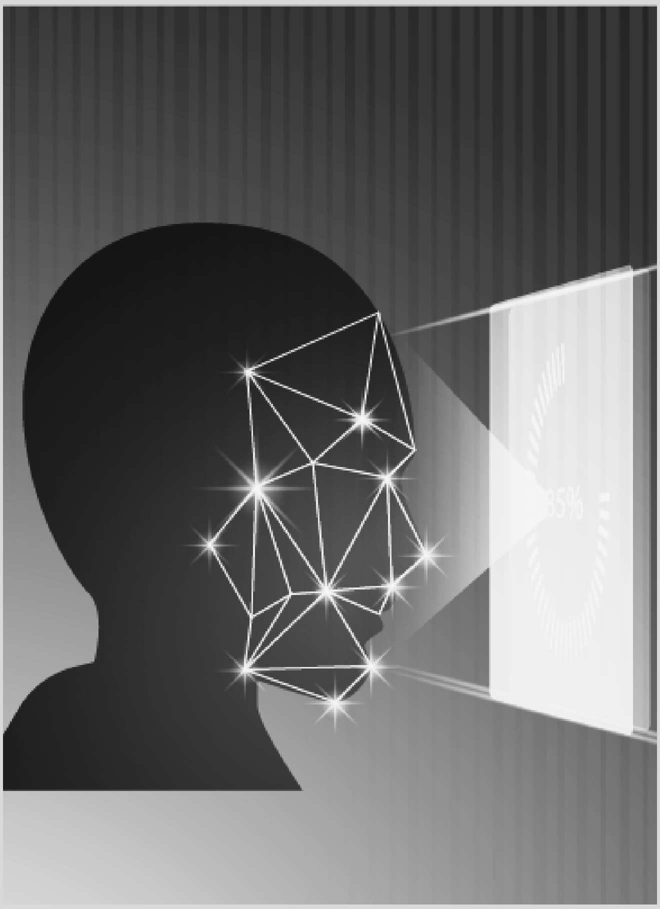
4. Panel Discussions..............09

5. IFF in the Media.....................10

Quad Cyber Challenge campaign will promote basic cybersecurity awareness among individuals, organisations, businesses and governments throughout the group. The efforts demonstrate the Quad's commitment to building regional capacity and ensuring the delivery of an open and secure telecommunications infrastructure in the Indo-Pacific.

NIST RELEASES NEW GUIDELINES FOR DIGITAL IDENTITY

The National Institute of Standards and Technology (NIST) has released new guidelines for digital identity management. NIST is updating its digital identity guidelines for the first time since 2017, which will help set the course for best practices in handling digital identity for organizations across all sectors. Digital identity is the online persona of a subject and how that subject is represented online. The guidelines focus on the use of biometrics, including facial recognition, to prove digital identity, especially with the proposed guidelines updating the use of facial recognition while downgrading the use of biometrics from the 2017 version. The NIST digital guidelines will directly address the struggles of facial recognition and biometrics. NIST is looking for feedback on the proposed guideline changes until March 24, 2023.



ASIA PACIFIC MOST ATTACKED REGION FOR THE 2ND YEAR

According to the X-Force Threat Intelligence Index published by IBM Security, the Asia Pacific region was the most attacked, in the world, for the second consecutive year, in 2022. The index analysed data from the company's Security Operations Centre and found that the region accounted for 53% of all attacks worldwide. The index also highlighted that the number of attacks targeting the Asia Pacific region had increased by 46% from the previous year. The most commonly targeted industries were technology and telecommunications, followed by finance, healthcare, and retail.

The report identified a number of factors contributing to the high number of attacks in the Asia Pacific region, to the increasing number of connected devices, rapid digitization of industries, growing sophistication of cybercriminals and the increasing use of artificial intelligence in attacks.

In response to the growing threat, the report has emphasized the importance of implementing effective cybersecurity measures, such as network segmentation, multi -

factor authentication and advanced threat detection. The report also recommended that companies collaborate with government agencies, industry associations, and other stakeholders to share information and best practices.

NEW SURVEY FINDS DFIR TEAMS AT HIGH RISK OF BURNOUT

A new survey conducted by Magnet Forensics, a software company based in Canada, has found that Digital Forensics and Incident Response (DFIR) teams predominately located in North America, Europe, the Middle East and Africa are at high risk of burnout due to the demanding nature of their work. The 2022 State of Enterprise DFIR report surveyed 400 DFIR professionals found that over half of the respondents reported a feeling of burnt out or stressed in their job.

