INDIA FUTURE FOUNDATION

Freedom of Expression, Trust and Safety on the Internet

NEWS FROM AROUND THE WORLD

INDIAN ARMY CREATES NEW SPECIALIST UNITS TO COUNTER CYBER THREATS

The Indian Army has established new specialist units, under its cyber warfare initiatives, to counter rising cyber threats and challenges posed by China and Pakistan. This decision was taken during the Army Commanders Conference held in the third week of April, which was chaired by Army Chief Gen Manoj Pande. The Command Cyber Operations and Support Wings (CCOSWs) have been established to safeguard communication networks and increase preparedness levels in this niche domain.

Cyberspace has emerged an integral part of the military domain in both the grey zone warfare and in conventional operations. The expansion of cyber warfare capabilities by adversaries has made the cyber domain more competitive and contested than ever before. The Indian Army is rapidly moving towards net centricity, which involves an increased reliance on modern communication systems at all levels.

The new CCOSW organisations will assist the formations to undertake mandated cyber security functions to strengthen the

IN THIS NEWSLETTER

cyber security posture of the Indian Army. The army has taken multiple steps in recent years to counter aggression by adversaries in the form of virtual honey trapping and hacking. The Defence Cyber Agency is working at the tri-services level to deal with these issues.

AI-POWERED PASSWORD CRACKERS PUT USER SECURITY AT RISK

A new study has revealed that over 50% of the commonly-used passwords can be easily cracked by artificial intelligence (AI) and that too in under a minute, raising concerns over the safety of personal data. The study, conducted by Home Security Heroes, an online identity security firm, tested 15,680,000 passwords using an AI password cracker called PassGAN. During the test it found that almost 51% of the most commonly used passwords can be cracked in less than a minute. Further the results of the test also revealed that 65% of passwords were cracked within an hour. Additionally, the study revealed that 81% of the passwords could be breached within a month.

The findings of the study will look scary to most, however, the study also noted that the ease of cracking a password depends on the complexity of the password. It has typically been seen that passwords are a mix of characters, symbols, and numbers and those which are at least 18 characters long, take much longer to crack. Passwords containing a combination of symbols, numbers, upper and lower-case letters are the most secure, as it could take up to 6 quintillion years to crack them.

The study emphasizes the need to create strong passwords that are at least 15 characters long, with a mix of characters, symbols, numbers and upper and lower-case letters. It is also advised that you change your passwords every three or six months. Further do not use the same password for multiple accounts.

Experts recommend using a password manager to generate and store complex passwords that are difficult to crack. By doing so, users can better protect their personal information and stay one step ahead of hackers.

PRIVACY AND SECURITY CONCERNS SURROUNDING CHATBOTS

Even though there is no denying the fact that chatbots have become an integral part of our lives, there are also grave concerns about their ability to spread misinformation on a large scale and the existential risks that they pose for humanity. In a recent move, Italy banned ChatGPT on grounds of privacy, as the Italian data regulator voiced concerns about the model used by ChatGPT's owner, OpenAI, and directed an investigation to see if the firm had broken strict European Union’s data protection laws. Chatbots collect vast amounts of data, including text, voice, and device information. That data can reveal information like one's location, IP addresses and so on. While chatbot firms say that users' data is required to improve services, collecting such information can also be used for targeted advertising. In contrast to search engines, chatbots can catch people off guard with their conversational style and encourage them to give away more information than they would have normally entered in a search engine. According to legal experts, chatbots may pose a greater privacy concern than search engines.

It is difficult to use chatbots privately and securely, but you can limit the amount of data they collect by using a VPN to mask your IP address. However, according to experts, the nature of a chatbot means that it will always reveal information about the user, regardless of how the service is used. Tech firms like Microsoft claim that their chatbots are thoughtful about how they use data to provide a good experience. They protect privacy through technology such as encryption and only store and retain information for as long as necessary.

Despite concerns about chatbots mentioned above, they can be useful at work, but experts advise caution to avoid sharing too much and falling foul of regulations such as the EU update to General Data Protection Regulation (GDPR). Companies like JP Morgan and Amazon have banned or restricted the use of chatbots for its staff for this reason. Free chatbot tools for business purposes may be unwise, according to legal experts, as they do not give clear and unambiguous guarantees on how they will protect the security of chats or the confidentiality of the input and output generated by the chatbot. If one has to use a chatbot, experts advise following their company's security policies and never sharing sensitive or confidential information, when interacting with chatbots.

