KIET GROUP OF INSTITUTIONS
Connecting Life with Learning
www.kiet.edu
Delhi-NCR, Ghaziabad
Toll Free No.: 1800-1200-106
CELEBRATING 25 YEARS OF EXCELLENCE
CYBER PEACE CENTRE

Volume 1 Issue 2
(Nov-Dec) 2023

CYBER कवच

CYBER PEACE CENTRE

Contents

Edited by :- Aditya Pandey & Vijay Yadav

CYBER PEACE CENTRE
CYBER कवच

Rising Tide of Crypto-Related Frauds Sparks Concerns in Financial Markets

Complied by:- Kartikeya Srivastava
Ex- President CPC

In recent months, the surge in popularity of cryptocurrencies has been accompanied by a concerning uptick in fraudulent activities, leaving investors vulnerable to scams and financial losses. As the crypto market continues to expand, so does the sophistication of fraudulent schemes, raising alarm bells among regulators and industry experts.

Cryptocurrency-related frauds take various forms, ranging from fake initial coin offerings (ICOs) to Ponzi schemes and phishing attacks. Investors, enticed by promises of quick and substantial returns, often fall victim to these deceptive practices.

One prevalent scam involves fraudulent ICOs, where unscrupulous actors create and promote fake projects, enticing investors to contribute funds in exchange for non-existent tokens. Regulators struggle to keep up with the ever-evolving tactics employed by these fraudsters, leading to a growing number of unsuspecting individuals falling prey to such schemes.

Ponzi schemes leveraging the allure of cryptocurrency have also gained prominence. Fraudsters promise lucrative returns by using funds from new investors to pay off earlier ones, creating a false sense of legitimacy until the scheme inevitably collapses, leaving many empty-handed.

Phishing attacks remain a persistent threat, with scammers deploying sophisticated tactics to trick users into revealing sensitive information or transferring their cryptocurrencies to fake wallets. Despite increased awareness, the success of these attacks highlights the need for enhanced cybersecurity measures within the crypto community.

Governments and regulatory bodies are grappling with the challenge of effectively policing the decentralized nature of cryptocurrencies. The lack of a central authority makes it challenging to track and prosecute those responsible for fraudulent activities, leaving investors with limited recourse.

Industry experts emphasize the importance of due diligence and caution when navigating the crypto landscape. Investors are urged to thoroughly research projects, verify the legitimacy of ICOs, and use secure wallets to mitigate the risk of falling victim to scams.

As the crypto market continues to evolve, the need for a comprehensive regulatory framework becomes increasingly evident. Striking a balance between fostering innovation and protecting investors will be crucial in ensuring the long-term viability and integrity of the cryptocurrency ecosystem.

In addition to the rising complexity of cryptocurrency-related frauds, another area of concern is the exploitation of decentralized finance (DeFi) platforms. DeFi, which aims to recreate traditional financial systems without intermediaries, has become a hotbed for scams due to its rapid growth and relative lack of regulation.

CYBER PEACE CENTRE
CYBER कवच

Navigating Ethical Crossroads in Cybersecurity Careers

Complied by:- Aditya Pandey
President CPC

In our increasingly interconnected world, the importance of cybersecurity professionals cannot be overstated. As guardians of the digital realm, these experts are tasked with protecting our virtual landscapes from the constant threat of cyber attacks. However, the pursuit of security in this technologically advanced era is not without its ethical challenges. This article dives into the complex ethical considerations that cyber defenders face in their roles, exploring the delicate balance between safeguarding digital assets and upholding moral standards.

Preserving Privacy in an Era of Surveillance:
As cybersecurity experts work diligently to fortify digital defenses, the question of privacy preservation looms large. Striking the right balance between monitoring for potential threats and respecting individual privacy is a nuanced challenge that requires a deep understanding of both technological capabilities and ethical boundaries.

The Ethics of Offensive Cyber Operations:
With the rise of offensive cyber operations, the ethical use of hacking techniques comes to the forefront. Cybersecurity professionals engaged in offensive strategies must navigate the fine line between protecting their organizations and avoiding collateral damage. The ethical implications of cyber warfare continue to intensify as the digital realm becomes a new battleground for geopolitical conflicts.