The survey identified several factors contributing to the high risk of burnout among DFIR professionals. These included heavy workloads, long working hours and the emotionally taxing nature of dealing with cyberattacks and security incidents. The survey also highlighted the lack of resources and support for DFIR teams, with many respondents reporting that they felt overworked and underappreciated. The consequences of burnout in DFIR teams can be significant, especially with increased rates of turnover and reduced productivity. The survey found that over a third of the respondents had considered leaving their job due to burnout and over half of them reported that burnout had a negative impact on their quality of work.

In response to the survey's findings, Magnet Forensics recommended that organizations take steps to address the issue of burnout among DFIR professionals. These include providing additional resources and support, such as training and mentoring programs and implementing policies to promote work-life balance and prevent overwork.

5G ROLLOUT DEMANDS CYBERSECURITY INVESTMENT

Lt Gen. (Retd) (Dr) Rajesh Pant, National Cyber Security Coordinator, Prime Minister’s Office, Government of India, has urged companies to prioritize investments in cybersecurity ahead of the 5G rollout in India. During the 17th edition of the India Digital Summit, Lt Gen (Retd) Dr Rajesh Pant emphasized the need for companies to secure their networks, develop comprehensive cybersecurity strategies and collaborate with the government and other stakeholders to address potential threats.

During the Summit, Lt Gen. (Retd) Dr Pant emphasized the need for companies to focus on securing their networks, especially considering that the widespread adoption of 5G technology is expected to increase the number of connected devices and data traffic. He highlighted the risks associated with cyber threats and the potential impact on critical infrastructure, including power grids and transportation systems. Lt Gen. (Retd) Dr Pant also stressed on the importance of developing a comprehensive cybersecurity strategy that includes measures such as risk assessments, employee training and incident response plans. He suggested that companies should collaborate with the government and other stakeholders to share information and intelligence on potential cyber threats.

DEEP REINFORCEMENT LEARNING SHOWS PROMISE FOR PROACTIVE CYBERSECURITY

In a significant development, researchers from the Pacific Northwest National Laboratory, Richland, Washington have made progress in utilizing Deep Reinforcement Learning (DRL) for protecting computer networks from sophisticated cyberattacks. In simulation settings that mimicked multistage attack scenarios involving different types of adversaries, DRL was able to prevent adversaries from achieving their goals up to 95% of the time. This outcome paves the way for autonomous AI's potential in proactive cybersecurity.

The researchers' first step was creating a dynamic attack-defence simulation environment to test various AI-based defensive methods under controlled conditions. This tool was vital in evaluating the performance of deep reinforcement learning algorithms, which are becoming increasingly popular as decision-support tools for cybersecurity experts. Unlike other AI systems that detect intrusions or filter spam messages, DRL allows defenders to plan sequential decision-making strategies and adapt to rapidly changing circumstances when faced with adversaries.

With deep reinforcement learning, cybersecurity can become smarter, enabling the detection of changes in the cyber landscape earlier, and giving defenders the chance to take pre-emptive measures to thwart cyberattacks.

IBM DETECTS RISING THREAT OF INFORMATION STEALERS

IBM’s Advanced Threat Detection and Response Team (ATDR) has reported an increase in the number of information stealers in the wild over the past year. Information stealers are malware that can scan for and steal sensitive data and credentials from users' devices. These malwares target various directories that usually contain sensitive information, such as login data from web browsers like Chrome, Firefox, and Microsoft Edge, as well as chatting applications like Telegram and Discord. Some of the popular information stealers include Redline, Raccoon, and Vidar.

The major threat posed by these information stealers is the compromise of users' credentials, which can lead to blackmail or be sold on the dark web. Furthermore, these malwares can evade anti-virus solutions and endpoint detection and response (EDR) platforms, resulting in a false negative that may go undetected unless explicitly searched for. IBM's ATDR team has been actively identifying these information stealers and documenting their behaviors and indicators to assist the community in detecting and developing custom detections to address this security gap.

