ATHENIAN TECH

NEWSLETTER

August 2025

THREAT INTELLIGENCE BY ATHENA

Issue #06

In this Newsletter

From the Editor's Desk

In these times cyber criminals use days of national importance to make their presence felt in a nation's cyberspace. India which even to this day remains one of the countries which faces the brunt of cyberattacks globally has repeatedly witnessed instances of its days of national importance being marred by the evil shadow of cyberattacks, and this year was no different.

Infact the chatter to do something big by cybercriminals, in and around India's 79th Independence Day was seen on chat rooms in different encrypted channels like Telegram, Signal and Atox. Infact these nefarious elements made their presence felt between 14-16 August. During this period Indian institutions and especially those from the critical sector were at the receiving of the volley of attacks that were unleashed by various groups like Red Wolf Team, Team Insane Pakistan and BD Anonymous. By different estimates between that period Institutions in India and more so Indian institutions endured the wrath of around 4,000 cyberattacks. The sectors that were most impacted by these attacks included the critical sectors, education and the private sector. Even High Courts succumbed to data breaches in which confidential information was compromised. As regards the nature of attacks that battered India, the cyber criminals employed a wide array of methods to dampen the spirit of India on one of it's most important day. Some of the prominent methods employed by cyber criminals in their efforts to destabilise India on it's 79th Independence Day included resorting to phishing, website defacements, data breaches and launching DDoS attacks.

Staying with data breaches, attackers infiltrated Salesforce CRM, exposing data of 2.55 million prospective Google Ads customers. AI-driven voice phishing tricked employees into approving malicious OAuth apps. Though no financial or password data was stolen, the scale of exposure was severe. The group ShinyHunters (UNC6040) claimed responsibility, of the attack. In another instance of data being compromised a vishing campaign against a third-party CRM exposed profile data of Cisco.com users. No passwords or proprietary data were leaked, but the attack highlighted vulnerabilities in human vigilance. Cisco shut down access, retrained staff, and tightened monitoring. The motorcycle manufacturer, Royal Enfield, too was allegedly hit by "blinkzk," who encrypted its servers, wiped backups, and claimed a "total lockdown." Though details remain unverified, the incident underscored manufacturing's vulnerability to ransomware and supply chain disruptions. Together, these breaches show that even leading global corporations remain vulnerable to social engineering, third-party risks, and ransomware.

From this issue onwards we have started a new section that deals on cyber frauds. In this issue two instances of digital arrest are also mentioned. These instances show that how this new form of scam apart from causing mental stress to the affected party also causes immense financial losses to them. In both the instances mentioned, in this issue, the aggrieved party lost money to the tune of crores.

As regards the emerging tech trends, in this issue we speak about the DEF CON 33, which was held in Las Vegas in which, cybersecurity professionals highlighted the shift from static defences to adaptive resilience. In the discussions that were held at the conference, AI's double role was a major talking point. On the one point it enabled faster anomaly detection but also fuelled deepfake scams and stealthier attacks. A key takeaway was that trust, ethics, and human judgment remained as vital as technology. Meanwhile, Augmented Reality (AR) is gaining traction across retail, education, healthcare, and field operations. By overlaying digital information onto real-world environments, AR enhances experiences but also expands the surface area for potential exploitation.

In this day and age when technology has permeated into every possible space of individual's life it has also affected our lives in ways that we could have never imagined. To give an idea, 20 years not many in India and even in its hinterland would have even thought of ordering fresh vegetables and getting the same delivered at the address of one's choice in the blink of an eye. These are days, carrying out such mundane tasks, with ease, is just one of the benefits of technology. However, there is also a darker side of this technology and it will bite you and bite you hard especially you are not careful. Its important to remember that for e-commerce transactions to successfully materialise, its important that the money travelling on the Internet highway reaches the destination where it's destined to. The fact that these days we read about so many Internet scams is testament to the fact that even to this day people are not that careful when making online transactions. The DIY section in this issue deals exactly with this issue and even gives some suggestions which you need to keep heed of so that you stay at an arms length of any online scam. These are simple things, which you need to follow. Its as simple as having a unique password, changing it regularly and enabling multi-factor authentication.

This issue is our sixth attempt towards making the world a safer place. We look forward to your suggestions as they help us improve which will only empower us to keep you the reader better informed. Till we meet again, do keep writing in to us at pankaj.toppo@atheniantech.com. Happy reading, we look forward to your comments and suggestions●

Pankaj Anup Toppo

Was India Under Siege On Independence Day?

Indian institutions and more so those from the critical sector were literally under siege in and around the nation's 79th Independence Day. In and around this historic day and on the momentous occasion of the 79th anniversary of the nation's Independence Day celebrations, the institutions particularly of the Government of India were battered by a volley of cyberattacks largely launched by the nefarious elements who did so what they did primarily as a symbolic gesture of denting India's pride on its most auspicious day, in recent history.

It needs to be mentioned that there was largely a lull in cyberattacks against institutions of the Government of India for most part of H1 2025. The attacks however gained in momentum post the horrific killing of 26 innocent tourists, by armed militants on 22 April 2025, in Pahalgam, in the union territory of Jammu and Kashmir. Post the killing of the innocent tourists, the intensity of cyberattacks against India gained momentum only to reach a state of lull after the announcement of ceasefire between the two nations after India launched Operation Sindoor on 7 May 2025.

While there was a lull in cyberattacks post the declaration of ceasefire, in the days preceding India's 79th Independence Day celebrations, there was chatter in various chat rooms on Telegram which gave the impression that something big was around the nation's 79th Independence Day. The day which the nefarious elements chose to symbolically dent India's pride is not just an occasion of festivity but a proud reaffirmation of India's unity, resilience, and sacrifices. Those groups with calculated intent, devised campaigns that were designed to inflict symbolic damage, disrupt essential systems, and create an atmosphere of fear. More than just cyber offensives, these actions represented an attempt to strike at the very heart of India's identity, pride and morale.

