ATHENIAN TECH

NEWSLETTER

October 2025

THREAT INTELLIGENCE BY ATHENA

Issue #08

In this Newsletter

From the Editor's Desk

As we have almost reached the fag end of 2025, it makes sense to pause for a while and look back at what has passed by in the major part of the year. In the realm ofcybersecurity, 10 months is a pretty long time, so before we actually bid adieu to 2025, it will be worthwhile to look at what all happened in the major part of this year. 2025 saw it all, from crippling ransomware attacks and state-backed espionage to AI-powered deceptionand deepfake-enabled scams. Incidents of the past prove yet again that cyberspace is the newest and most contested arena of strategic power. This is a space where power games are expected to play out, especially in the future, considering the world is becoming increasingly digitised at a rapid pace.

If one looks back, it can be safely said that we have made rapid and steady strides in bolstering our digital defences through a multi-layered cybersecurity framework. Prominentamong the organisations that stand guard in bolstering the nation's cyber defences are the Indian Computer Emergency Response Team (CERT-In), the National Critical Information Infrastructure Protection Centre (NCIIPC), and the Indian Cybercrime Coordination Centre (I4C). According to the government's own estimate, over 86 per cent of Indian households are now connected to the Internet, which is a positive development, as it provides better governance among other benefits. However, the negative side of this expanded digital landscape also means that the attack surface for the nefarious elements has increased.

To counter the menace of cyberattacks/threats, the government has launched a series of citizen-centric and institutional initiatives, including the National Cyber Crime ReportingPortal, CyTrain, and Sahyog. While these initiatives were launched on the one hand to encourage citizens to report cyber incidents, the broader aim was to bolster national preparedness. Among other things, these initiatives saw more instances being reported. For example, cyber incidents increased from 1.02 million in 2022 to 2.26 million in 2024. The bright side of these initiatives was that they played their part in preventing potential financiallosses exceeding ₹5,489 crore. Amid rising AI-driven deception and supply-chain attacks, India's emphasis on cyber discipline, collaboration, and resilience is key to securing its digital future.

While the institutions of the Government of India facedthe brunt of cyberattacks on two separate occasions for most of 2025, the corporate sector was not spared either.

From the Editor's Desk

In October, Generali Central Life Insurance, formerly Future Generali India Life Insurance (a joint venture between the Generali Group and the Central Bank of India), fell victim to a ransomware attack by the Medusa group, which infiltrated the servers of the company and encrypted critical data and demanded a ransom of USD 500,000 (₹4.2 crore). The matter reached the Bombay High Court, which directed the relevant authorities to take the necessary steps to prevent the spread of compromised files in the ransomware attack, thereby marking this as the first judicial intervention in an active ransomware attack. An investigation into the matter revealed that the breach was the result of a phishing attack. Although sensitive information has been compromised, it has been reported that policyholders' funds are safe. Teams, on the other hand, have been tasked with assessing the violations under the Digital Personal Data Protection Act, 2023.

In a separate incident, in October, a chink in India’s cloud revolution came to light. Researchers at UpGuard discovered an unprotected Amazon Web Services (AWS) S3 bucket, which contained 2.73 lakh bank-transfer records worth nearly ₹380 crore. The database contained sensitive information, such as names, account numbers, and IFSC codes. By the time the access was revoked, web crawlers had mirrored portions of the dataset. India's Banking regulator, the Reserve Bank of India (RBI), and NPCI, India’s umbrella organisation that facilitates services like UPI Payments, traced the data to a third-party reconciliation vendor that had ignored basic security controls, constituting a breach of the Digital Personal Data Protection Act, 2023.

In another incident, in early October, the Indian subsidiary of the German engineering major Klingelnberg Group suffered a crippling ransomware attack by the Black Shrantac collective, which is infamous for targeting European automotive suppliers. In the aforementioned attack, the threat actor group stole 1.1 terabytes of sensitive data, including blueprints and invoices, and demanded $400,000 (approximately ₹3.3 crore) for non-disclosure. However, in this case, the company did not pay the ransom; instead, it restored operations from offline backups after the attack.

This response from the company to ransom demands was widely praised and should serve as the foundation for a disciplined incident response.