SECURING GAMING CONSOLES SHOULD BE A PRIORITY

Video game consoles have become a popular form of entertainment for both adults and children worldwide, with an estimated 3.09 billion active gamers. However, the rising popularity of video gaming has attracted cyber-criminals looking to target players' login credentials and personal information. A recent survey of 1,000 gamers, in the US, found that two-thirds of daily or almost daily players had experienced hacking or scams while playing. Xbox users were the most targeted, with 87% experiencing at least one hacking attempt. The consequences of being hacked included compromised email (53%), phone numbers (48%), payment data (45%), financial accounts (43%) and social media accounts (38%). On average, gamers lost $330 due to compromised data.

While some gamers employed multiple-character passwords and avoided clicking suspicious links, 48% of those who relied solely on passwords had been hacked. Gaming companies and users must deploy every defensive measure available, including secure multi-factor authentication, updating software and device firmware and being cautious with cheat codes and links in emails.

SAFER INTERNET DAY

Safer Internet Day is an annual event celebrated on the first Tuesday of February, with the aim of promoting a safer and better Internet experience for people all over the world. The event was first initiated by the European Union, in 2004, and has since grown to be celebrated globally, with more than 180 countries participating in the event, in 2023.

The theme for Safer Internet Day 2023 was "Together for a better Internet", highlighting the importance of collective efforts in creating a safer online environment. The Internet has become an integral part of our daily lives, and it's essential to ensure that we use it safely and responsibly. Safer Internet Day aims to raise awareness among individuals, especially children and young people, about the potential risks associated with the Internet and how to stay safe online.

The event aims to promote safe online behaviour and encourage people to adopt good digital habits such as using strong passwords, avoiding sharing personal information online and being mindful of online interactions. Safer Internet Day also encourages the involvement of stakeholders such as parents, teachers, and policymakers in promoting online safety. It provides a platform for discussions and collaborations on issues related to online safety and helps to raise awareness on the need for policies and regulations to promote a safer Internet experience for all.