Navigating Dual-Use Technologies:
Many cybersecurity tools are designed for both defensive and offensive purposes, presenting a dual-use dilemma. Professionals in this field must be mindful of the broader implications of their work, acknowledging that the same technologies developed to protect against cyber threats could potentially be repurposed for malicious activities.

The Art of Persuasion versus Manipulation:
In the pursuit of securing systems, cybersecurity experts often employ social engineering tactics to identify vulnerabilities. However, the ethical use of these techniques is crucial to prevent manipulation or exploitation. Striking a balance between ethical persuasion and unethical coercion is a delicate task that requires a strong ethical foundation.

Ethics in Collaboration with Law Enforcement:
As cyber threats become more sophisticated, collaboration between cybersecurity professionals and law enforcement becomes imperative. Yet, ethical questions arise concerning the extent of cooperation and the potential for overreach. Finding the equilibrium between effective cybercrime prevention and the protection of individual rights remains an ongoing challenge.

Conclusion:
The world of cybersecurity is not only a technical domain but also one fraught with ethical considerations. As the demand for cybersecurity expertise continues to grow, the ethical dimensions of this field must be at the forefront of education and professional practice. By navigating these ethical challenges with integrity and a commitment to societal well-being, cybersecurity professionals can truly become stewards of the digital realm.

CYBER PEACE CENTRE

CYBER कवच

The Hidden Dangers of APK Modes

Complied by :- Sachin Gupta
Member CPC

APK modes, short for Android Application Package modes, enable users to modify and enhance their apps' performance, appearance, or features. These modes are often used for various purposes, such as unlocking premium features, disabling ads, or modifying the user interface.

Security Risks: APK modes often require users to grant extensive permissions to the modified app, which can lead to security vulnerabilities. When you install a modified APK, you're essentially trusting an unknown source with access to your device, personal data, and potentially sensitive information.

Malware and Viruses: Many APK mode sources are unverified and not from official app stores, making them a potential breeding ground for malware and viruses.

Fig1:- Download the Apk

There are a lot of people who are using modded APKs these days without any thought about the risks that they may be opening themselves up to. While it is true that these modified versions of apps can offer some great benefits, there are also some serious risks associated with their use.

STRUCTURE OF DEEP/DARK WEB

Complied by :- Suryansh Deshwal
Coordinator CPC

To better understand the concept of Deep Web, it is necessary to look at the structure of the internet. The Internet consists of multi-level layers. Content, security and accessibility differ in each layer.

Level 0 (Common Web): It is the layer that makes up the internet we use daily.

Level 1 (Surface Web): Surface Internet. To reach the internet you need to make some simple queries through the search engines. Security cameras servers, Access databases are examples. Temp mail services provide this level of service on sites that provide DNS inquiry services.

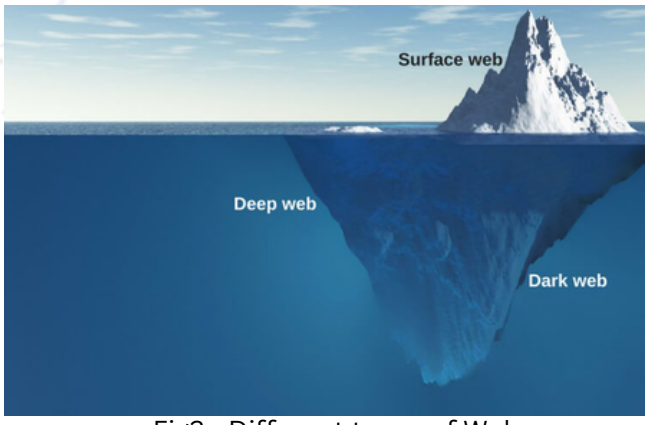

Fig2:- Different types of Web

Level 2 (Bergie Web): Internet only. At this level, there are sites where search engines lock search results, FTP servers, non-indexed adult movies.

Level 3 (Deep Web): Beginner Deep Web Level. Is divided into two.
Proxy Level: It is the level where there are any .onion sites but all kinds of illegal sites. Often they are not indexed by search engines.

