INDIA FUTURE FOUNDATION

Freedom of Expression, Trust and Safety on the Internet

NEWS FROM THE INDUSTRY

SINGLE CORE PROCESSOR CRACKS SIKE, A CONTENDER FOR POST-QUANTUM ENCRYPTION CANDIDATE ALGORITHM

National Institute of Standards and Technology (NIST), Gaithersburg, Maryland, United States, in wake of the emergence of quantum decryption held a competition to select algorithms for Post Quantum Cryptography (PQC). The goal of PQC is not only classical decryption but also to resist quantum computing based techniques, in the future. It is believed that in the near future quantum decryption will make the present-day encryption standards like RSA obsolete.

Wouter Castryck and Thomas Decru, researchers from Katholieke Universiteit Leuven, Belgium have cracked this Supersingular isogeny Diffie–Hellman key exchange (SIDH) with their Magma programme, which they ran on an outdated single core Intel Xeon processor, from 2013. It is said that the math behind the algorithm was targeted instead of any vulnerabilities in the code.

The paper showed that Supersingular Isogeny Key Encapsulation (SIKE) was vulnerable to "glue-and-split" theorem. SIKE was developed by researchers from many big companies like Microsoft, Amazon, Linkedin, Texas Instruments and many more. This development came as a blow to SIKE which has now been invalidated but for all methods based on SIDH.

IN THIS NEWSLETTER

CERT-IN ISSUES A HIGH-SECURITY ALERT FOR WINDOWS USERS

The programme that safeguards Windows from viruses, malware, and other threats, known as Windows Defender, may be compromised in some versions of Microsoft Windows, according to an advisory from the Indian Computer Emergency Response Team (CERT-In), an agency under the Ministry of Electronics and Information Technology (MeitY).

The Credential Guard feature of Windows Defender, which comes pre-installed on majority of Windows PCs, poses a security risk to Windows users. The problem that leads to the default is classified as a zero-day vulnerability. This implies that it can only be discovered when it is in use. Due to its ability to spoof and appear to be an authorised user, it has access to the entire domain. This might have very bad consequences for companies and organisations that use domains to administer each computer or account connected to the system as a whole.

TWILIO EXPERIENCES A SERIOUS DATA BREACH

A breach occurred at Twilio (a developer of communications APIs) as a result of an SMS-based phishing attack. Twilio clients Authy, a two-factor authentication app, and Okta, an authentication company, were all unintentional secondary victims of the incident. An attack that looked like it came from Twilio's IT department was specifically aimed at the company's employees.

The attack was designed to trick employees into providing their employee credentials. The stolen information was then used to gain access to Twilio’s internal systems, allowing them to access Twilio’s customer data.

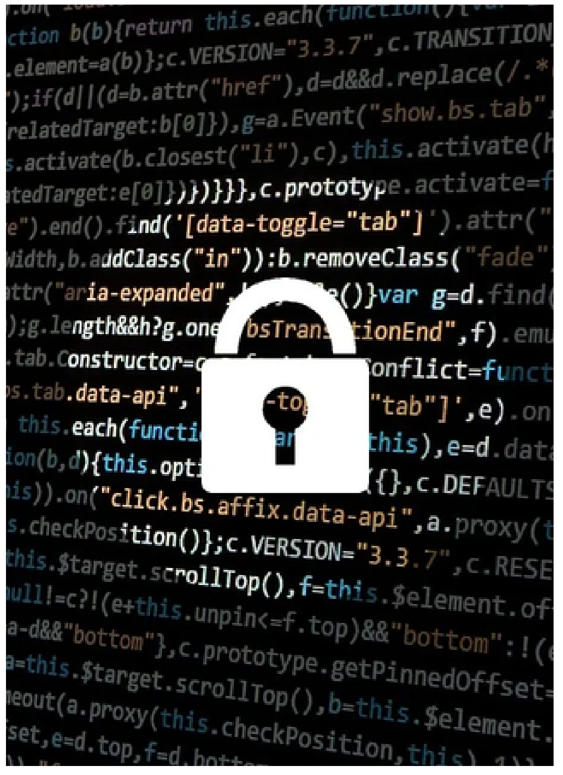
After several employees fell for the SMS phishing attack that gave threat actors access to internal systems, Twilio reported that they had been infiltrated. Threat actors might have had access to data of 163 Twilio customers, and they could have utilised that data in additional supply-chain attacks.