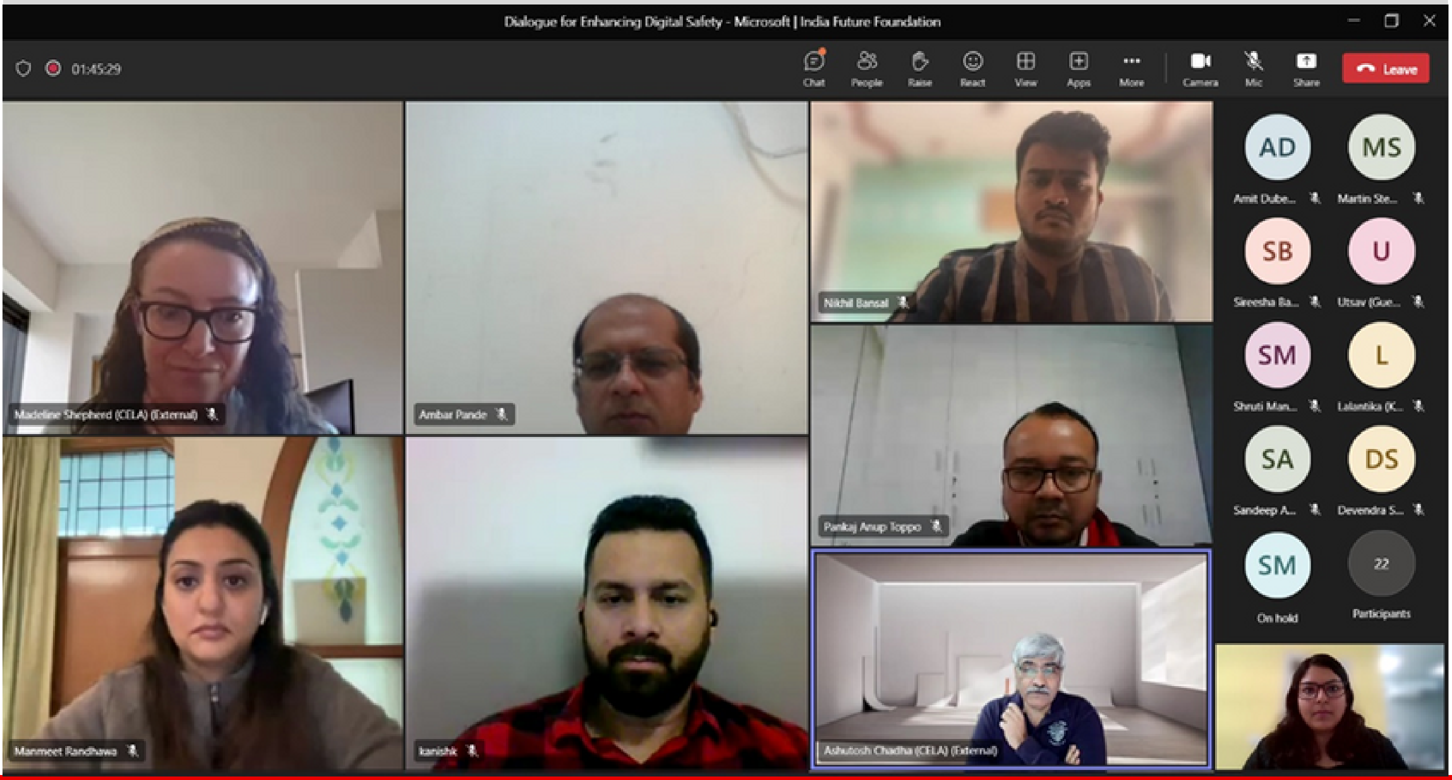
OUR EVENTS

Dialogue for Enhancing Digital Safety

India Future Foundation (IFF) in collaboration with Microsoft organized a "Dialogue for Enhancing Digital Safety" to mark Safer Internet Day on February 7, 2023. This event aimed at creating awareness about the need for enhancing digital safety among children by bringing together experts from the tech industry and civil society. The dialogue was led by Ms Madeline Shepherd, Digital Safety Lead- Asia Pacific Microsoft who presented the Global Safety Survey Index 2023 published annually by Microsoft. The event was moderated by Mr Kanishk Gaur, Founder, IFF.

As per the survey, globally 69% of respondents- experienced risk of some nature. Most of the respondents experienced risks in the form of hate speech and cyber bullying which formed a part of personal risks. Other form of risks, to which the respondents were exposed to were violent risks such as terrorist content, gory content, sexual solicitation, revenge porn or publication of photos without consent. At a global level more than 50% of the respondents have been exposed to risks of misinformation/disinformation, which was a major risk in the survey.