In the weeks preceding the Independence Day, our monitoring teams noticed a sudden spurt in activity on encrypted communication platforms such as Telegram, Signal, and Atox. Hacktivist groups, including the Cyber Jihad Movement, BD Anonymous, Team Insane Pakistan, and individual members of the Allied Muslim Hacktivist Coalition, were seen sharing threats, spreading propaganda, and posting digital posters and warnings. Many of these were circulated on popular public Telegram groups and those linked to the Cyber Jihad Movement. It was apparent that they were planning something big around India's 79th Independence Day celebrations.

What heinous designs were being hatched in the encrypted communications platforms did see the light of day between 14-16 August. For 72 hours, a fresh wave of cyberattacks battered institutions, especially of the Government of India, and more so those part of the critical infrastructure. The sectors that faced the brunt of these attacks were government, defence, BFSI, Healthcare and organisations from the education sector. The period between 14-16 August witnessed over 4,000 incidents, including phishing, fake websites, data breaches, and scams. In all around 100 institutions experienced a direct impact from the Independence Day 2025 cyberattacks.

The coordinated strikes, around the nation's 79th Independence Day underscored a sobering truth— India's adversaries are increasingly relying on cyberwarfare to complement physical hostilities, leveraging symbolic dates to magnify global attention. As Independence Day 2025 demonstrated, the nation now stands in a world where patriotic milestones can double up as digital battlegrounds.

Not The First Time

Scammers targeting, especially critical institutions, is not a new phenomenon. In fact, a pattern of orchestrated cyberattacks has emerged earlier as well around occasions of national importance.

To highlight a recent example, on 15 August 2024, as India celebrated its 78th Independence Day, hacktivist groups targeted government digital infrastructure. Prominent among the organisations which launched the offensive against India included names like "Angel of Death," which even claimed responsibility for breaching the mail server of the State Government of Rajasthan. The group heightened its intimidation tactics by posting a video that appeared to show its control over the compromised email panel and even sent phishing emails to further their campaign.

In a related incident, the pro-Bangladeshi hacktivist group ‘THE ANONYMOUS BANGLADESH’ targeted an Indian Law Association. This group went beyond simply defacing the website and provided backdoor shell access with altered credentials. This illegal access effectively allowed other attackers to exploit the compromised web panel, thereby increasing the threat to the organisation’s data and systems.

Intelligence analysis shows that these attacks were not isolated incidents. Hacktivist groups from Indonesia, Pakistan, Turkey, and even the United States of America took part in these coordinated offensive campaigns. Such multinational involvement emphasises the global nature of cyber threats that coincide with India’s occasions of national importance, highlighting the urgent need for increased vigilance and international cooperation in bolstering cybersecurity efforts.

Pattern of Attack

A review of recent cyber incidents, around 15 August 2025, reveals that the attackers did not act in a disorganised manner. Instead, they consistently adhered to well-defined methods, each with a specific goal. Analysing these attack patterns gives a deeper understanding of not only their objectives, common targets, and operational tactics but also empowers us to be aware of attacks of similar nature. Analysing the pattern of such attacks only augments our cyber security efforts and holds us in better stead in the future.

1. Data Exfiltration and Leaks

The gravest incidents, around 15 August 2025, revolved around pilfering and exposing sensitive data of the organisations that were compromised. Judicial bodies emerged as top targets, with intrusions being reported in the High Court of Andhra Pradesh and the High Court of Punjab & Haryana. In these cases, attackers even claimed access to millions of case records, FIR details, personal information of judges and even Aadhaar data of individuals. Some of the groups to which such attacks can be attributed include names like Team Insane Pakistan, whose explicit goal was to compromise confidential government records and erode public trust.

Critically, the private sector too was not spared. Some of the companies from the private sector which faced the wrath of these cyberattacks included names like NIVED India and Jet Save Tours India, which witnessed data breaches during this period.

2. Service Disruption via DDoS Attacks

Not every attacker is motivated by access to information. Several groups seek to simply disrupt vital services of a particular organisation or an entity. During the period under study, Groups like Red Wolf Team and BD Anonymous orchestrated Distributed Denial of Service (DDoS) attacks on key organisations that form the digital infrastructure, of the country and included names like Digital India portal and Indian Railways. By overwhelming servers with astronomical volumes of malicious traffic, these attacks can paralyse services on which millions depend on. The main objective behind these attacks is to create chaos and dent public trust in essential platforms, primarily of the Government of India, more so in this case.

3. Website Defacements

Website defacement is something which nefarious elements regularly resort to primarily for maximum visibility with minimal technical complexity. Some of the institutions which bore the brunt of the attacks included names like Alipurduar University, Maitreyi College (University of Delhi) and Samastipur College (Lalit Narayan Mithila University Kameshwaranagar, Darbhanga). Especially in case of these three institutions their official webpage was defaced and instead of the information about the institution and the different educational courses it offers, the official webpage carried propaganda or politically charged messages. Similarly, private entities like SLC Partners and SFCF also saw their pages hijacked as digital billboards for displaying the message of the attackers. Though such attacks inflict less direct damage, their high visibility serves as a public show of the institution's vulnerability.

4. Exploitation of Application Weaknesses

Some adversaries exhibit deeper technical prowess by exploiting vulnerabilities within applications. In one case, Team BD Cyber Ninja took advantage of exposed file paths in the payroll systems of SSM World. Such penetrations go beyond mere surface defacement, involving detailed reconnaissance and exploitation of "deep" application weaknesses. These actions threaten the ongoing integrity of critical systems and highlight the importance of robust application security.

5. Psychological and Symbolic Operations

Many attacks are timed for maximum psychological impact, most notably around Independence Day. The websites that were defaced displayed slogans like "There is no power on Earth that can undo Pakistan." In some cases, attackers sent fake SMS messages purportedly from the systems of a particular High Court masquerading as "Independence Day greetings." These acts are designed to provoke, intimidate, and shape public perception, proving that the goals of such attacks extend beyond technical damage to include psychological warfare and propaganda.