Another breach that made headlines in October was the breach at Avnet Inc., a global electronics distributor, which affected the company's EMEA operations. The threat actor, in this incident— known as "Black Phoenix"—leaked the compromised data online.

Although October was the month that witnessed the festivals of Dussehra and Deepawali across the country, like any other month, it also saw a flurry of scams in which the common man was conned. Prominent among the scams that made headlines in October was the "DigitalArrest" scam, which the Maharashtra Cyber Police cracked. In the said scam, fraudsters posing as CBI and ED officials used AI-generated video calls, staged against fake police station backdrops, to extort victims. Equally sinister and devastating were romance-investment schemes. These were also known as "pig-butchering" scams. In this form of scam, a 50-year-old tech executive lost around ₹73 lakh. In the said incident, the scammers posed as financial advisors and lured the tech executive through a dating app into a fake crypto-trading platform, which promised 20 per cent daily returns. In a major step towards combating such scams, authorities from the U.S. and the U.K. dismantled a massive cyber-fraud network linked to Cambodia's Prince Holding Group, which is accused of orchestrating global "pig-butchering" scams, in a major cross-border operation on October 14, 2025. Investigations revealed scam compounds across Cambodia and Laos, where trafficked workers, from foreign nations, were coerced into impersonating as financial advisors or romantic partnersonline. Victims across 40 nations—including thousands in India—lost life savings in these scams.

Last but not least, one of the most common questions that most of us ask when visiting a public place is how to connect to a public W-Fi. After all, in this connected world, who will hate free data? But should you connect to a public W-Fi? Is it safe? Remember, public Wi-Fi's—at airports, cafés, and malls—continue to serve as an easy target to intercept data or inject malware into your instruments. Follow our quick safety guide to stay safe when using public Wi-Fi, especially if you need to connect urgently. Simple measures include verifying SSIDs, using HTTPS-only sites, enabling VPNs, disabling Bluetooth, and forgetting public networks after use, which can drastically reduce your risk exposure. The key lesson: cybersecurity is not just a technical responsibility but a behavioural discipline.

We hope you like this issue as much as we liked putting it together. We look forward to your suggestions, as they help us strive to excel in our endeavour towards making the world cyber-safe. If you have any suggestions on how we can improve this honest effort, please write to us at pankaj.toppo@atheniantech.com. Till we meet again next month. Happy reading.

Pankaj Anup Toppo

India is Expanding Its Digital Frontier

The Government of India has made significant strides in strengthening its digital defences through a structured and multi-layered cybersecurity framework. According to a recent note by the Press Information Bureau, this framework places the Indian Computer Emergency Response Team (CERT-In) at the core of real-time monitoring, threat detection, and incident response.Working in tandem,the National CriticalInformation Infrastructure Protection Centre (NCIIPC) safeguards critical sectors, including banking, energy, and telecommunications, while the Indian Cybercrime Coordination Centre (I4C) leads efforts to trace, investigate, and dismantle cyber fraud networksthat operate across jurisdictions.

India's digital transformation stands as one of the defining successstories of the 21st century. Over the past decade,the country has rapidly evolvedinto one of the most digitally connected economies in the world, with over 86 per cent of households now being connected to the Internet. This transformation has led to smoother governance, efficientcommunication, a boomingfintech ecosystem, and improved citizen services. Yet, beneath these achievements lies a growing and complex challenge: cybersecurity. Every new connection expands the nation's digital footprint and, with it, the potentialattack surface for adversaries seeking to exploit vulnerabilities within networks, systems,and institutions.

In today's interconnected landscape, the distinction between civilian and strategic targets has largely become obsolete. Cyberattacks that once focusedsolely on government institutions or defence entities now extend to every aspect of digital life, from hospitals and universities to logistics chains and financial systems.What began as isolated hackingincidents has now evolved into a global scale that is driven by data theft, espionage, and large-scale disruption. Modern adversaries range from organisedcriminal syndicates that are motivated by profit to hacktivist collectives and state-sponsored groups pursuing geopolitical objectives.