Strengthening Your Defenses: Comprehensive Guide to Data Security

Complied by :- **Vijay Yadav**
Coordinator CPC

In an era dominated by digital advancements, the protection of sensitive data has become paramount. Cybersecurity is no longer just an option; it's a necessity. This newsletter aims to unravel the intricacies of data security, providing insights and strategies to fortify your defenses against evolving cyber threats.

Endpoint security is equally crucial, with antivirus software, device encryption, and robust management practices. Develop and regularly test an incident response plan, educate employees on security best practices, and foster a security-conscious culture within the organization.

Regularly back up critical data, maintain physical security measures, and assess and manage third-party vendors for compliance. Stay abreast of regulatory requirements, continuously monitor and audit systems, and promptly apply security updates and patches. Incorporate secure development practices, use encrypted communication channels, and establish policies for secure data disposal.

Data security is not a one-time effort but an ongoing commitment to protect what matters most. By integrating these key elements into your cybersecurity framework.

Fig3:- Strengthening the Security

Use secure communication channels: Encrypt emails and messages containing sensitive information.

Data is the lifeblood of organizations and individuals alike. From personal information to critical business data, safeguarding against unauthorized access, breaches, and theft is imperative. Let's explore key elements of an effective data security strategy.

Securing data involves implementing robust encryption methods to protect sensitive information. Regularly update software and conduct thorough security audits to identify vulnerabilities. Enforce strong access controls, educate employees on cybersecurity best practices, and back up data regularly. Establish comprehensive incident response plans, monitor network activity diligently, and collaborate with cybersecurity experts to ensure a layered and effective approach to data security.

Israel-Palestine cyberwar: Case Study

Complied by:- Indu Shekhar Pandey
Coordinator CPC

Introduction: The Israel-Palestine conflict, a long-standing geopolitical issue, has witnessed not only physical confrontations but has also spilled over into the digital realm, giving rise to a complex and evolving cyber war. Hackers have stepped up efforts to take down the websites of Israeli and Palestinian humanitarian groups since Hamas attacked Israel on Oct. 7. Cyber conflicts among these nations.

Ongoing Cyber Espionage: In recent years, both sides have continued to engage in cyber espionage, with reports of malware campaigns, phishing attacks, and other cyber activities aimed at gathering intelligence and compromising sensitive information.

Significant hacktivist collectives like KillNet and Anonymous Sudan have not only drawn numerous followers but have also significantly inflated this number, leading to considerable disruptions.
KillNet, a pro-Russian hacking collective, justified its actions against Israel by referencing Israel's support for Ukraine in 2022, which Russia perceived as a betrayal and this also applies to many pro-Russian groups.

Anonymous Sudan, highly suspected of having Russian support, targeted Israeli alert systems, claiming responsibility for disrupting Israel's Tzeva Adom early warning radar system and launching a DDoS attack on the Jerusalem Post news service.

Motivations:

1. National Security Concerns: Both Israel and Palestine view cyber capabilities as essential components of their national security strategies. They seek to safeguard critical infrastructure, military assets, and sensitive information from cyber threats.

2. Propaganda and Perception Management: Cyber activities are employed to shape global perceptions and gain support for their respective causes. Both parties utilize social media, websites, and other online platforms to disseminate propaganda, control narratives, and influence international opinions.

3. Espionage and Information Warfare: Cyber espionage plays a significant role in this conflict, with each side attempting to gain intelligence on the other's military strategies, political plans, and internal affairs. Information warfare, including disinformation campaigns, aims to sow confusion and distrust.

Fig4:- Israel and Palestine War

Pro-Palestine Groups	Pro-Israel Groups	Neutral Groups
Hacktivism Indonesia	Anonymous Sudan	KromSec
Sylhet Gang-SG	Gaza parking lot crew	Cyber Army of Russia
Team_insane_Pakistan	Isr@CyberH3ll	Threat Sec
Pakistani Leet Hackers	ICD-Israel Cyber Defence	
Dark Storm Team	Termux Israel	
Team Azrael Angel of Death	Kerala Cyber Xtractors	
Anonymous Russia	Silent One	
User Sec	Garuna Ops	
Anonymous Sudan	UCC Team	
Kill Net	Indian Cyber Force	

Table 1:- Hacker Groups Involved in the Israel-Palestine Conflict

Conclusion: The Israel-Palestine cyber war represents a new dimension in an already complex geopolitical conflict. As technology continues to advance, the potential for cyber activities to play a decisive role in shaping the narrative and outcome of the conflict becomes increasingly significant. The challenge for the international community lies in establishing norms and mechanisms to mitigate the risks associated with cyber warfare in this volatile region.