Overall, these incident patterns underscore the reality that contemporary cyberattacks against India are coordinated, purposeful, and multi-layered, blending technical skill, strategic timing, and information warfare to undermine confidence, siphon data, and project influence.

Why Does India Face the Heat of Such Attacks?

India faces an array of ongoing and multi-faceted cyber-threats primarily from countries who view India as an ongoing target due to various geopolitical, ideological and strategic issues.

Pakistan is a key instigator of sustained cyber hostility primarily due to the historical and ongoing rivalry and territorial disputes, with India. APT36 and similar groups work within or in alignment with Pakistan and regularly target institutions of the Government of India and institutions of the Ministry of Defence. Furthermore, hostile groups sponsor or facilitate malicious domain registrations within sensitive networks to conduct credential harvesting, spear phishing, and long-term intelligence testing. This form of persistent and targeted hostile cyber-attack is intended to erode India's national security and regional advantage.

As regards the source, from where these attacks can be traced, Pakistan tops the tables. This is not at all surprising as the nation (read Pakistan) has gone to war against India on numerous occasions, ever since it was born in 1947, and in all the cases the former was the aggressor. Even in the cyberattacks that have battered institutions of the Government of India and Indian institutions in the private sector, the attacks can be traced to our neighbour. In some cases the attackers could also be traced to countries like Malaysia and those in West Asia. Some actors acting from these regions were motivated to conduct cyber actions out of ideological or sectarian solidarity while others do it purely because of hostility towards India. Some even do it to exploit existing communal and regional tensions, in India. Additionally, states from this region occasionally act as a proxy or safe-haven for hacktivist groups or as a facilitator of technology that continues asymmetric warfare while having the potential for plausible deniability.

At a strategic level, state and non-state and regional actors are constantly attempting to destabilise India by continuing to build internal social and political fault-lines involving propaganda, misinformation and harassment operations.

Their cyber espionage operations are usually concentrated on gathering intelligence and understanding the Indian government, defence and economic sectors.

Impact

As a result of the aligned nature of the cyberattacks, their effects have also cascaded across institutions, businesses and the public sphere in India. The immediate impact of the attacks was seen in the delivery of government services. The intrusion, in this case at two High Courts, in different states meant that the said courts were rendered unavailable for many, and case management systems and communication networks in its jurisdiction were unavailable, contributing to delays in delivery of justice and carrying out routine business of the said courts. The exposure of sensitive records, including personal information of judges and millions of legal documents, led to concerns for the officials involved, and the credibility of individuals and the security of the judicial system eroded public trust.

As financial and reputational impact unfolded throughout the public sector, many private businesses, such as NIVED India and Jet Save Tours India, which were compromised by data breaches. Such incidents lead to substantial erosion of intellectual capital. The fact that some of the defaced websites were also related to educational and social non-profits has further led to embarrassment and public scrutiny of other organisations cyber security readiness.

Additionally, considerable consumer-facing operations, beyond the public sector, were brought down by attacks. DDoS attacks related suppression campaigns caused outages to high-traffic public services, such as the Digital India portal and Indian Railways in India, inconveniencing end-users and amplifying other concerns associated with the resilience of critical components to the nation’s digital infrastructure.

Psychologically, the attack campaigns were able to instil fear, cause anxiety and create uncertainty across the society.

Google CRM Breach Exposes 2.55 million Records

Google recently reported a data breach. In the said breach on 7 August 2025, the contact details and business notes of about 2.55 million prospective Google Ads customers were exposed from its Salesforce Customer Relationship Management (CRM) platform. Although no financial information, passwords or active Ads account data were compromised in this breach, the incident has raised concerns due to the sensitivity of the leaked business data, which included fields like name, email IDs, phone numbers and other business-related information of customers, primarily small and medium-sized businesses.

This breach occurred because a cybercriminal group gained unauthorised access to Google's third-party Salesforce CRM platform. Google uses this platform to manage and improve interactions with prospective Ad customers, primarily small and medium-sized businesses.

The tactics, techniques, and procedures (TTP) of the attackers involved advanced social engineering, notably vishing (voice phishing), where AI-generated voice calls were used to impersonate IT support and deceive Google employees into approving malicious OAuth applications like a fake Salesforce Data Loader. Google confirmed that its core operational systems, including active Ads accounts, Merchant Centre, and Google Analytics, were not impacted by the breach, and customer financial information and account passwords remained secure.

ShinyHunters, an APT group, also known by the alias UNC6040. claimed responsibility, for the breach, and demanded a ransom of 20 BTC (about $2.2 million as of August 2025), later insisting the ransom demand was "just a prank." The group's collaboration with Scattered Spider linked the breach to a broader pattern of social engineering attacks against platforms like Salesforce. Extortion attempts and intimidation are common tactics, sometimes delayed for months after initial access as attackers seek to maximise impact.

Google's Response

Google's Threat Intelligence Group executed a swift impact analysis and mitigation, shutting down the affected Salesforce instance and notifying all relevant authorities and customers. The company confirmed that the attack did not affect customer accounts, Google Ads, or other core systems. Google is now partnering with forensic investigators and tracking UNC6040 for ongoing monitoring and prevention.

Industry Wake-Up Call

The Google Salesforce breach highlights a growing threat vector: attacks through third-party service providers and SaaS platforms. Even the most advanced organisations face risks from sophisticated, psychologically targeted social engineering. Businesses are encouraged to enforce rigorous vendor controls, conduct regular awareness training, and monitor all integrations continuously. This breach ranks among the most significant of 2025, alongside other major incidents impacting high-profile companies.

Data Breach Hits Cisco

Cisco Systems reported a data breach resulting from a sophisticated voice phishing (vishing) attack targeting one of its third-party customer relationship management (CRM) systems. On 24 July 2025, cybercriminals impersonated trusted individuals during phone calls to manipulate a Cisco employee into granting unauthorised access to the CRM platform. This platform contained basic profile information of users registered on Cisco.com, mainly comprising full names, organisation name, physical addresses, Cisco-assigned user IDs, email addresses, phone numbers, and associated account metadata such as account creation dates. Notably, Cisco confirmed that no passwords, authentication credentials, proprietary business information, or sensitive customer data were accessed or compromised during this incident.