Recognising this evolvingthreat landscape, the Government of India has expanded its citizen-facing and institutional initiatives to raise awareness, coordinate responses, and address such incidents. Platforms such as the National Cyber Crime Reporting Portal have simplified incident reporting, enabling faster action and broader participation. The CyTrain portal provides law enforcement and investigative agencies with the necessary technical training to address sophisticated cyber offences. Meanwhile, initiatives such as Sahyog for rapid content takedownand the Bharat National Cybersecurity Exercise 2025 underscore India's focus on preparedness through simulation, collaboration, and real-time coordination among government bodies, private-sector entities, and critical infrastructure operators.

The Numbers Tell a Cautionary Tale

The statistics emerging from these efforts reveal both progress and peril. Reported cybersecurity incidents in India have increased from 1.029 million in 2022 to 2.268 million in 2024, reflecting both the rise in digital penetration and improvements in reporting mechanisms. The financial impact of cyber fraud has reached ₹36.45 lakh, reported on the National Cyber Crime Reporting Portal (NCRP) as of 28 February 2025. More significantly, proactive coordination among government agencies and financial institutions helped prevent losses of over ₹5,489 crore in potential cyber fraud cases.

This duality of rising threats and equally growing resilience defines India's cybersecurity journey. The allocation of ₹782 crore in the Union Budget 2025 towards cybersecurity initiatives, alongside the establishment of cyber forensic laboratories,further reinforces the government's recognition that cybersecurity is no longer a technical issue alone, but is a national imperative.

The Changing Nature of Cyber Threats

The threat environment itself has grown increasingly dynamic. The past few months have seen attackers deploy sophisticated ransomware strains that are capable of evading traditional defences, exploiting zero-day vulnerabilities in supply chains, and weaponising artificial intelligence for deception at scale. Data is no longer the only target;trust has become the new currency of cyber conflict. When customer records are stolen, it is not just a breach of privacy but also an erosion of confidence. When websites of the state/government and its institutions are defaced or portals are disabled, the loss is not merely operational but also psychological, which is a direct assault on public morale.

India's critical sectors,including finance, transport, healthcare, and manufacturing, have increasingly come under the crosshairs of hostile actors. Many entities in these sectors, despite adopting cybersecurity standards, remain vulnerable due to third-party dependencies, unpatched systems,or human error. The interconnected nature of modern digital supply chains means that a single compromised endpoint can lead to cascadingfailures across multiple networks.

Moving Towards a Culture of Cyber Discipline

The Bharat National Cybersecurity Exercise 2025, held from July 21 to August 1, reaffirmed India's growing commitment to strengthening its cyber resilience. Bringing together over 600 participants, including cybersecurity professionals, regulators, and policymakers, the exercise served as a national test of preparedness. Its centrepiece, STRATEX,was a large-scale simulated cyber breach scenario that evaluatedreal-time coordination, decision-making, and inter-agency response under pressure.

India now stands at a critical intersection where its digital transformation fuels innovation and growth,but also expandsthe surface area of cyber threats. As one of the fastest-growing digital economies, the nation has become both a symbol of progress and a prime target for cybercriminals. Through its multi-layered response framework, the government continues to strengthen defences, prevent fraud, and dismantle cybercrime networks using advanced forensics, big data analytics, and indigenous security tools.

Ransomware Hits Generali Central Life Insurance

On 20th October 2025, GeneraliCentral Life Insurance, a joint venturebetween
A major ransomware attack hit the Generali Group and the Central Bank of India. The attack, attributed to the infamous Medusa group, crippled the company's internal document servers, forcing the company to take several systems offline. The hackers claimedto have exfiltrated sensitive corporate data and demanded a ransom of approximately USD 500,000 (₹4.2 crore) to prevent the leak of the compromised information.

However, instead of accepting the ransom demand,the company's swift response established an unusual legal precedent. On 21 October 2025, Generali Central Life Insurance approached the Bombay High Court, seeking protection of its digital assets. The court acted swiftly, issuing a "John Doe" order against the unknown hackers, preventing them from selling or publishing the compromised data. (A "John Doe" order is a court order issued against unidentified defendants, commonlyused to protect intellectual propertyrights like copyrights and trademarks from anonymous infringers.) The Bombay High Court also instructed the Department of Telecommunications (DoT), Government of India and various social media intermediaries to block all links and accounts sharing the stolen content.This is one of the rare cases where the Indian judiciary directly intervened during an active cyber-extortion incident, acknowledging that ransomware attacks today threatennot just data but also the integrity of an enterprise itself.

