OCT 2024

CYBER BYTE

CENTRAL RESERVE POLICE FORCE

Special Edition

Govt. Bans Dozens of illegal Betting App

A new scam, known as **“Digital Arrest“**

Hackers use AI-generated code to infect devices with malware

1.CYBER GEEKS NEWS

A) Govt bans dozens of illegal betting app.

WE'RE CLOSE!
WE'RE GOING TO GET IT THIS TIME!
I CAN FEEL IT!
YOU'RE BROKE- LET'S GO HOME
$
CASINO
ROCKFORD
QUAST © 2012 ROCKFORD REGISTER STAR

Government has banned over two dozen websites allegedly laundering money from illegal offshore betting applications that were masquerading as ecommerce and forex trading portals, following investigations by the Enforcement Directorate (ED).

They include OctaFX, Fairplay, Magicwin, Mahadev Online Book and 30 others, operated by promoters located in Spain, Dubai, Russia and Pakistan. Proceeds of Crime Pegged at ₹10,000 crore

The ED probe found multiple companies were created in the name of fake ecommerce websites and current accounts were opened in the name of these fictitious shell companies. Forex trading websites were also floated for the purpose of routing the proceeds of crime.

Suggestions.

Before downloading any betting software, it's crucial to ensure its reliability and trustworthiness through thorough research.

It's essential to verify that the betting app you're considering is authorized and regulated by a reputable governing body in your jurisdiction.

Exercise caution when you receive unsolicited texts, emails, or social media messages promoting betting apps or claiming that you've won prizes.

Before committing to a betting app, it's essential to thoroughly review the terms and conditions provided by the platform.

B) A new scam, known as "Digital Arrest"

Digital (house) arrest is the virtual restraint of individuals, a tactic cybercriminal use to trap victims in their homes and defraud them. The scammers use AI-generated voice or video calls to impersonate law enforcement officials, creating fear by falsely accusing victims of wrongdoing, generally related to their Aadhaar or phone number. They demand money in exchange for closing the case, often threatening the victim with arrest if they don't comply. The victims have to stay on video call until they fulfil their demands. In some cases, criminals claim the victim has received or sent illegal parcels, such as drugs or counterfeit passports. They may also threaten to involve the victim's relatives or friends.

Case study- i.)

A doctor based in Noida lost Rs 60 lakh to a Digital Arrest scam. doctor received a call from fraudsters posing as officials of TRAI, saying that her phone number was being used to circulate illegal obsence videos. She was threatened until she complied to their demands. Before this, scammers posed as police personnel and extorted Rs 83 lakh out of a 72-year-old woman in South Delhi's CR Park.

Case study-ii.)

A group of scammers posing as CBI officers targeted a Lucknow writer-poet and kept him under digital arrest for six hours. Victim received a video call from a man who claimed to be CBI Inspector Rohan Sharma on July 7. The imposter told victim that he was under investigation for a money-laundering case and threatened to arrest him.

The scammer's attire convinced victim that he was a real police officer. While keeping him under digital arrest for six hours, the scammers requested victim to recite couplets by famous poets Mirza Ghalib and Faiz Ahmed Faiz. The scammer promised to release him within 24 hours and said he could avoid jail time by accepting their demands.

How to avoid falling victim to digital scams?

- Be wary of unexpected calls or messages from unknown numbers or individuals claiming to be law enforcement or government officials.
- Never share personal information or payment details with unverified people.
- Don't panic or act impulsively, even if threatened with arrest or legal action.
- Report suspicious calls or messages to the authorities immediately.
- Report these incidents to the cybercrime portal (https:// www. cybercrime. gov.in) or dial the helpline number – 1930.

C) Hackers use AI-generated code to infect devices with malware.

- One of the strongest use cases for today's generative AI models is using them to write hundreds of lines of code in a matter of minutes. However, hackers are reportedly misusing these tools to generate malicious code, according to new research published on Tuesday, September 24. Security researchers at HP found that hackers launched a malicious campaign targeting French speakers. As part of the campaign, the bad actors sought to access and record **victims' screens and keystrokes by infecting their devices with malware known as AsyncRAT.**

THE GOOD NEWS IS YOU'RE HEALTHIER THAN EVER. THE BAD NEWS IS, OUR AI SAYS YOU'LL BE DEAD IN A WEEK.

This malware contained code that was written in VBScript and JavaScript programming languages with the help of generative AI tools, as per the report.

The report by HP's threat security team is significant since it shows that hackers are moving beyond using generative AI to lure victims through phishing attacks.

Defending Against AI-Based Cyber Attacks.

While AI-based cyber-attacks pose a significant threat, there are steps that can be taken to defend against them. Here are some key strategies:

Adopt a layered security approach.