CyberBytes: "Your Monthly Cybersecurity Briefing"

Complied by
Aryan Sharma and Jhalak Jain
Cooridanator CPC

Chess.com Faces Potential Data Breach: 800K User Records at Risk of Compromise

On 10 November,2023 Chess.com, a leading online gaming platform for chess enthusiasts, is reportedly grappling with a substantial data breach. Over 800,000 user records are said to have been exposed in the incident. The breach, attributed to an individual using the alias 'DrOne,' has raised serious concerns.

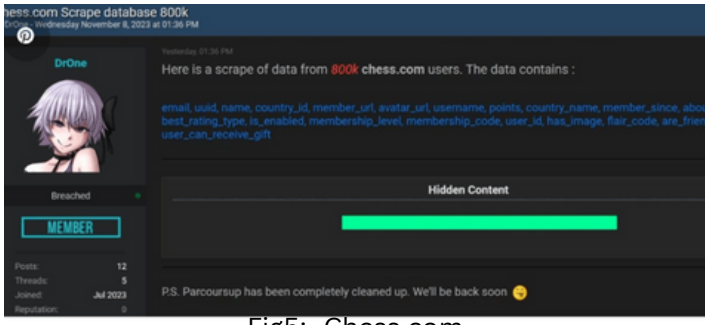

Fig5:- Chess.com

LockBit Ransomware Exposes Gigabytes of Boeing Data

Fig6:- Lockbit Ransomware

The LockBit ransomware group has disclosed data pilfered from Boeing, a major aerospace company specializing in commercial airplanes and defense systems. The leak site operated by the hacker group predominantly features backups for various systems, with the latest ones timestamped on October 22. On October 27, the ransomware actor targeted Boeing, setting a deadline of November 2 for the company to establish contact and initiate negotiations.

Cybercriminals Utilize Microsoft Access Feature to Illegitimately Acquire NTLM Tokens from Windows User

Microsoft Access is a relational database management system developed by Microsoft that allows users to store and manage data. Hackers target it because vulnerabilities in Access can be exploited to gain unauthorized access to databases, compromising sensitive information. Traditional defenses against NTLM attacks, such as blocking outbound traffic on ports 139 and 445, can be bypassed using a new method via MS Access "Access Link Tables." This method enables attackers to target internal users directly by establishing connections to external databases using linked tables.

Fig7:- NTLM Attacks

81.5 crore Indians' personal data leaked, claims hacker

On the dark web, sensitive details of 81.5 crore Indians have surfaced, potentially constituting the largest data breach in India's history. The disclosure was made by a hacker named 'pwn0001.' The compromised information is suspected to originate from data gathered by the Indian Council of Medical Research (ICMR) during COVID-19 testing, although the exact source remains unknown.

Fig8:- Data Leaks

GLIMPSES

Cyber Awareness Month

In Cyber Awareness Month Cyber Peace Centre, KIET Group of Institutions composed an awareness drive inside and outside the KIET campus on 25th October 2023 in which they aware students, faculty members, venders, shopkeepers etc.

Newsletter: Cyberकवच, @kiet.edu

In Cyber Peace Centre, KIET Group of Institutions launched the Cyberकवच Newsletter of Cyber Peace Centre on 2nd November 2023 the Honourable Joint Director, Dr. Manoj Goel presented it to all Kietians through email.

Codefesta Hackathon 2.0, Jaipur

The GIH CODEFIESTA 2.0 Hackathon, is a 24-hour long Hackathon t to build something unique to solve problems from various spheres of modern human life.On 18th-19th October 2023 our club members Aditya Agarwal, Soumya Gupta, Kanishak Joshi and Anurag Chaudhary participated in that and win the hackathon.

Cyber Awareness Desk

In Cyber Awareness Month Cyber Peace Centre, KIET Group of Institutions composed an awareness drive inside and outside the KIET campus on 27th October 2023 in which they aware 150 college students.