Anatomy of the Breach

Preliminary investigations suggest that the compromise likely originated from a targeted phishing campaign targeting employees responsible for internal policy and HR documentation. Malicious email attachments disguised as updated company policies were used to install the payload, granting the attackers remote access to the insurer's internal network. Once inside, the Medusa operators encrypted critical systems and left behind a ransom note on the affected machinesdemanding payment in cryptocurrency.

The company has confirmed that policyholder funds, customer paymentdata, and insurance claims systems remain secure, althoughroutine internal operations experienced temporary disruption. Cyber-forensic specialists were engaged to evaluate the full extent of data exfiltration and trace the intrusion path. The insurer has also notified the sectoral regulators and data protection authorities about the breach, in accordance with the Digital Personal Data Protection (DPDP) Act, 2023.

Massive Exposure of 2.73 Lakh Bank Transfer Records

In one of the most disturbing exposures of financial data this year, cybersecurity researchers uncovered an unprotected Amazon Web Services (AWS) S3 bucket containing over 2.73 lakh Indian bank transfer records. The database, discovered by security analysts at UpGuard, was publicly accessible without authentication and contained National Automated Clearing House (NACH) transaction PDFs containing sensitive financial details.

Each PDF file included names, account numbers, IFSC codes, transaction amounts, and timestamps, revealing the payment history of individuals and small businesses across multiple states. The exposed data appeared to originate from several financial intermediaries and service vendors responsible for bulk electronic fund transfers. What made the discovery alarming was the absence of any visible ownership tag, leaving investigators unsure which institution or vendor the database belonged to.

The exposure was initially detected on 26 August 2025 but came in the public attention in late September when the researchers published their findings, prompting regulators to intervene. By the time access was restricted, the database had already been indexed by several open-source data-crawling tools, significantly increasing the risk that records would be downloaded and reused by malicious actors.

Regulatory and Sectoral Response

The Reserve Bank of India (RBI) and the National Payments Corporation of India (NPCI), which overseesthe NACH infrastructure, have since initiateda joint audit to trace the origin of the data. Initial indications suggest that the exposed files may have been generated by a third-party fintech vendor contracted for automated bank reconciliation services. The absenceof encryption, combined with the publicly readable permissions on the AWS bucket, points to a clear violation of basic data-handling protocols under the provisions of the Digital Personal Data Protection (DPDP) Act, 2023.

Cybersecurity specialists have warned that such leaks, though often unintentional, can have severe repercussions. With nearly ₹380 crore in cumulative transactions represented in the leaked PDFs, analystscaution that even a small fraction of the data could be misused to carry out identity theft or social engineering, potentially resulting in significant financial fraud.

Cloud Misconfigurations on the Rise

This incident underscores a rising trend in India, where misconfigured cloud infrastructure is a leading cause of data breaches. According to CERT-In's mid-year report, over 27 per cent of all reportedbreaches in 2025 were linked to publicly exposed storage buckets or databases, often due to human error or inadequate monitoring of third-party vendors.

The AWS exposure highlights the urgent need for continuous compliance monitoring, automated cloud audits, and strict vendor accountability. While the exposed bucket has since been secured, the episode serves as a stark reminder that in today's interconnected financial ecosystem, data protection is only as strong as the weakest link in the supply chain.

Ransomware Hits Klingelnberg India

On 3 October 2025, German engineering giant Klingelnberg Group's Indian subsidiary, headquartered in Pune, Maharashtra, reported a major ransomware intrusion that disrupted its design and production planning systems. The attack, claimed by the "Black Shrantac" ransomware group, on
Underground leak forums exposed the vulnerability of India's rapidly digitising manufacturing sector.

The alleged threat actors claimed to have exfiltrated nearly 1.1 terabytes of internal data, including technical schematics, supplier invoices, and employee HR records, from Klingelnberg India's internal servers. The group, which has been active since early 2024, is known for its attacks on European automotive suppliers and tool-manufacturing networks. In a post-dated October 5, Black Shrantac threatened to publish "confidential gear-technology documentation" if a ransom of USD 400,000 (≈ approximately ₹3.3 crore) was not paid within seven days.