This involves deploying multiple security solutions at different points of your network to protect yourself from a variety of threats. This includes enabling Multi-factor authentication, encryption on data at rest and in transit, and implement firewalls, to name a few.

Implement strong authentication and authorization controls.

This will help to prevent unauthorized access to your systems and data.

Educate your employees.

Awareness training can help employees to identify and avoid phishing attacks and other social engineering techniques.

Stay up-to-date on the latest threats.

Be sure to keep your software and systems up-to-date with the latest patches and security updates.

Develop a comprehensive incident response plan.

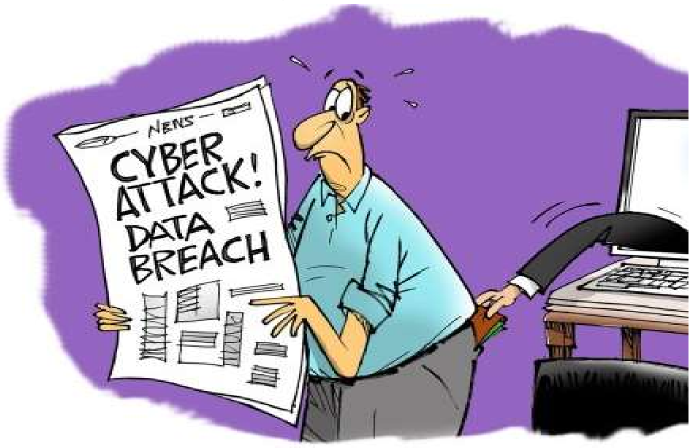
This will help you to quickly and effectively respond to cyber-attacks.

2.CYBER FRAUDS

A) Navi Mumbai Cyber Scams.

Fake police setups, emotional manipulation exploit fear to dupe victims.

Extortion tactics have grown more sophisticated, with cybercriminals impersonating law enforcement officers to threaten "digital arrests" for fabricated charges, cyber expert and head of growth at Bureau ID—a trust network that facilitates end-to-end identity verification, compliance, and fraud prevention for new-age businesses.



The Ministry of Home Affairs and the Indian Cyber Crime Coordination Centre (I4C) have flagged a surge in such scams. In one case, a cyber gang extorted Rs 26.52 lakh from a Ghansoli resident in Navi Mumbai, claiming his name was linked to terrorists. The gang threatened to arrest him on sedition charges. Cybercriminals have wreaked havoc across the country, with Navi Mumbai reporting cyber frauds exceeding Rs 2 crore daily. Over 200 cases have been registered in the past year, involving losses of over Rs 200 crore, according to local officials.

The Ghansoli victim, a doctor, was contacted by the gang on Aug. 26, posing as police officers. They conducted a video call, displaying a fake police setup and convinced him the case was a national security issue. The gang alleged the victim's account was tied to terrorist Yakub Memon and drug trafficking.

Under duress, the victim transferred Rs 26.52 lakh across various accounts, but later realised it was a scam and filed a complaint with the Nerul Cyber Police. The case is under investigation.

Securing Against Emotional Hacks.

Scammers bypass security by exploiting human emotions. While two-factor authentication and phone verification help, they are less effective against social engineering scams like video-based extortion. Jois suggests stronger transaction-level protections, including stricter identity checks, dynamic transaction limits, and real-time fraud alerts. Financial institutions should enhance fraud detection systems and implement risk-based identity verification for sensitive actions to better prevent such scams.

B) Three from Coimbatore held for duping Chennai man of ₹1.15 crore.

The Cyber Crime Wing of Tamil Nadu police on Thursday (September 26, 2024) arrested three men from Coimbatore, suspected to be the key accused in a cyber fraud case, wherein ₹1.15 crore was allegedly swindled from a person in Chennai.

Chennai resident received a call on WhatsApp on August 24 from an unknown person claiming he had a summons from the Mumbai High court. The caller instructed the victim to press '0' for further details. Upon doing so, another impersonator picked up the call, alleging that the complainant was involved in illegal money laundering activities through an ICICI bank account in his name in Mumbai East, Andheri branch, and that he needed to speak with the Mumbai Cyber Crime department.

The complainant, fearing for his safety, transferred a total of ₹1.15 crore through RTGS in five transactions from his two bank accounts.

Following his complaint to the Cyber Crime Wing of Tamil Nadu police, a case was registered. Additional Director General of Police, Cyber Crime Wing, Sandeep Mittal, said, "Our investigation revealed that the complainant's lost amount was transacted to the beneficiary bank account (SBI Account) of Vin Power Energy Solutions Private Limited. A special team was formed to secure the accused involved in the crime and to retrieve the amount lost. The special team has taken swift action by arresting the accused."