The attackers employed social engineering methods primarily through advanced vishing tactics, demonstrating the growing threat of human-targeted attacks against corporate security. By using phone-based deception to bypass technical controls, the attackers were able to exfiltrate data from the cloud-based CRM system before Cisco detected and terminated their access. This incident aligns with a series of recent similar breaches affecting other global companies via third-party SaaS CRM platforms, underscoring the vulnerabilities such platforms face when employee vigilance is compromised.

Upon discovering the breach, Cisco immediately shut down the unauthorised access and launched a comprehensive forensic investigation to assess the scope and impact. Affected users were promptly notified, and regulatory authorities as well as law enforcement agencies were informed in accordance with data protection laws. Cisco also implemented enhanced security measures, including retraining staff on recognising and defending against social engineering and vishing tactics, strengthening access protocols for third-party services, and increasing real-time monitoring of critical systems.

This breach serves as a wake-up call for the industry, highlighting that cyber threats extend beyond technical vulnerabilities into human factors. Organisations must prioritise continuous cybersecurity education of its employees, rigorously audit third-party vendor’s security practices, and fortify defences against sophisticated social engineering attacks.

Royal Enfield Hit by a Ransomware Attack

On 12 August 2025, Royal Enfield, a well-known Indian motorcycle manufacturer with a global reach, was hit by a ransomware attack that was attributed to a cybercriminal “blinkzk.” Royal Enfield, part of the Eicher Motors group, maintains substantial operations in manufacturing, distribution, and service across several countries, making the claimed attack highly disruptive in its scope.

According to underground forum posts, the attacker claimed to have encrypted all corporate servers and wiped available backups, effectively creating what they described as a total “data lockdown.” The initial breach notice stated that the stolen data was being put up for bids, a model commonly seen in double-extortion ransomware campaigns. However, a subsequent update declared that a “bounty was paid” and that the data had been deleted.

Cybersecurity researchers reviewing the claims noted that while the forums contained references to internal systems and potential samples of company data, the full scope of the attack remains difficult to verify independently. This mirrors tactics often used by ransomware groups, releasing partial or unverifiable evidence to maximise psychological pressure on victims and push them towards negotiation.

The actor, “blinkzk,” has become a prominent figure within cybercrime circles, and is allegedly connected to other organised ransomware syndicates. His record of attacks includes significant attacks on multinational corporations across various industries, showcasing both increasing operational complexity and expanding influence in the global ransomware ecosystem.

This recent incident highlights the growing danger for high-value manufacturing and automotive firms, where disruptions can spread across production, supply networks, and customer service. The said breach emphasises on the vital need for having in place resilient cybersecurity measures, backup integrity, and quick incident response to safeguard sensitive data and maintain business continuity amid rising ransomware threats ●

Latest Cyber Scams

Cyber scams have increasingly become one of the major concerns in today's hyperconnected world. While on the one hand as technology permeates into every possible aspect of an individual's life, adding value to it in more ways than one could have ever imagined, there is a darker side, even of these advancements in technology, which like the benefits, which technology brings along, affects individuals negatively in ways that one could have never imagined. Nefarious elements riding on the back of new and evolving technologies, through sophistication, siphon your hard-earned money, in other cases, rob organisations of their confidential data. What's worse is that through employment of such sophisticated tools sinister elements can have a negative impact on the lives of hundreds, if not thousands in the blink of an eye. This section highlights the major frauds that made headlines, in the month gone by. This is our attempt at keeping you, the reader, aware of the latest trends, in the realm of cyber frauds, in the digital world.

Man Loses ₹1.4 Lakh After Calling Fake Blinkit Customer Helpline

On 4 August 2025, a 64-year-old resident of Tolichowki, Hyderabad, fell victim to a carefully planned cyber fraud which involved Blinkit. In the said matter the individual placed an order through the Blinkit application. However when he received the order the said individual was surprised to find that one item from the same was missing. To know the details of the missing item he Googled for the customer care number of Blinkit and called on the first number that the search engine threw up. The aggrieved individual called on the said number, in a move to inform Blinkit about the missing number, but in process got conned.