SENSITIVE DATA OF ICICI BANK GETS LEAKED DUE TO MISCONFIGURED SYSTEMS

In February 2023, cybersecurity researchers from Cybernews discovered a misconfigured cloud storage belonging to ICICI Bank, one of India's largest private banks, which exposed sensitive data of the bank and its clients. The leaked data included bank account details, credit card numbers, full names, date of birth, home addresses, phone numbers, emails, passports, IDs, Indian taxpayer identification numbers, bank statements, filled-in know-your-customer forms and the employee CVs.

Despite the Banking, Financial Service and Insurance (BFSI) sector being a "Critical Information Infrastructure," the bank failed to ensure the security of its crucial data, putting both the bank and its clients at risk. If malicious actors accessed the exposed data, the company could have faced devastating consequences.

Cybernews researchers assert that access to the Digital Ocean bucket belonging to ICICI Bank was fully restricted on 30 March, after they reported the issue to the bank and Indian Computer Emergency Response Team (CERT-In). it needs to be noted that there has been no official comment by the Bank on the matter.

RBI ASSESSES FULLERTON INDIA CREDIT COMPANY'S SYSTEMS FOLLOWING ALLEGED DATA BREACH

Officials from the Reserve Bank of India (RBI) visited the Fullerton India Credit Company's main office to assess the non-bank finance company's (NBFCs) systems and its response to an alleged data breach. The incident was reportedly disclosed to relevant stakeholders and Fullerton India has been working with its in-house teams and global experts to confirm the incident and evaluate any potential threat assessment. According to reports, the Lockbit 3.0 ransomware group had demanded a ransom of Rs 24 crore by April 29 to avoid the release of 600 GB of sensitive customer and company data. The RBI team will investigate the incident to determine how Fullerton India's systems were hacked, how long the leak went undetected, and the response once the leak was detected. Fullerton India Credit Company provides working capital loans for small and medium-sized enterprises, among other lending products.

RBI ISSUES NEW NORMS FOR OUTSOURCING OF IT SERVICES BY BANKS AND NBFCS

The Reserve Bank of India (RBI) has released detailed guidelines for outsourcing of IT services by banks, NBFCs and regulated financial entities to ensure that such arrangements do not undermine their responsibilities and obligations to customers. The 'Master Direction on Outsourcing of Information Technology Services' aims to provide effective management of attendant risks. The norms will take effect from 1 October 2023, giving entities sufficient time to comply with the requirements. According to the RBI, the underlying principle of these guidelines is to ensure that outsourcing arrangements do not impede effective supervision by the Central Bank and that outsourcing should neither impede nor interfere with the ability of the regulated entities to effectively oversee and manage their activities. The guidelines also require regulated entities to evaluate the need for outsourcing of IT services based on comprehensive assessment of attendant benefits, risks and availability of commensurate processes to manage those risks.

USE OF AI CHATBOTS IN JOB APPLICATION PROCESSES

The AI-powered chatbot, ChatGPT, has gained immense popularity since its launch due to its ability to efficiently meet user demands. Recently, a Reddit user shared his experience of using ChatGPT to apply for jobs and create personalized CVs according to job postings. The user gave his CV and job description to ChatGPT, that adapted the CV to fit the person specification for the role and provided exemplary answers to the interview questions. The user reported receiving numerous interview invitations after using ChatGPT's services to create their CV.

While using ChatGPT for writing resumes can yield great results, it is important to note that AI-generated CVs have limitations. A human-written CV can showcase a person's personality and communication skills, which can be challenging for an AI chatbot to replicate. Therefore, job seekers should use ChatGPT's services as a supplement to their own efforts in creating a well-crafted CV. ChatGPT can provide guidance and suggestions, but the individual should ensure that his/her CV is a true reflection of their skills and experiences. It is also advisable to proofread the CV for any errors or inconsistencies before submitting it.