How the Intrusion Unfolded?

Preliminary investigations revealed that the attackers gained access to Klingelnberg India's network by compromising a vendor's remote maintenance account used for servicing one of the company's Computer-Aided Manufacturing (CAM) systems. Once inside, they deployed a modified version of the LockBit 3.0 ransomware, which locked the company files and renamed them with the extension ". bksrant." The malicious software quickly spread through shared drives and encrypted the firm's central Enterprise Resource Planning(ERP) system, disrupting order processing across its facilities in Pune, Bengaluru and Faridabad.

The company's European headquarters confirmed that factory machines and assembly-line equipment were not affected, though digital systemsfor production planning and internal communication were temporarily taken offline. Cybersecurity experts from Kroll Cyber Advisory and CERT-In responded within hours to contain the breach. Their analysis showed that data had been transmitted to servers locatedin Bulgaria and Romania, which matched the knowninfrastructure used by the Black Shrantac ransomware group.

Impact on Operations and Supply Chain

The breach resulted in an estimated 72-hour downtime, delaying the exports of precision gear components destined for automobile clients in Germany, Japan, and the US. Financial analysts estimate immediate losses of ₹18–20 crore due to operational disruptions and the costs of data recovery.

To mitigate further impact, Klingelnberg India initiated full system restoration from offline backups and rotated all administrative credentials. No ransom payment was confirmed. Instead, the company pursued full data-recovery procedures and filed a detailed report with the Maharashtra Cyber Police under Sections 43 and 66 of the Information Technology Act, 2000.

Avnet Confirms Data Theft in Cloud-Storage Breach

On 7 October 2025, Avnet Inc., one of the world's largest electronics distributors, confirmed that its Europe, Middle East, and Africa (EMEA) division had suffered a data breach after attackers gained unauthorised access to a cloud-hosted storage environment linked to its internal sales portal. The company disclosed that certain historic point-of-sale (POS) records, customer contact information, and product quotations were accessed in what investigators described as a targeted data-theft operation.

The breach came to light after a threat actor using the alias "BlackPhoenix" posted a claim on an underground forum on 4 October, offering what they described as "Avnet Europe customer data archives 2022–2024" for sale. The actor shared partial samples containing client email addresses, order codes, and transaction metadata, prompting the company to initiate an internal forensic review. On 7 October, Avnet publicly acknowledged the intrusion, stating that "an external threat actor gained limited access to an isolated cloud system used by our EMEA sales enablement platform."

Forensics Reveal Misconfigured Cloud Access

Preliminary investigations indicated that the attackers exploited a misconfigured API key in a third-party analytics integration used to synchronise sales data between regional offices. This vulnerability allowed the adversaries to authenticate into a Microsoft Azure storage container without additional credentials. Forensic logs suggest that data exfiltration occurred over a six-hour period between September 30 and October 1, with approximately 1.3 terabytes of files being copied before Avnet's security operations centre detected the anomaly.

While the stolen files contained client company names, purchase histories, and contact details, Avnet Inc. confirmed that financial data, passwords, and payment credentials were not exposed, as the affected environment did not handle transactional processing. Nonetheless, cybersecurity experts have warned that even such metadata can be leveraged in targeted phishing or supply-chain impersonation attacks.

Response and Global Coordination

Avnet immediately decommissioned the affected cloud, rotated all API keys, and launched a global containment and notification processto alert users and stop the spread. Regulatory authorities across the EU, including the UK Information Commissioner's Office (ICO) and Germany's Federal Commissioner for Data Protection (BfDI), too, were informed about the breach.

In its official statement, Avnet Inc emphasised that "core IT systems, order processing, and supply-chain networks remain fully operational and secure." However, industry analysts highlight that this breach illustrates the growing complexity of cloud governance in multinational operations. With distributed access models and dozens of interconnected vendors, even a minor misconfiguration can expose enterprise data on a large scale.