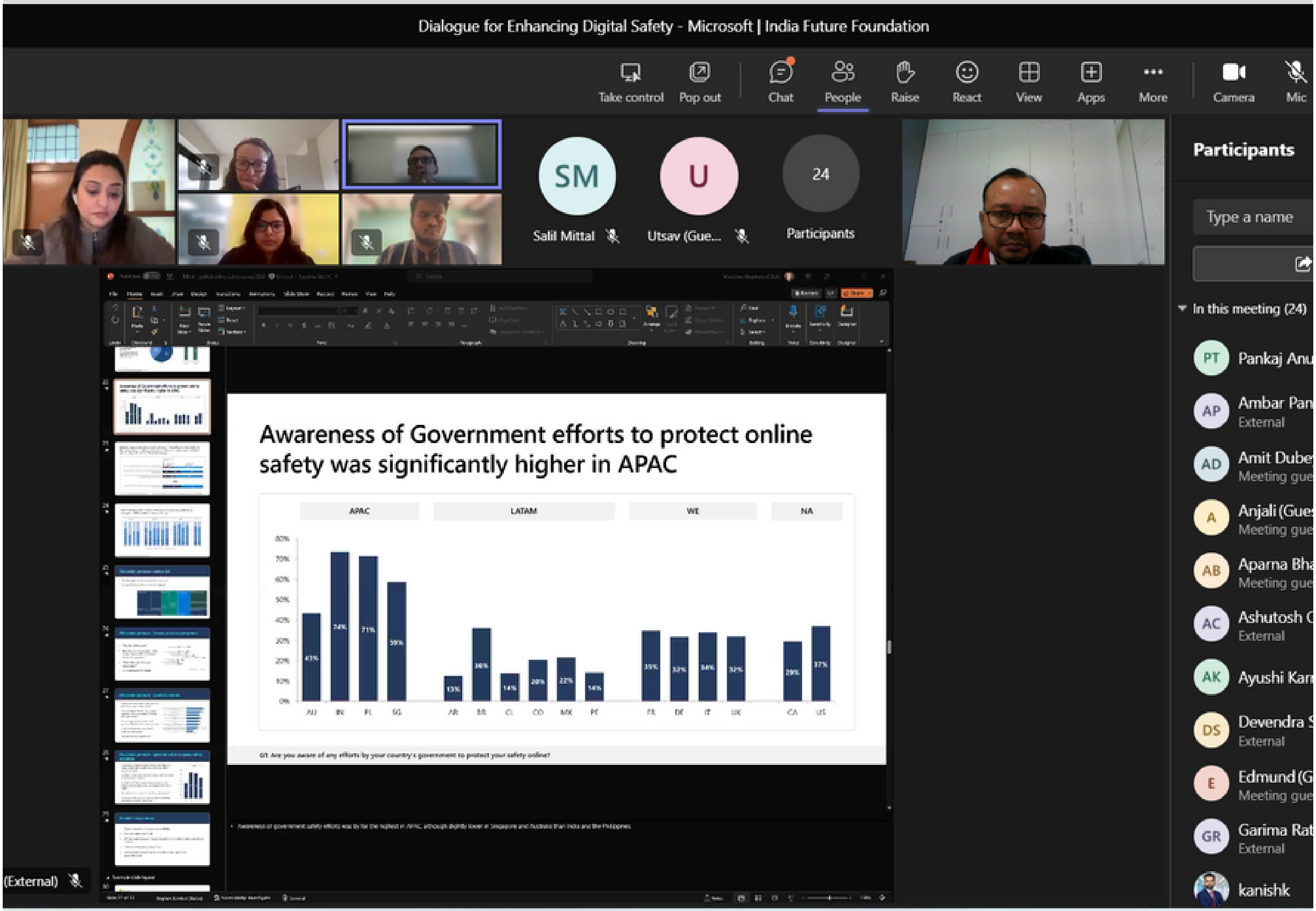
These online harms result into a loss of trust in other people, leads to mental health compromises and loss of reputation. These harms, when considered in the case of juveniles becomes even more dangerous, as they have consequences which go beyond the online world. Children/teenagers get affected by them in their formative years which can lead to a lifelong trauma. The survey also pointed out the level of awareness among the parents and adults about online harms that kids might be exposed to, initiatives taken by parents to ensure child safety and steps taken by teenagers to protect themselves from online risks. The survey also looked at the awareness among citizens, about government campaigns and initiatives regarding online safety of children, along with the trust that people have on online platforms to take steps for reducing risks and develop tools for child safety.



During the discussions regarding the report's data on awareness of government agencies and helplines, there was a focus on the possibility of a ground reality that differed from what was reflected in the survey results. Many people who are victims of cybercrimes such as cyber bullying do not know which agency to approach. This causes mental harassment, especially among teenagers and at times, they are also driven to suicide. The survey also pointed towards the lack of solutions that are available for content filtering, on the Internet, for children.

There is a need for government policies or guidelines that mandates having a “Child Safe Switch.” Further, while preparing a roadmap for digital safety, the impact on mental health of teenagers should be considered. At the same time, children should also have access to a forum at the school level that not only provides assistance in case of cyber incidents, at the school level, but also inculcates the practice of Internet safety among students.

Some of the attendees at the consultation included Mr Salil Mittal, Lead Cyber Security – Emerging Technologies, Jio; Mr Utsav Mittal, CEO, Xiarch; Mr Ambar Pande, Principal Consultant, Program Manager at Govt of M.P (e-Governance); Martin Stewart, First Secretary, Cyber Policy, British High Commission New Delhi; Mr Ashutosh Chadda, Director and Country Head Government Affairs & Public Policy, Microsoft; Mr Sandeep Arora, Public Policy and Government Affairs, Microsoft and Dr Shruti Mantri, Associate Director, Indian School of Business.


Dialogue for Enhancing Digital Safety - Microsoft | India Future Foundation

Awareness of Government efforts to protect online safety was significantly higher in APAC

Q1: Are you aware of any efforts by your country's government to protect your safety online?

- Awareness of government safety efforts was by far the highest in APAC, although slightly lower in Singapore and Australia than India and the Philippines.