INDONESIAN HACKTIVIST GROUP TARGETS 12,000 INDIAN GOVERNMENT WEBSITES

The Indian Cybercrime Coordination Centre (I4C) recently issued an alert, warning of a cyberattack by an Indonesian "hacktivist" group that has allegedly targeted 12,000 government websites, in India. According to the alert, the group has been launching denial of service (DoS) and distributed denial of service (DDoS) attacks on state and central government websites. The alert also revealed that the group had released a list of government websites it plans to target.

The Government of India had recorded 19 ransomware attacks against various government organisations, in 2022, which is almost triple the number recorded in the previous year. In 2021, a Malaysian hacktivist group targeted websites of the Government of India over comments made against Prophet Muhammad, including the website of the Indian Embassy in Israel and National Institute of Agricultural Extension Management, an autonomous extension and agribusiness management institute, in Hyderabad.

To secure its websites, the government released the Guidelines for India Government Websites (GIGW 3.0), providing guidelines to officials on how to safely develop, maintain, and manage government websites, portals and mobile applications. The guidelines recommend encrypting passwords, ensuring software and plugins are up-to-date and limiting website backend access to high-level employees with experience in handling website security. The Government of India’s alert and guidelines emphasize the need for continuous vigilance and cybersecurity measures against increasing cyber threats targeting government organisations.

MUMBAI POLICE ARREST TWO FOR CYBERCRIME IN JHARKHAND'S NAXAL-OCCUPIED REGION

On 09 April 2023, the Mumbai Police arrested two people in connection with cybercrime in Jharkhand's naxal-occupied region. The accused allegedly stole INR 1.5 lakh from a victim by sending him a fake link disguised as an electricity bill payment. The victim reported the incident to Mumbai's Gamdevi Police, stating that he lost INR 1,49,964, which he had been saving for his wedding, after receiving a text regarding his electricity connection. According to the police, the victim received a message on his phone stating that his electricity connection would be disconnected if the bill amount was not paid that day. The message included a payment link, which the victim clicked and lost INR 1.50 lakh.

The two accused have been booked under sections 420 of the Indian Penal Code and 66C and 66D of the Information Technology Act, 2000. Previously, three men were arrested in a different cybercrime case, in Jharkhand. This incident highlights the need for increased awareness among the public about the dangers of cybercrimes and the importance of being vigilant against such fraudsters.

POLICE RECOVER INR 2.79 CRORE SIPHONED OFF FROM VICTIMS' ACCOUNTS IN SIX MONTHS

The Cybercrime Investigation Cell of the Union Territory of Chandigarh police recovered around INR 2.79 crore siphoned off from victims' accounts in nearly six months. The police also seized an SUV purchased from the cheated money and recovered Rs 8.50 lakh, in cash. The police claim that if victims approach them within the "golden hours" of the crime, the money lost can be recovered in a majority of financial fraud cases.

According to a police official, instances of cybercrimes have increased manifold among gullible people, who have lost their hard-earned money. However, reporting the incident without delay can increase the chances of recovery. The police have also warned people to refrain from clicking suspicious links and responding to calls and messages from unknown numbers. In case of cyber frauds, immediately call '1930' or '112' and share the transaction details. It can help block money before it lands in the hands of the fraudsters. The key takeaway from the police's advice is that if people approach them immediately after being defrauded, there is a good chance that the money can be recovered.

IP UNIVERSITY INTRODUCES NEW COURSE ON CYBER SECURITY

Guru Gobind Singh Indraprastha University (IP University), Delhi has recently launched a new course on cyber security. The university aims to equip students with the latest knowledge and skills in this field.

According to a statement by the Delhi government, the cyber security course, aims to equip students with the knowledge and skills to identify and prevent cyber threats and attacks.

The launch of the new course is part of the university's commitment to providing students with the best quality education and exposure to the latest trends and practices in their respective fields.