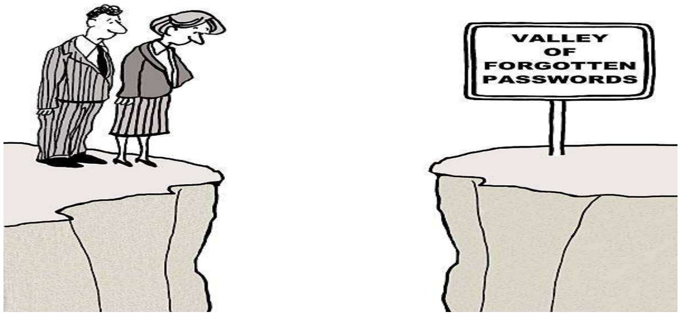
All the three accused were sent to judicial custody, and further investigation is on to arrest other persons involved in the crime.

3. TIP OF THE MONTH

A) Tips for Secure Online Transactions.

- **Change your password regularly.**

For the first time you login to your internet banking account, you will need to use the password provided by the bank. However, you need to change this password in order to keep your account safe.



In addition, keep changing your password at regular intervals. More importantly, always keep the password confidential.

- **Do not use public computers to login.**

JUSTIN, WHERE'S YOUR HOMEWORK?
IT GOT STOLEN OFF THE SERVER BY RUSSIAN HACKERS.

Avoid logging in to your bank account at common computers in cyber cafes or libraries. These are crowded places, and there are more chances of your password being traced or seen by others. If you have to login from such places, make sure you clear the cache and browsing history, and delete all the temporary files from the computer. Also, never allow the browser to remember your ID and password.

- **Do not share your details with anyone.**

Your bank will never ask for your confidential information via phone or email. So, whether you get an apparent phone call from the bank or an email requesting your details, do not give out your login information. Use your login ID and password only on the official login page of the bank, which should be a secure website. Look for 'https://' in the URL when logging in; it means that the website is secure.

I DIDN'T OPEN ONE EMAIL THIS WHOLE MONTH!
CYBERSECURITY TRAINING CERTIFICATE
A+

- **Keep checking your savings account regularly.**

  Check your account after making any transaction online. Verify whether the right amount has been deducted from your account. If you see any discrepancies in the amount, inform the bank immediately.

- **Always use licenced anti-virus software.**

  To protect your computer from new viruses, ensure that you always use licenced anti-virus software. Pirated versions of anti-virus software may be available for free, but they may fail to protect your computer from new viruses prevalent in the online world. In addition, you will get notifications for updates in the software periodically. Make sure that you keep your anti-virus updated, so that your confidential information is always protected.

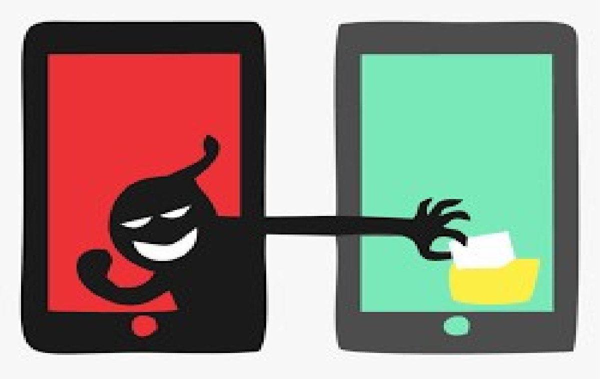
- **Disconnect the internet connection when not in use.**

  Most broadband users do not disconnect the internet connection on their computer when they are not using it. Malicious hackers can access your computer via an internet connection and steal your confidential banking information. To keep your data protected, ensure that you disconnect from the internet when you do not require it.

Type your internet banking URL.

It is a safer to type your bank URL in the address bar of the browser than clicking on links given in an email. There are instances of fraudsters sending emails with fraudulent websites links that are designed exactly like the bank’s original website. Once you enter your login details on such a website, they may be used to access your account and steal your money. While logging on, check for 'https://' in the URL and ensure that it is your bank’s authentic website.

B) MOBILE SECURITY TIPS.



C) 1. Keep software updated.

Software updates not only introduce new features and performance improvements but also patch known security vulnerabilities. Therefore, ignoring these updates can leave your devices vulnerable to cyberattacks. Always keeping both the operating system and installed applications up to date is an essential measure to ensure maximum protection against potential threats.

2. Use strong passwords.

Strong passwords are the first line of defense against unauthorized access to your devices and your data. Avoid using too easy to guess passwords, such as "123456" or "password," as well as obvious and easy-to-find personal dates, such as the user's birthday. The best option is to choose long and unique passwords that combine letters, numbers, and special characters to make decryption more difficult.