PANEL DISCUSSIONS

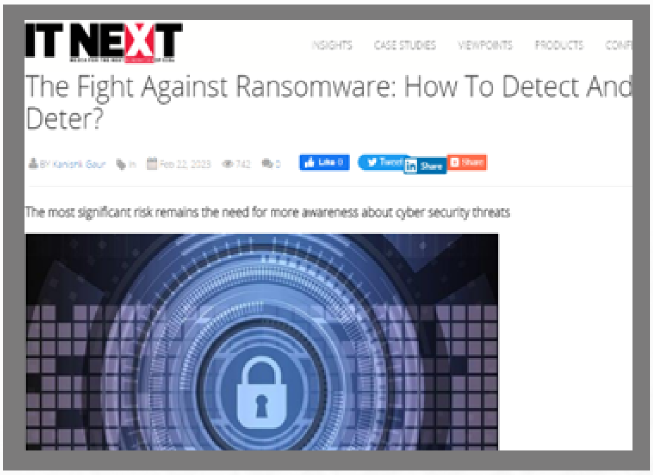
Conference on Cyber Warfare: Contours and Concepts

Lisianthus Tech, an organisation that provides IT security services, in collaboration with Keysight Technologies, Sectrio and Rah Infotech organized a conference on Cyber Warfare: Contours and Concepts on February 23rd, 2023. The conference focused on the emerging threats due to cyber warfare and its impact on national security. Mr Kanishk Gaur, Founder, India Future Foundation participated in this conference as a panellist on the topic “Technologies and strategies to detect and counter cyber-attacks across Digital Borders.”

The discussion explored strategies and current policy frameworks for countering cyber-attacks across digital borders. Mr Gaur shared his views about preparing India for counter offensives against cyber warfare in the future. He also talked about reducing India’s dependency on foreign countries for cyber security while strengthening the domestic policy and rules for countering cybercrimes.

IFF IN THE MEDIA

Amit Dubey, Co-Founder, IFF, shared valuable insights on staying safe from cyber frauds on Money9.

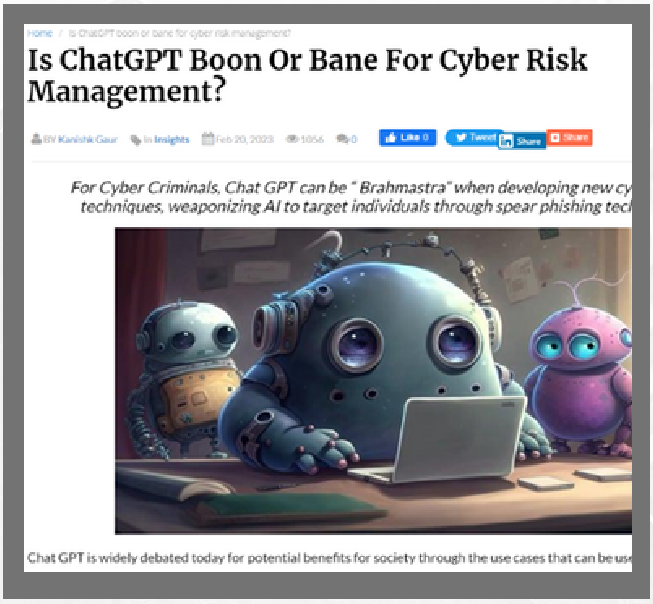


The Fight Against Ransomware: How To Detect And Deter?

BY Kanishk Gaur · In · Feb 22, 2023 · 742 · 0

The most significant risk remains the need for more awareness about cyber security threats

Kanishk Gaur, Founder, IFF, shared his thoughts on the detection and deterrence of ransomware attacks in ITNext.



Home / Is ChatGPT boon or bane for cyber risk management?

Is ChatGPT Boon Or Bane For Cyber Risk Management?

BY Kanishk Gaur · In Insights · Feb 20, 2023 · 1056 · 0

For Cyber Criminals, Chat GPT can be " Brahmastra" when developing new cy techniques, weaponizing AI to target individuals through spear phishing tec

Chat GPT is widely debated today for potential benefits for society through the use cases that can be us

Kanishk Gaur, Founder, IFF expressed his views on ChatGPT in CIO&Leader.

Amit Dubey, Co- Founder, IFF participated in a conference organized by IMA India.

INDIA FUTURE
FOUNDATION

Contact Us

☎ +91-1244045954, +91-9312580816

Building no. 2731 EP, Sector 57, Golf
Course Ext. Road, Gurugram,
Haryana, India – 122003

✉ helpline@indiafuturefoundation.com

🌐 www.indiafuturefoundation.com