Latest Cyber Scams

In today's hyper-connected world, where technology is deeply intertwined with every aspect of daily life, cybercriminals have found new ways to exploit the very essence of human trust. Gone are the days when cybercrime was merely about exploiting system vulnerabilities. Today, it's about exploiting emotions and perceptions, thereby denting the human psyche. October 2025 witnessed this alarming evolution, as India's rapidly digitising population became a prime target of fraud that was less about code and more about being cunning, or, as one might say, sneaky.

From digital arrest scams executed over video calls to elaborate investment and dating app frauds that fed on greed and emotional vulnerability, these scams reflected not just technical deception but psychological warfare. Each incident served as a stark reminder that in the digital era, manipulation of the mind can be just as devastating as manipulation of the machine.

As law enforcement agencies intensify crackdowns and awareness campaigns gain momentum, one truth stands tall in the world of cybercrime today that it is not just about stealing money or data, but about eroding the fragile trust that binds our digital existence. This section highlights the most notable scams observed in October 2025 cases, revealing the growing sophistication, audacity, and emotional depth of modern-day cyber deception.

Digital Arrest Scam Unmasked

In a major breakthrough in October, the Maharashtra Cyber Police busted one of India's largest "digital arrest" operations —a criminal network that extorted money from victims by impersonating law enforcement officials on phone and video calls. The investigation, which concluded on 10 October 2025, led to the arrest of seven key members operating out of Thane and Navi Mumbai and uncovered a sophisticated laundering system involving more than 6,500 mule bank accounts.

The syndicate's modus operandi followed a now-familiar pattern of psychological coercion. The perpetrators in this type of scam would often call individuals posing as officers of the Central Bureau of Investigation (CBI) or the Enforcement Directorate (ED). Using AI-generated voices and WhatsApp video calls staged against fabricated police station backdrops, the fraudsters falsely accused potential targets of being involved in money laundering or data theft and then ordered them to transfer funds "for verification."

Anatomy of the Fraud

Investigators revealed that the gang routed payments through 13 layers of accounts before converting the proceeds into cryptocurrency and withdrawing them through offshore exchanges. The total amount traced so far exceeds ₹58 crore, although officials believe the real figure could be much higher. Each account in the chain was maintained under fake or stolen identities purchased on the dark web for ₹500–₹1,000 per record.

The scammers operated a structured, call-centre-like setup that mimicked official procedures. They used pre-written scripts, templates for fake "CBI case numbers," and forged digital warrants to make their operation appear legitimate and intimidating. Their targets ranged from small-business owners to retired professionals across Maharashtra, Gujarat, and Delhi. In many instances, victims were kept under constant online surveillance for days, forcing them to stay connected on video calls, ordering them not to disconnect, claiming that doing so would be treated as "non-cooperation" or an "attempt to escape custody."

Victims were then monitored constantly through video calls; as a result, they were cut off from family or friends and were pressured to transfer money under the illusion of clearing false charges.

Crackdown and Policy Implications

Acting on financial intelligence from multiple banks, the Maharashtra Cyber Police froze ₹17.6 crore in 420 active accounts and traced links to servers in Cambodia and Myanmar, where similar scams were executed. Authorities are now coordinating with Interpol's ASEAN Desk to repatriate suspects who are believed to have fled abroad.

Officials have warned that "digital arrest" fraud has become the fastest-growing social engineering crime in India, with cases rising 340 per cent year-over-year. The Ministry of Home Affairs, Government of India, has since directed telecom providers to enable a real-time number verification system that flags suspected impersonation calls within seconds.

The dismantling of this ₹58-crore network marks a turning point in India's response to psychological cyber-extortion, proving that even well-orchestrated transnational scams can be disrupted when law enforcement, banks, and telecom regulators act in unison.

Gurgaon ‘Bumble’ Investment Scam

In what the Gurugram Police have described as a “classic case of emotional engineering,” a 50-year-old IT professional from Gurgaon, Haryana, lost ₹73 lakh in a meticulously orchestrated romance cum investment scam that began on the popular dating platform “Bumble” and ended with a series of fraudulent transfers to overseas accounts. The case, registered on 16 October 2025 at the Gurgaon Cyber Police Station, highlights the increasing sophistication of “pig-butchering” scams, a sophisticated investment fraud where scammers develop a long-term, trusting relationship with a victim before convincing them to invest large sums of money in a fake scheme.