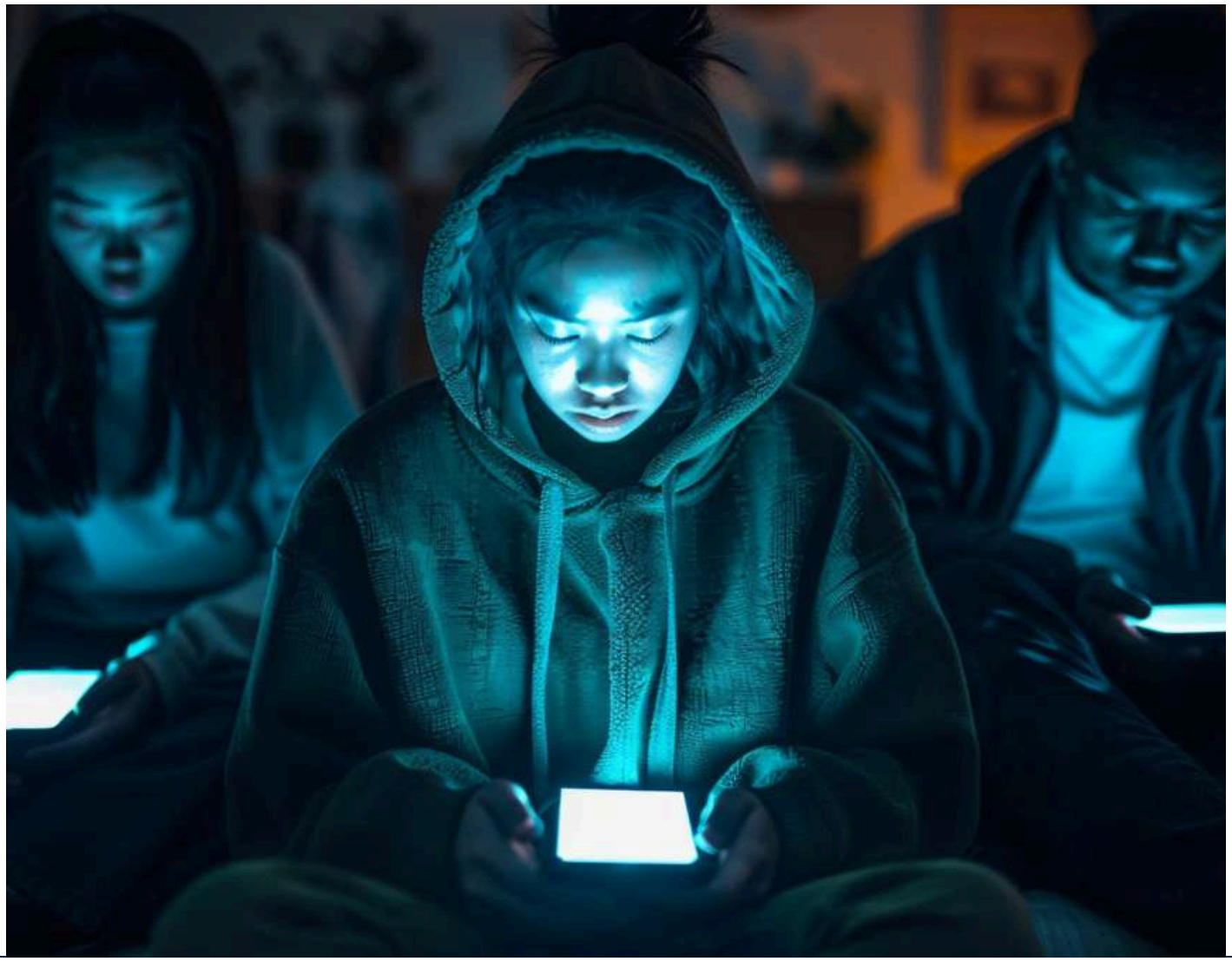
It is worth mentioning that Blinkit on its website (https://blinkit.com/contact) clearly mentions the following, "*Blinkit does not have any official customer care phone line. Beware of fake numbers! For any issues, please use our in-app support only, where we are available.*"

In the process of informing Blinkit about the missing item, from the items that the gentleman had ordered, the said individual lost a huge amount of money. Scammers in a meticulously planned move siphoned off ₹1,40,024 from the said individual's account.

On the face of it this incident showcases how an individual was conned in a harmless process of registering a complaint regarding a missing item from his/her order. However, at the bottom of this scam lay a fake website which contained fake numbers of the customer care numbers of Blinkit. Especially considering the rapid pace at which the world around is getting digitised and more so India is, cybersecurity experts warn that such fake numbers often appear in Google search results because scammers exploit search engines by creating fraudulent websites, abusing Google Business listings, or running misleading ads that rank high in the search results. This results in innocent customers biting the bullet mostly elderly people (primarily due to ignorance) and young children (out of curiosity).

In this case, alarmed by the financial loss, the man immediately brought the matter to the notice of the cybercrime wing of the Hyderabad Police. The police registered a formal complaint and launched an investigation into the matter. Further, authorities have warned the public about such scams, emphasising the dangers of trusting customer care numbers found through unofficial online searches. They have gone ahead and advised consumers to verify contact details, of the organisation before calling, through official applications or websites and to exercise caution when sharing screen access or authentication details over calls or messaging platforms.

This case serves as a reminder of the increasing sophistication of cybercriminals, who use social engineering tactics such as vishing and phishing to exploit unsuspecting individuals. This case also emphasises on the importance of digital vigilance, especially when conducting financial transactions or interacting with third-party customer service channels.



CBI Busts Illegal Call Centre Racket in Nashik

The Central Bureau of Investigation (CBI) has busted an illegal call centre masquerading as that of Amazon in Igatpuri, Nashik, Maharashtra. The raids led to the arrest of five individuals and seizure of a wide variety of assets, including a fleet of luxury cars. Acting on specific intelligence inputs, the agency raided the call centre which ran its operations from a rented property at the Rainforest Resort. In the resort the men behind the fake call centre put together a comprehensive cyber fraud centre, through which they used to con people with ultimate goal being to make a quick buck from the hapless victims. The call centre was used to con unsuspecting citizens primarily from countries like United States of America and Canada. The unsuspecting victims were cajoled into biting the bullet through phishing and misleading calls. Instead of demanding direct cash transfers, the perpetrators instructed victims to pay in the form of gift cards or cryptocurrency, as these channels are harder to trace compared to regular bank transactions.

To sustain the operations, of the fake call centre, the culprits recruited many operators—working in roles such as dialers, verifiers and closers—creating a structured chain of deception. During the investigations, as many as 62 employees were found to be at work, with fraudulent calls in progress targeting foreign nationals. The sophistication of the setup, indicated careful planning and a large-scale execution.

The search operations brought to light 44 laptops, 71 mobile phones, and other incriminating digital evidence. In addition, officials seized unaccounted cash worth ₹1.20 crore, half a kilogram of gold, and seven luxury cars collectively valued at around ₹1 crore. Proceeds from cryptocurrency transactions, including nearly 5,000 USDT valued at approximately ₹5 lakh, and Canadian gift vouchers worth 2,000 CAD, were also detected.

ED Busts Fake Call Centres in Delhi

In a recent move the Enforcement Directorate (ED), in raids at three locations in South Delhi busted call centres that were involved in selling fake software to US nationals. These raids were conducted in the Khanpur area of South Delhi. The searches, which began around 31 July continued well into 01 Aug 2025 thereby underscoring the scale of the operation.