3. Activate Auto-Lock.

Automatic device locking is an essential security measure that prevents unauthorized access in case of loss or when the phone is left unattended. Configure the device to lock automatically after a short period of inactivity and set a password or secure unlocking method to unlock it as an additional barrier to protect your privacy and all the personal data the device may contain.

4. Avoid using public networks.

Public Wi-Fi networks are not a safe place for your devices, as they often lack the necessary security measures to protect your information. It is advisable to avoid connecting to unsecured Wi-Fi networks, such as those found in cafes or airports, and even consider using a virtual private network (VPN) to encrypt your data and protect your privacy while using the Internet.

5. Download apps only from trusted sources.

Installing applications from unofficial or unreliable sources can expose you to security risks, such as malware installation or loss of personal data. When looking for new applications, the safest option is to download them only from official app stores, such as Google Play Store or App Store, where the risk probability is lower because applications are scanned and verified before being published.

6. Review app permissions.

" THE TOASTER HAS BEEN HACKED INTO THINKING IT'S A BLENDER."

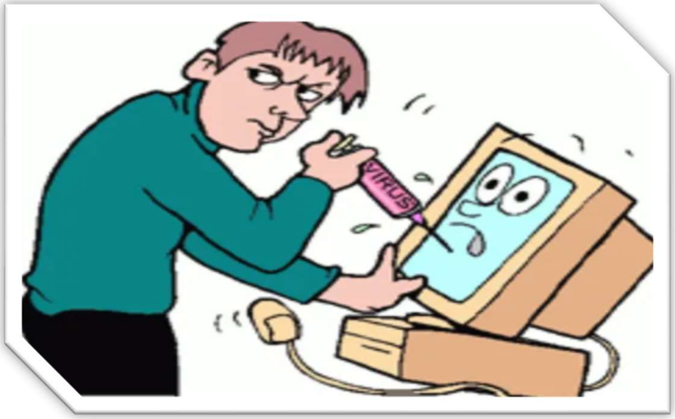
Before installing a new application on a device, it is important to carefully review the permissions requested by that application. It is advisable to disable any additional permissions that are not strictly necessary for the application's operation and consider removing applications that request excessive access to your personal data. Limiting app permissions can help protect your privacy and online security.

7. Regularly backup your data

Regular backups of important data, such as photos, videos, and other documents, are essential to protect them against possible losses or theft of your devices. To make these backups, you can use cloud services such as Google Drive or iCloud, or external storage devices to back up your data regularly and ensure they are protected in case of emergency.

8. Use security apps.

To enhance device security, you can install reliable security applications, such as antivirus and anti-malware, to protect it against known threats such as viruses, malware, and phishing.



These types of applications can scan devices for malicious software and provide real-time protection against malicious websites and potentially dangerous downloads.

9. Enable remote wipe feature.

Activating the remote wipe feature on your device allows you to remotely erase your personal data in case of loss or theft of the device. This can help protect your confidential information and prevent unauthorized access to your data if your device falls into the wrong hands.

D) Online gaming fraud.

online gaming industry has experienced tremendous growth in recent years, with millions of players engaging in immersive virtual worlds and competitive gameplay. Unfortunately, this surge in popularity has also sparked an increase in online gaming fraud. Unscrupulous individuals have sought to exploit the industry through fraudulent activities, leading to financial losses and reputational damage for gaming vendors.

Online gaming fraud apps typically involve malicious software or scams that target gamers, compromising their personal data, financial information, or in-game assets. Some common types of online gaming fraud apps include:

1. Phishing apps: Mimic popular games or platforms to steal login credentials.

2. Malware-infected apps: Hide malware, damaging devices or stealing sensitive information.

3. Fake game mods or cheats: Promise advantages but contain malware or steal data.

4. Scam apps: Promise rewards or in-game currency but require payment or personal info.

5. Keyloggers: Record keystrokes to steal login credentials.

6. Ransomware: Lock devices or accounts, demanding payment.

7. Social engineering: Manipulate gamers into revealing sensitive info.

8. In-game item scams: Fake offers for rare or valuable items.

9. Account takeover tools: Steal or hijack gamer accounts.

10. Fake gaming platforms: Unofficial platforms distributing malicious games.

E) Suggestion avoid falling victim.

1. Download games from official stores.

2. Verify app permissions.

3. Be cautious of suspicious links or emails.
4. Use strong passwords and two-factor authentication.
5. Monitor account activity.

6. Keep devices and software updated.

7. Use reputable antivirus software.

8. Research games and developers.

महानिदेशालय
हिंदी दिवस समापन समारोह
2024
(राजभाषा हीरक जयंती वर्ष)
केंद्रीय रिजर्व पुलिस बल

महानिदेशालय
हिंदी दिवस समापन समारोह
2024
(राजभाषा हीरक जयंती वर्ष)
केंद्रीय रिजर्व पुलिस बल