The victim first came in contact with a woman claiming to be a Singapore-based financial consultant through “Bumble” in early September. Within days, the interaction shifted to WhatsApp and Telegram, where the suspect convinced him to “invest” in a cryptocurrency trading platform that promised 15–20 per cent daily returns. The platform appeared legitimate, complete with live dashboards, trading graphs, and fabricated profit notifications. Encouraged by initial “earnings,” the victim invested multiple times in the platform, only to find that withdrawals were blocked and that his account was frozen under the pretext of “tax compliance.”

How the Scam Was Executed?

Forensic investigators found that the fraudulent app’s domain was registered under a Hong Kong-based entity with servers in Malaysia and Cambodia. The platform mimicked the interface of licensed exchanges and even displayed fake Securities and Exchange Board of India (SEBI) registration numbers, in a move to win the victim’s trust. The scammers used AI-based conversational scripts to maintain daily contact, portraying empathy and emotional intimacy to lower suspicion.

The victim made 23 bank transfers over 17 days, totalling ₹73,14,600, routed through accounts in Delhi, Mumbai, and Jaipur before being converted into cryptocurrency on Binance and OKX. Investigators later discovered that at least 11similar complaints had been filed across the NCR using the same trading domain.

Law-Enforcement Action and Public Advisory

The Gurgaon Cyber Crime Unit, in collaboration with the Intelligence Fusion and Strategic Operations (IFSO) wing of Delhi Police, blocked the fraudulent website and initiated a request through Interpol's Crypto-Asset Recovery Programme (CARP) to trace the flow of funds. Police have warned that such scams are increasingly linked to organised cyber syndicates operating from Southeast Asia, particularly those connected to call-centre compounds in Cambodia and Myanmar, where trafficked workers are forced to run large-scale crypto frauds.

Authorities have urged dating-app users to be cautious of individuals who quickly steer conversations toward investments. The Indian Cyber Crime Coordination Centre (I4C) has also issued an advisory to all major dating platforms to deploy AI-driven fraud-detection algorithms that flag suspicious account behaviour.

The Gurgaon case exemplifies how cybercriminals are merging emotional manipulation with fintech deception, weaponising trust to orchestrate high-value scams across international boundaries.

Pune Tech Professional Duped of ₹3.66 Crore

A shocking case from Pune, Maharashtra, once again highlights the growing scale and sophistication of investment-application frauds. A 37-year-old software engineer, employed at a multinational IT firm, was duped of ₹3.66 crore after being lured into a fake online trading platform that promised lucrative returns through cryptocurrency and foreign exchange investments. The fraud, uncovered on October 12, 2025, represents one of the largest single-victim cyber-financial scams reported in the city this year.

The victim came across a promotional post on Instagram, purportedly from a verified investment influencer offering mentorship in digital asset trading. After clicking on the link and joining a Telegram "VIP Trading Group," he was persuaded to download a trading app that mimicked the interface of a well-known brokerage firm. The scammers, posing as professional analysts, guided him to make initial deposits of ₹50,000 and ₹2 lakh, which generated visible "profits" on the dashboard, a tactic designed to gain trust and encourage larger transfers.

How was the Fraud Executed?

Over the next month, the victim made a series of incremental payments to accounts linked to shell companies registered in Delhi and Mumbai, totalling ₹3.66 crore. Each time, he was shown falsified portfolio growth, real-time charts, and fabricated SEBI registration numbers. When he attempted to withdraw his profits, the app displayed messages demanding an additional 20 per cent "withholding tax" before releasing funds, a common deception used in similar international scams.

Forensic experts from the Pune Cyber Crime Unit discovered that the application's servers were hosted in Singapore, while its payment gateways routed transactions through Hong Kong, the UAE, and Turkey, before converting to cryptocurrency wallets controlled by the fraudsters. The domain registration was found to be less than 45 days old, a typical red flag in such schemes.