A JAVASCRIPT BUG SCANNER USING GRAPHS FINDS MORE THAN 100 ZERO-DAY FLAWS IN NODE.JS FRAMEWORKS

A graph-based code analysis tool that was created by researchers at Johns Hopkins University, Baltimore, United States of America, found a variety of JavaScript software vulnerabilities.

The tool, known as ODGen, was demonstrated at the Usenix Security Symposium, at Boston, this year and tackled some of the issues that prevented the adoption of graph-based security tools for the analysis of JavaScript applications. Applying ODGen to thousands of Node.js libraries allowed the researchers to demonstrate the tool's usefulness by finding 180 zero-day vulnerabilities and 70 Common Vulnerabilities and Exposures (CVEs).

Graph-based scanners analyse source code files to create a graph structure that describes an application's many attributes and execution paths. The source code vulnerabilities can then be modelled using this graph.

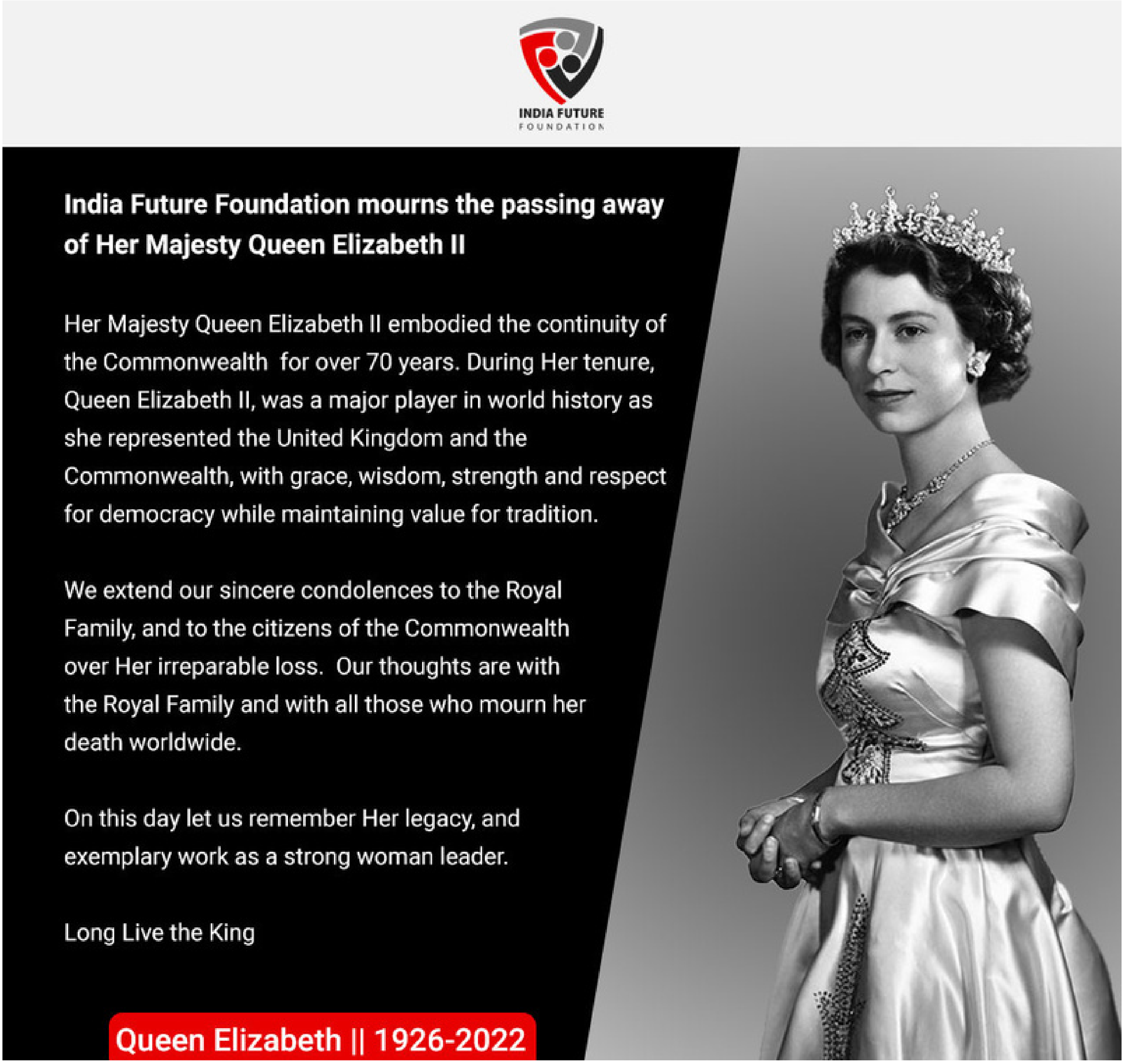


GITLAB FIXES A SERIOUS REMOTE CODE EXECUTION FLAW

GitLab released a security update to fix a serious vulnerability that might result in remote code execution (RCE). According to a GitLab advisory, the flaw might allow a logged-in user to execute the code remotely using the "Import from GitHub API" endpoint. The security flaw, identified as CVE-2022-2884, affects GitLab Community Edition (CE) and Enterprise Edition (EE) versions between versions 11.3.4 and 15.1.5. It also affects all versions beginning with 15.2 before 15.2.3, and all versions beginning with 15.3 before 15.3.1.

Since the releasing the security patch, GitLab has been urging all users to download the most recent version. This means all GitLab installations should be immediately upgraded to one of these versions because they contain critical security patches. The fixed version is currently running on GitLab.com, according to the blog post. Through HackerOne's bug bounty programme, it was reported to GitLab by 'yvvdwf'.

THE END OF AN ERA



INDIA FUTURE FOUNDATION

India Future Foundation mourns the passing away of Her Majesty Queen Elizabeth II

Her Majesty Queen Elizabeth II embodied the continuity of the Commonwealth for over 70 years. During Her tenure, Queen Elizabeth II, was a major player in world history as she represented the United Kingdom and the Commonwealth, with grace, wisdom, strength and respect for democracy while maintaining value for tradition.