The accused allegedly posed as legitimate vendors of popular products such as Microsoft Windows while in reality they were selling pirated software. The ED which is examining the financial trail, which points to foreign remittances worth nearly ₹100 crore that was routed between 2016–17 and 2024–25. Officials added that the proceeds were part of a broader network of deception designed to exploit unsuspecting buyers overseas.

The Khanpur crackdown highlights not only the global reach of such cyber-enabled fraud but also the painstaking effort required to trace illicit money flows that can stretch across borders and that too for years. Authorities believe the case will serve as a test of India's ability to dismantle financial crime networks that thrive in the shadows of the digital economy.

Retired Couple Endured 11 Days of 'Digital Arrest' and Lost ₹2.4 Crore

A retired couple, from Kerala, both fighting cancer, lost ₹2.4 crore after falling victim to a cybercrime known as “digital arrest.” The matter relates to Kochi, in Kerala, and highlights how technology is used to carry out scams in a novel manner. The primary motive of scammers behind devising new methods, through a heady mix of technology and made up authority, is to instill a sense of fear in the victim with the intention of making a quick buck.

Before getting into the details of the case, it is necessary to get an idea of what a digital arrest scam is. A digital arrest scam is an online fraud in which criminals pose as law enforcement officials (e.g., CBI, income tax, or customs officers) and intimidate victims with false accusations of crimes, such as tax evasion or financial misconduct. These scammers often use fake police station backdrops on video calls, so that they appear credible. The victims, who quite often include retired pensioners, are threatened with a “digital arrest warrant” and are pressured to transfer money to clear their name, for the said case, in which they are falsely accused. Once the money is sent, the scammers disappear, leaving financial loss and destroyed families behind.

Coming to the case, the ordeal for the unlucky couple began 11 a.m. on 10 August 2025, with an unexpected call from an unknown international number. The caller claimed to be calling from the Telecom Regulatory Authority of India (TRAI), India’s telecom regulator. The caller stated that the wife’s telephone number was linked to an ongoing money laundering investigation by the CBI. This was followed minutes later by a WhatsApp video call from a person dressed as a CBI officer, complete with official emblems in the background and a translator who was fluent in Malayalam.

The 'officer' showed a Canara Bank ATM card and claimed that it belonged to the wife, alleging that she had received ₹20 lakh since 2022 as part of suspicious transactions. Despite protests from the wife that she did not have an account with Canara Bank, the callers presented her with her Aadhaar card, convincing the couple of the authenticity of their allegations. From that moment, they were trapped.

The scammers imposed a strict lockdown on the couple. For the next 11 days, the couple was subjected to constant psychological pressure and were virtually held under surveillance through WhatsApp video calls. On 13 August after appearing before a ‘CBI judge’ through video conferencing who confirmed their identity, they transferred ₹50 lakh to a so-called Supreme Court bank account for "verification." In the following days, they transferred further amounts—₹70 lakh, ₹50 lakh, ₹20 lakh, and another ₹50 lakh—totalling around ₹2.4 crore, all from their life savings accumulated through decades of service.

The transfers were dispersed across various banks, including Karnataka Bank, Bank of India, Yes Bank, IndusInd Bank and ICICI Bank. Sensing foul play, a manager from Bank of India questioned the couple about the frequent money transfers but they were coached, by the perpetrators to explain that the money was meant for buying a plot to build a house.

The ordeal came to an end on 21 August when the wife’s younger brother, a retired bank employee residing in Wayanad, grew suspicious of her odd behaviour over the past few days. Upon visiting them, he immediately recognised the scam, took the husband to the bank to halt the last transfer, and even helped lodge a police complaint.

The Kasaragod Cyber Police confirmed that while the final ₹50 lakh transaction was frozen under lien, the majority of the funds had already been dispersed in smaller amounts. The police suspect the scammers operated from Southeast Asia, possibly Cambodia. The couple now hope that their experience will serve as a warning to others.

This incident is one among the many recent 'digital arrest' scams being reported across India, where fraudsters impersonate law enforcement authorities, abduct victims psychologically through fake warrants and video calls, and coerce them into transferring money over days or weeks.

Authorities advise extreme caution when receiving unsolicited calls from supposed government agencies, recommend verifying contacts independently, and caution against transferring money or sharing sensitive information digitally under duress.

Noida Family Loses ₹3.21 Crore in a 'Digital Arrest' Scam

A Noida-based family has been defrauded of ₹3.21 crore in what the police describe as a "digital arrest" scam that stretched for days. The elaborate con, reported by the Noida Cybercrime Police on 22 Aug 2025, combined fear, impersonation and constant surveillance to trap the victims into draining their life savings.

The ordeal began on 25 July when the head of the family received a call from a person claiming to represent the Telecom Regulatory Authority of India (TRAI), India's telecom regulator. The caller alleged that the victim's Aadhaar and mobile number were linked to money laundering activities and even threatened to block his SIM card. Soon after, the family was contacted over WhatsApp by individuals posing as officers of the Mumbai Cyber Crime Branch and the CBI. They told the family that they were implicated in 24 criminal cases.

To heighten the intimidation, the fraudsters used WhatsApp video calls to maintain round-the-clock surveillance. According to the FIR, the family was made to believe that they were to be placed before a Prevention of Money Laundering Act, 2002 court judge through a video link. Under these sustained threats, the suspects instructed them to transfer their funds to what they described as "verification accounts" in order to clear their names.

The Noida family came to know they were victims of a scam when the daughter was allowed to step out, of the house, for some important work after being under surveillance for weeks. She mustered the courage to approach the Cybercrime Branch police station on 22 August. During this visit, she was informed that the calls and video monitoring claiming to be from TRAI, Mumbai Cyber Crime Branch, and the CBI were from cyber fraudsters. The family then disconnected communication with the suspects and filed a formal complaint.