GENESIS MARKET, A LARGE ONLINE MARKET FOR STOLEN DATA, BUSTED

European Union Agency for Law Enforcement Cooperation (Europol) recently announced that the international police had taken down one of the largest online markets for stolen identities and account details called “Genesis Market.” The operation, dubbed "Operation Cookie Monster," involved 17 countries, resulted in 119 arrests and was led by the FBI and the Dutch police. Genesis Market was a dangerous marketplace that sold stolen account credentials to hackers globally and had listed identities of over two million people for sale. The global sweep resulted in action against criminals in countries such as Australia, Britain, Canada, the United States, and in over ten European countries. The market offered "bots" for sale that had infected victims' devices through malware or other methods. Unlike other "dark web" services, Genesis was available on the open web, although it was obscured from law enforcement behind an invitation-only veil. The closure of Genesis Market follows several other cyber crackdowns involving Europol, including the shutting down of Raidforums, a massive online forum that sold access to hacked databases, and the disrupting of the world's most dangerous cybercrime malware tool called EMOTET.

TRADERS' BANK ACCOUNTS FROZEN AS A RESULT OF CYBERCRIME PROBES

Several traders in Kerala have had their bank accounts frozen due to the increasing number of cyber fraud cases, in the area. According to reports, investigation agencies have taken stringent measures to address the issue, leading to frozen bank accounts of traders. It has been learnt that the accounts were frozen as a result of diversion of swindled money to hundreds of other bank accounts within minutes.

The freezing process is not limited to UPI transactions alone, and the accounts of several people who used other modes of bank transactions such as NEFT and RTGS were also frozen.