We extend our sincere condolences to the Royal Family, and to the citizens of the Commonwealth over Her irreparable loss. Our thoughts are with the Royal Family and with all those who mourn her death worldwide.

On this day let us remember Her legacy, and exemplary work as a strong woman leader.

Long Live the King

Queen Elizabeth || 1926-2022

IFF SIGNS AN MOU WITH KERALA POLICE

IFF has signed an MOU with the Kerala Police. Under this partnership, IFF will train law enforcement officers, in the state, especially on ways to use advanced tools, that will especially empower them in solving cyber related crimes. Such efforts will also help them make Internet a safer place for citizens, especially in the state of Kerala.

KOOTTU

The Kerala Police in association with Meta, which works at the forefront with law enforcement agencies, to promote digital safety for students and children, and Kailash Satyarthi's Bachpan Bachao Andolan (which believes in the safety and rights of children), came together to launch project “KOOTTU” to spread awareness about the need to care for children against online abuse.

The project was also supported by Child Line, Maklab Innovations, Indian Medical Association, Inker Robotics, Bodhini, Kerala Cyberdome, and Counter Child Sexual Exploitation Centre (CCSE) of the Kerala Police.

The week-long event was inaugurated by the Hon’ble Chief Minister of Kerala, Shri Pinarayi Vijayan, and the event was held on the 26 July at 09.30 am, at Cotton Hill Girls Higher Secondary School, Thiruvananthapuram, Kerala. As a civil society implementation partner, India Future Foundation (IFF) assisted with the implementation of this project in selected districts, across Kerala, to spread awareness about cybersecurity. Mr Amit Dubey – Co-founder, IFF, had an interactive training session with the students at the KOOTU event to educate and empower them in maintaining digital hygiene Other prominent figures at the event included Shri P Prakash IPS, Inspector General of Police, South Zone, Thiruvananthapuram; Shri Jeevan Babu IAS, Director of Education-Department Jagathi, Thiruvananthapuram; Shri Rakhi Ravi Kumar, Counsellor, Vazhuthacaud; Shri Vijay Pamarathi, Trust and Safety Manager, Meta; Shri Vincent, Principal, Cotton Hill Girls Higher Secondary School; Smt Nishanthini IPS, Deputy Inspector General of Police (DIG), Thiruvananthapuram Range; and Ms Manmeet Randhawa, Head-Corporate Communications & Strategic Alliances, IFF.