Since 25 July 2025, the family carried out multiple RTGS transactions, with the total amounting to ₹3.21 crore. The episode underscores how cybercriminals are now blending digital platforms to inflict psychological coercion, effectively confining victims to a virtual cage of fear. For the Noida family, what began as a routine phone call transformed into weeks of intimidation, leaving them financially and mentally devastated and highlighting the rising menace of "digital arrest" scams in India's cybercrime landscape ●

DEF CON 33: Inside the Global Hacker Gathering

As cyber threats become AI-driven, the conversation within the global security community is shifting from defending static perimeters to building adaptive, intelligence-led resilience. At the DEF CON 33, that was held in Las Vegas, Nevada, from 7 to 10 August 2025, this shift was more than just being theoretical; it played out in real time through live hacking challenges, deep-technical briefings, and collaborative threat simulations that forced delegates to rethink the fundamentals of detection, verification, and rapid response.

When analysing the core technical content of this year's DEF CON, it is not just the scope that made it stand out. Instead, every discussion carried a sense of urgency. At times, demonstrators moved seamlessly from showcasing AI-enabled deepfake scams to holding detailed discussions of supply chain compromise case studies. However, the underlying theme of the talks converged into one clear message: resilience is less about building thicker walls and more about developing systems that can think, adapt, and recover swiftly. This sense of urgency was heightened, especially since malicious actors actively exploited many of the vulnerabilities that were discussed, at the conference.

The focus on AI and security was hard to miss, filling both formal sessions and casual conversations in the hallways. Experts pointed out that AI can be a double-edged sword: it can quickly spot unusual patterns that humans might miss, but attackers can also use the same technology to sneak past security systems. The talks didn't just cover technology; they also touched on issues of ethics, rules, and the role of humans. A significant concern was whether current identity verification methods, such as biometric checks, can keep pace with AI tools that create convincing fakes. The takeaway was simple: the future of cybersecurity isn't only about building stronger systems, it's about making sure people can continue to trust what they see and use online.

This evolving context highlights a crucial fact: technology alone will not ensure security. The human elements of trust, judgment, and ethics remain central to resilience. While AI is likely to change our threats and defences fundamentally, the global security community can support the development of a holistic environment that combines innovative thinking, strong governance, and ethical commitment. Ultimately, we will view AI as a tool to shift from reactive defence to adaptive, intelligent systems that can foresee threats, respond swiftly, and recover more effectively- aiming towards a society with a digital safety environment.

Augmented Reality

Augmented Reality (AR) is rapidly developing as a transformative technology and is moving beyond simple overlays and filters to provide fully interactive, immersive experiences. Unlike traditional digital content, AR seamlessly integrates virtual objects and information into the real world, thereby enhancing the user's perception and interaction.

AR systems are designed to autonomously recognise environments and context, making smart decisions about what content to display and how to interact with users in real time. This goal-oriented behaviour makes AR highly efficient; for example, it only activates visual elements or instructions that are relevant to the current situation, eliminating unnecessary distractions and focusing on the user's immediate needs.

AR operates by gathering data from multiple sources, such as device sensors, cameras, GPS, and user interactions, to understand the user's surroundings and intentions accurately. Once it interprets the environment, AR engines use reasoning and pattern detection to overlay the right digital content, whether it's navigation guidance, virtual try-ons, educational tools, or interactive visualisations. The system adapts and learns from each interaction, improving accuracy and user experience over time.

Emerging Use Cases and Examples

Today, AR is present in nearly every sector, both tech and non-tech. In retail, AR allows virtual product previews, enabling customers to see how a particular furniture fits in their space or how clothes would look on them before they make the buy decision. In the education sector, AR brings textbooks to life with 3D models and interactive lessons. For field operations and maintenance, AR provides real-time instructions and step-by-step overlays directly on equipment, guiding users through complex procedures.

In healthcare, AR helps visualise anatomy and procedures for practitioners and students. For entertainment, AR creates immersive games and experiences, blending physical and digital worlds. AR also streamlines onboarding and training by overlaying helpful instructions in real-world environments, making complex tasks more accessible.

By automating content delivery, adapting in real time, and continuously learning from user behaviour, AR is not only improving specific tasks but also fundamentally redesigning how people interact with technology and how their interactions are impacted because of their interactions with technology●

In the hyper-connected world that we live in the present day, it will be cliched to say that technology has impacted our lives in more ways than we could have ever imagined even 25 years ago. At the turn of the century, ATM's were slowly making their presence felt. People were slowly getting used to it. During those days, the humble ATM machine was primarily used to withdraw money. Not only the elderly but even the working class was still getting used to it and the naysayers still queued in front of the good old bank teller, which had fixed timings of operation. And then the Internet boom happened and riding on the back of this wave of new technology, Internet banking took off and it was only a matter of time before e-commerce got new wings. Gone are the days when one used to go to the bank teller to withdraw and deposit cash. Even buying household groceries can be ordered from the comfort of your home and then delivered at the address of your choice in a matter of minutes. Behind all this convenience your and our money moves on the Internet highway. For the money to reach the intended destination without any hitch one needs to take certain precautions. Afterall these modern electronic highways are more often than not surveyed by nefarious elements who are on the prowl to subvert your money from the destination where you had sent, to the place where they want to. Below mentioned are some of the practical steps that you should ideally take to protect your money and personal financial data.

Strengthen Password & Access Management

One of the most critical steps in ensuring safety, primarily of your financial data, is to create a unique and strong password and implement access control. This involves generating strong, unique passwords, using a mix of upper- and lower-case letters, numbers, special characters, and symbols. Avoid reusing the same password across multiple platforms. It is also advisable to update your passwords regularly, especially after any breach or if you notice any suspicious activity, in your account. To make secure management easier, you should use a reputable password manager.

Enable Two-Factor Authentication (MFA)

Enabling Multi-Factor Authentication (MFA) adds an extra layer of security to your account. Instead of relying solely on a password, which can be guessed, leaked, or stolen, MFA combines two or more different verification methods. It uses your phone or a security key, along with your biometric information, such as your fingerprint or face as the second key. In present times, you should ideally be using MFA to stay safer online.