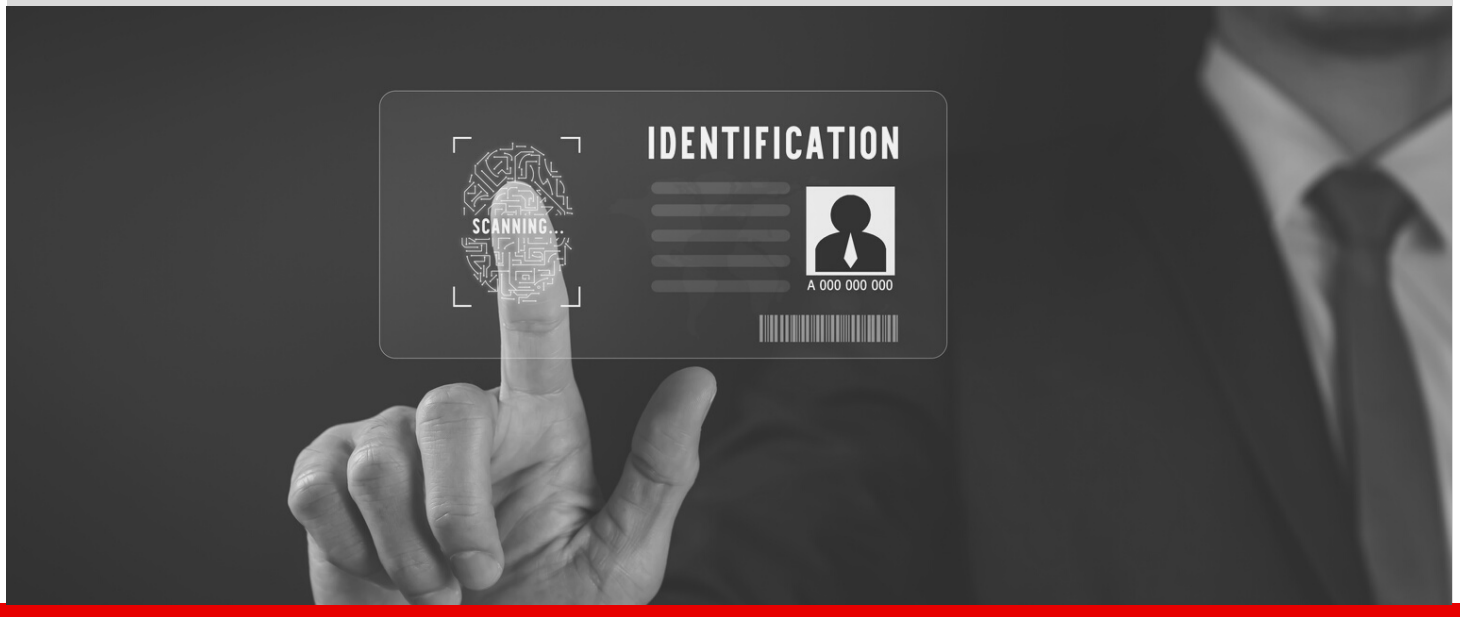
IDENTITY MANAGEMENT DAY

Identity Management Day, which is held on the second Tuesday of April each year, was established by the Identity Defined Security Alliance (IDSA), provides free vendor-neutral education and resources that help organizations reduce the risk of a breach by combining identity and security strategies, in partnership with the National Cybersecurity Alliance (NCA), a 501 USA non-profit organization founded in 2001, that promotes cyber security, privacy, education and awareness. This year it was celebrated on 11 April. This day is aimed at raising awareness about the importance of managing and protecting digital identities. The purpose of this day is to encourage individuals and organizations to take proactive steps towards protecting their online identities.

The management of digital identities is becoming increasingly important as more and more of our daily lives are conducted online. Identity theft, data breaches and other forms of cybercrimes are becoming more common and the consequences can be devastating. Identity Management Day serves as a reminder that protecting our online identities is essential to safeguarding our personal and financial information.

On this day, individuals and organizations are encouraged to take steps to protect their digital identities, such as using strong passwords, enabling two-factor authentication and being cautious when sharing personal information online. It's also a good time to review privacy settings on social media and other online accounts and to update any outdated security software or applications.

Identity Management Day is a chance for users to reflect on their responsibility to safeguard digital ecosystem, whether they are consumers, employees, or partners. It is crucial to recognize that user's online behaviours have consequences. Some of the bad habits that one should refrain from, when online are reusing a password and clicking on a suspicious link can have severe implications not only on our individual lives but also on the corporate networks where they interact. Therefore, while we celebrate this occasion on 11 April 2023, we must prioritize the importance of proper identity management every day.



SYMPOSIUM ON THE DIGITAL INDIA ACT - CRAFTING AN OPEN, SAFE, TRUSTED AND ACCOUNTABLE CYBERSPACE

Mr Amit Dubey, Co–Founder, India Future Foundation participated in a panel discussion at the Symposium on the Digital India Act. The Symposium was held on 21 April 2023 at the India Habitat Centre. It was organized by Cyber Cafe Association of India (CCAOI), which is a trust, with the objective of promoting Internet to the common masses across the nation through the ecosystem of Internet in India, in collaboration with GradeAce.

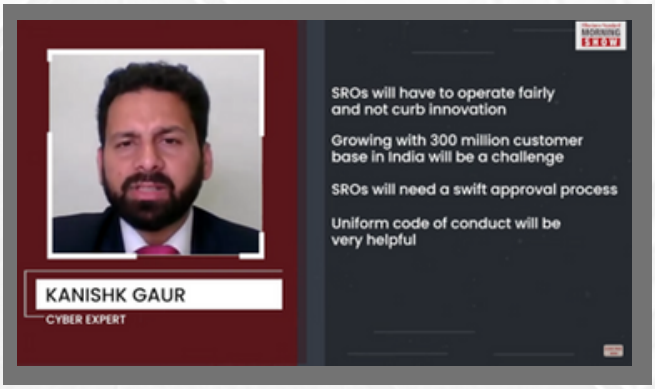
The panel explored establishment of an open, safe, transparent and responsible cyberspace which is based on reliable and trusted Internet. The various roles played by policy, ethical standards and technical regulations are the backbones, based on which the cyberspace can be made accountable. While Open Cyberspace is the need of the hour, it is also vital that there are regulations in place that ensure that safety, trust and accountability of the cyberspace.

The panel emphasised that a concentrated effort by stakeholders, can create a cyberspace that is open, safe, trusted, accountable and that supports the growth and development of our digital economy and society. It requires the development and implementation of effective policies, practices and standards, as well as promoting a culture of responsibility, accountability and ethical behaviour.

IFF IN THE MEDIA

Mr Kanishk Gaur, Founder, IFF writes about in CIO&LEADER about impact of ignoring cyber threats on businesses.

Mr Kanishk Gaur, Founder, IFF shares his opinion about online gaming rules on CNN-News18.



Mr Kanishk Gaur, Founder, IFF shares insights about online gaming rules and its aspects in Business Standard.

Mr Kanishk Gaur, Founder, IFF writes about cybersecurity resilience for the future of businesses in CIO&LEADER.

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