HON. CHIEF MINISTER
POLICE
STATE LEVEL INAUGURATION OF
PROTECTING CHILDREN IN CYBERSPACE

CYBER MANTHAN

IFF, in association with Microsoft, conducted an exclusive session on 'Securing India's Cyber Space from Emerging Threats' from the perspective that ensures strengthening security positions to protect, the MSME's in India, against cyber attacks.

In this session, the current situation, in the country, was analyzed and the following points were discussed. Securing India's Cyber Space from Emerging Threat Vectors

- Cyber vulnerabilities and safeguards during cyber-warfare
- Future of cyber-warfare
- What could India do to secure its critical infrastructure from emerging cyber threat vectors?
- How to strengthen the security position to protect against cyber-attacks?

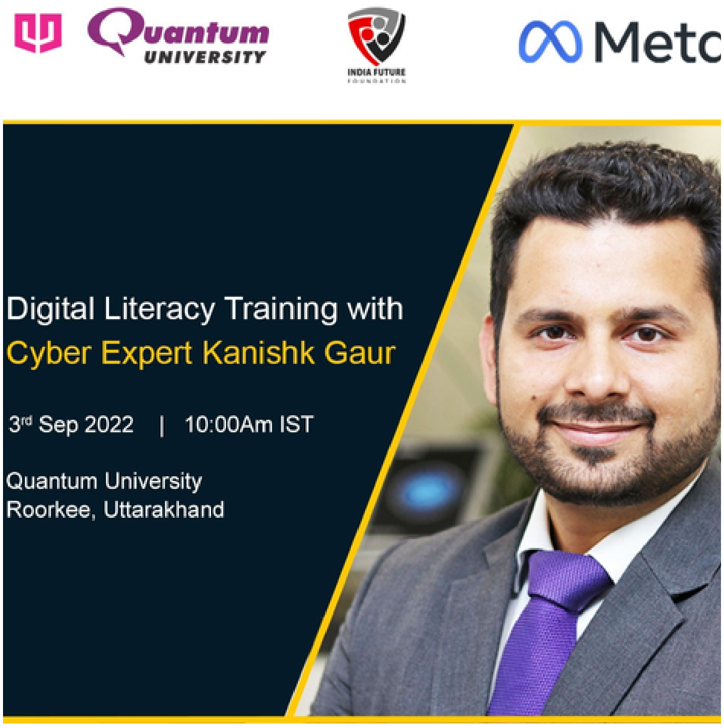
The time has long gone when people in the management didn't realize the importance of security, and security professionals needed to convince them to implement security measures. Now security is not an additional cost of doing business but a necessary investment for most organizations.

Through this consultation, IFF intended to highlight the need to secure and safeguard India's future digital ecosystem and provide a concrete solution to tackle the emerging threat vectors.

TRAININGS PROVIDED

DIGITAL LITERACY PROGRAMME AT QUANTUM UNIVERSITY

IFF in association with Meta Platforms and Quantum University, Roorkee, Uttarakhand, launched the 'Digital Literacy Programme' with the aim to educate children on how to protect themselves from technology-related crimes. The launch was done at Quantum University where students from different schools participated in the program. Cyber experts from IFF conducted an interactive session for students, teachers, and all attendees about cyber awareness and digital safety.



Digital Literacy Training with
Cyber Expert Kanishk Gaur

3rd Sep 2022 | 10:00Am IST

Quantum University
Roorkee, Uttarakhand

Mr Amit Dubey – Co- founder, IFF, interecting with students during training session at the KOOTU event. For more on the KOOTU event please see OUR PROGRAMMES (Page no 05).

HOW PEDOPHILES, DRUG TRAFFICKERS AND MONEY LAUNDERERS USE THE INTERNET

IFF conducted a training workshop, in Guwahati, for law enforcement officials, on social media crimes, money laundering, drug trafficking, and paedophilic use of the Internet. The session was conducted in association with the United Nations Office on Drugs and Crime (UNODC). At the training, law enforcement officials were educated on cryptocurrencies and the dark web function so as to empower them to stop drug trafficking and paedophilic activities, that happen there. They were also trained for tracking cryptocurrencies at the training programme.