Use Secure Networks

Using a secure network is essential for protecting your personal and sensitive data. Wi-Fi networks found in cafés, restaurants, airports, and other public places are often exploited by hackers because they are easy to hack. You should avoid using Internet services, by logging on to such networks. However, if you are in a position where you have to connect to such a network do that through a trusted Virtual Private Network (VPN), as it encrypts your Internet traffic and masks your IP address. This makes it harder for hackers to track or steal your data. Your personal Wi-Fi should be protected with a strong password and use WPA2 or WPA3 encryption standards.

Be Wary of Phishing and Fraudulent Messages

Cybercriminals frequently impersonate banks or payment services via email, calls, or SMS, with the intention of stealing your banking credentials or to trick you into transferring money to them. Be vigilant of messages with such strange looking links, from suspicious numbers or urgent requests for your financial information especially from unknown numbers. Never click on links sent to you from unknown numbers or download attachments from unknown/unexpected sources, and always verify directly with your bank before taking any action.

Check Your Account Statements Regularly

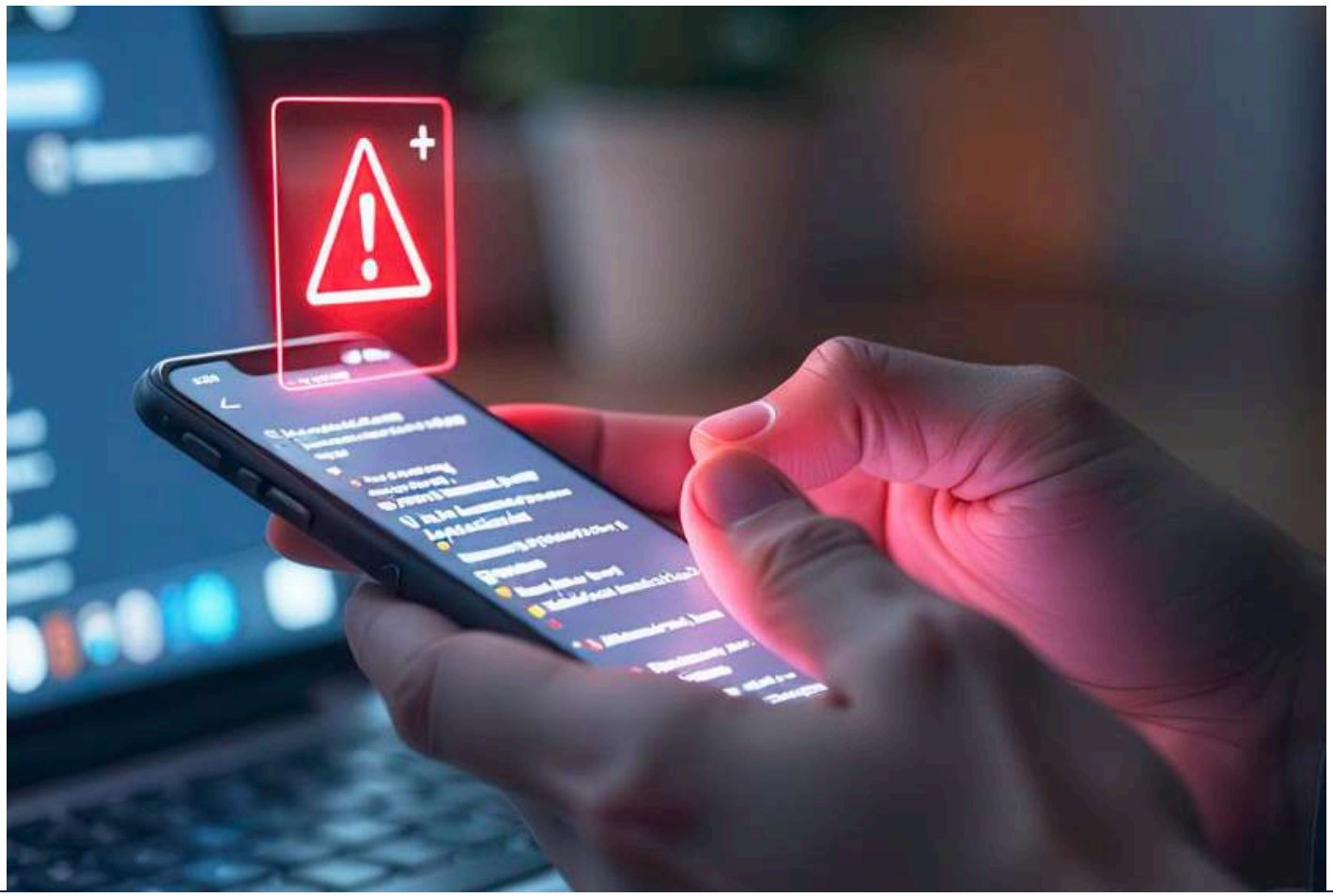
It is recommended that one of the best practices to ensuring your financial security is to check your bank statements and most importantly your transaction history. If you receive a message from your bank alerting you about a transaction which you have not done, inform the bank at the earliest. Bring it to their notice.

Update Software and Apps

For security purposes, you must keep your banking applications, web browsers, and payment gateways up to date. New vulnerabilities are released daily, and as technical issues are discovered, developers release updates and patches to help resolve vulnerabilities. To make it easier for you and to keep it safe, turn on automatic updates so your devices and apps can ensure that versions are up to date and are running the latest version of the software, thereby making it hard for nefarious elements to steal your information.

Do Not Share Your Financial Information

Banks and financial institutions regularly tell their subscribers not to share bank passwords, OTPs or any related information with anyone. Take such messages seriously. They also mention in such messages that banks never ask such information or any related information from their customers. For your own mental sanity, at no cost share any financial information that is yours with anyone ●



Athenian Tech

Contact Us

www.atheniantech.com

https://www.linkedin.com/company/athenian-tech/