The dark web is not accessible with normal browsers, and it needs a special browser called TOR. The dark web houses plenty of illegal activities like drug dealings, weapon dealings, contract killing, and selling paedophilic material as well as red rooms where they torture people or animals with cruelty and sell it to interested people.

Training on different types of attacks like phishing, vishing, whaling, malware, and ransomware were also included.The training programme was attended by six Assistant Commissioners of Police (ACP), 43 Sub-inspectors, 10 crime branch officers, five criminal investigation department (CID) officials and one official from the Himachal Pradesh Nasha Nivaran Board (HPNNB) officer. The presiding guest at the training programme was Shri Harmeet Singh IPS, (Commissioner of Police, Guwahati).

SCAMMERS USING NEW WAYS TO SCAM PEOPLE

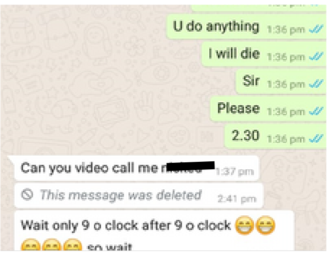
IFF launches a report on consumer frauds on social media. Though social media is a modern phenomenon, it has transformed the way customers seek information, engage with one another, and interact with businesses.

Social media is the most common/preferred way to stay in touch, in these times and especially during the lockdowns that were the order of the day, during the Covid-19 pandemic. Social media platforms such as Facebook, Twitter, WhatsApp, and Instagram have approximately 4.70 billion active users, globally, with numbers increasing at a rate of one million every day. Social media played a key role in helping families and friends stay connected through these stressful times. This also meant that social media was a huge repository of consumer data and the world became more digital due to the Covid-19 pandemic. While being connected to social media has its benefits, there are some negatives as well. Over the years, fraudsters have also started to make the most of social media and this has meant a rise in social media frauds. Social media scams have been around for long, and fraudsters have adapted their modus operandi to exploit, the social media, more so during the pandemic.

Because of the extensive usage of social media, fraudsters have many options to contact consumers and conduct fraud using various methods. Scammers come up with new and inventive ideas to defraud individuals of their money or gather personal information that may be exploited for financial gain. Social media scams can potentially cause significant financial losses, emotional distress, and a loss of consumer confidence. To safeguard customers and minimize harm, immediate action is required.

CHINESE LOAN APPS

Despite the recent banning of hundreds of lending apps, fraudulent loan applications targeting Indians in the middle class and those who lack financial literacy are once again on the rise. These applications have, in some cases, even harassed or assaulted borrowers to get them to pay back. Ok Cash, Go Cash, Flip Cash, ECash, and SnapItLoan were among the five such applications that Google or Google Play Store removed after being contacted. At least 400,000 to 1 million people downloaded and took loans from these applications during the Covid-19 lockdown. They provided loans at almost 35% rate of interest. Those applications were used to get the contact list and gallery permissions, if the borrower was unable to pay at a given time. There were also instances where the representatives used to mentally assault defaulters by abusing or morphing their family picture into some pornographic content, or by reaching out to member in their contact list. Hundreds of people have so far taken their own lives after falling for these loans. In recent times, more than 15 persons have committed suicide in several states.


U do anything 1:36 pm

I will die 1:36 pm

Sir 1:36 pm

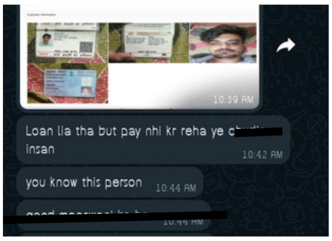
Please 1:36 pm

2.30 1:36 pm

Can you video call me [redacted] 1:37 pm

This message was deleted 2:41 pm

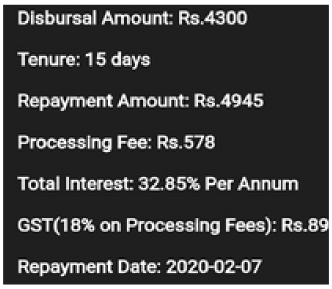
Wait only 9 o clock after 9 o clock 😁😁 😁😁😁 so wait


10:39 AM

Loan lia tha but pay nhi kr reha ye [redacted] insan 10:42 AM

you know this person 10:44 AM

[redacted]


Disbursal Amount: Rs.4300

Tenure: 15 days

Repayment Amount: Rs.4945

Processing Fee: Rs.578

Total Interest: 32.85% Per Annum

GST(18% on Processing Fees): Rs.89

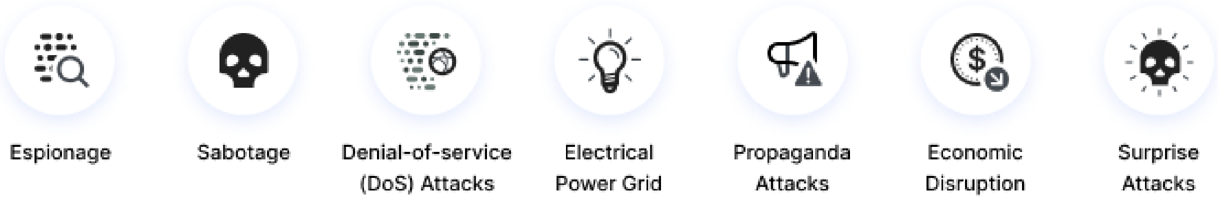
Repayment Date: 2020-02-07

REPORTS PUBLISHED

HYBRID WARFARE

IFF has launched a discussion paper on “Lessons India can take from the first hybrid war,” in light of the ongoing war between Russia and Ukraine. The war between Russia and Ukraine is undoubtedly the first hybrid war that the world has seen. Among other things, this war has taught important lessons, especially to countries, that nations can take cognizance of and, more so, India, considering the peculiar position that India is placed in. This paper invites discussions on the same "Lessons India can learn from the first hybrid war."

Hybrid warfare refers to the combined employment of conventional and unconventional means of force and subversion/coercion to win a war. These instruments or tools are employed in unison, typically discreetly, to exploit an opponent's weaknesses and create synergistic results.



Elaborating on why the ongoing war between Russia and Ukraine, is the first hybrid war, in a press briefing on the cyber-conflict between Russia and Ukraine, Victor Zhora, the deputy head of Ukraine's cyber security agency SSSCIP, had stated that the state (read Ukraine) is engaged in a war both online and on the ground. The ministry (SSSCIP) claims that its infrastructure and Government networks are always the targets of cyber-attacks, with specific individuals also being singled out. It asserted that while its cyber defences repel most attacks, the confrontation with Russia was unprecedented and referred to as a "hybrid war."

India will need to take care of itself in such a situation, if such a situation arises. There will also always be restrictions on India's international security alliances and defence cooperation because it is not a member of any formal security alliance, and it is unlikely it will ever be. As a result, New Delhi will eventually need to define a path based on independence to safeguard and develop its security objectives. Read the paper here.

We seek your inputs on dimensions that must be considered for future hybrid warfare, highlighting the need to secure and safeguard India's future digital ecosystem and provide a concrete solution to tackle the emerging threat vectors. Please click on the below mentioned form to register and share your thoughts, on the matter. Link to Google Form

IFF IN THE MEDIA

SAFE IN CYBERIA
NDTV 24x7
In Partnership with MYN
AMIT DUBEY
NEED OF THE HOUR: DIGITAL TOOLKIT FOR TEENS
2
S AND STANDARDS LAID DOWN BY NE

Amit Dubey, Co-founder, IFF, shared his views on India's cybersecurity in a discussion on NDTV 24*7.

Amit Dubey, talked on the havoc created by Chinese loan apps in India, on NEWS 18.

THE INSIGHTS OF CYBERWORLD
KANISHK GAUR
Cyber Security, Public Policy & Digital Technology Expert

Kanishk Gaur, Founder, IFF, at the workshop, spoke to students, on basics of cybersecurity, web 2.0 security strategies and security threats.

नजानी कॉल बना देगी 'कंगाल'
ZEE उत्तर प्रदेश उत्तराखंड
पी शर्मा
अमित दुबे
आदित्य राठौड़
10 टिप्स बैंक फ्रॉड से बचाएंगे
समय-समय पर ATM कार्ड का पासवर्ड चेंज करें
Hindi News to Home screen

Amit Dubey discussed the new modus operandi of Cyber Criminals on Zee Uttar Pradesh Uttarakhand.

INDIA FUTURE
FOUNDATION

India Future Foundation

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