Law Enforcement Response and Victim Recovery Efforts

The Pune Cyber Crime Cell, in collaboration with the Indian Cyber Crime Coordination Centre (I4C), has initiated proceedings to track cross-border financial flows. Multiple cryptocurrency wallets linked to the case have already been flagged, and authorities have requested a blockchain forensic trace through Chainalysis. The Enforcement Directorate (ED) has also been briefed on the suspected overlap between this case and similar investment fraud operations targeting victims in Bengaluru, Noida, and Hyderabad.

Cybersecurity experts warn that these scams exploit India's fast-growing retail investor base, combining the appeal of quick profits with the anonymity of crypto transactions. A report by the Reserve Bank of India (RBI) estimates that financial cyber frauds involving trading platforms have surged 412 per cent in FY 2024–25, with average per-victim losses exceeding ₹38 lakh.

U.S.–U.K. Takedown of Southeast Asia's "Pig-Butchering" Empire

In a landmark international operation, authorities from the United States of America and the United Kingdom have jointly dismantled one of the world's largest cyber-fraud syndicates, which was responsible for orchestrating mass-scale "pig-butchering" investment scams across Asia, Europe, and North America. The coordinated action targeted entities affiliated with the Prince Holding Group, a Cambodia-based corporation long suspected of being a front for cross-border scam operations.

According to the U.S. Department of Justice (DOJ), 1,27,271 Bitcoin, valued at nearly $14.9 billion (₹1.24 lakh crore), were seized in a sweeping global asset freeze spanning Singapore, Cambodia, Hong Kong, and Dubai. The operation followed months of intelligence coordination through the Joint Cybercrime Action Taskforce (J-CAT), under the auspices of Europol and the U.K. National Crime Agency (NCA).

How did the Empire Operate?

Investigators revealed that the syndicate operated sprawling “scam compounds” across Cambodia and Laos, employing trafficked workers to carry out scripted online investment and romance scams. Recruits, many of whom were lured from India, Malaysia, and the Philippines with promises of IT jobs, were held under intimidating conditions and were forced to impersonate financial advisors or romantic partners on messaging apps such as WhatsApp, Telegram Line.

Victims were gradually “fattened up” with fake profits on fraudulent investment platforms before being drained of their life savings, a process dubbed pig-butchering by investigators. The scam network is estimated to have defrauded over 1,90,000 victims globally, with individual losses ranging from $10,000 to $500,000.

The DOJ accused Chen Zhi, chairman of Prince Holding Group, and six other executives of money laundering, human trafficking, and racketeering. Forensic blockchain tracing linked the group to a chain of Singaporean shell companies that converted crypto proceeds into real estate investments and luxury assets.

Implications for Asia-Pacific and Beyond

Law enforcement agencies across India, Vietnam, and Thailand have launched their own investigations into regional offshoots of the Prince Group network. India’s I4C has identified at least 68 victims domestically who lost over ₹12 crore to affiliated platforms in recent months.

The global crackdown has been addressed as a template for cross-border cybercrime enforcement, integrating blockchain forensics, human trafficking rescue operations, and financial sanctions within a single strategic framework

AI Assistants That Work Without the Internet (Offline AI)

For years, Artificial Intelligence (AI) was something that lived in distant data centres analysing voice commands, recognising faces, or translating text through massive cloud servers. However, this dependence on cloud connectivity often raised privacy concerns and slowed response times. The latest evolution in AI has changed that. A new generation of offline AI assistants can now run entirely on local devices, processing data directly on smartphones, laptops, or smart home gadgets without sending information to the Internet.

This development has been made possible by advances in on-device machine learning (ML), enabling smaller, more efficient models to perform complex tasks with minimal processing power. These models are trained in the cloud but deployed locally, enabling instant actions such as voice transcription, language translation, photo enhancement, and personalised recommendations, all while keeping user data secure and private.

Companies such as Apple, Google, and Samsung are leading this shift. Apple's latest iPhones and MacBooks now run AI models locally for autocorrect, image recognition, and voice input, while Google's Pixel devices perform real-time translations without external servers. This shift not only reduces dependency on Internet connectivity but also helps users in low-network or rural areas access intelligent features seamlessly.

Privacy advocates have welcomed this trend as a turning point for responsible AI. By processing data locally, users regain control over personal information, a crucial step in an era when data breaches and digital surveillance have become global concerns. Moreover, local AI reduces latency, energy consumption, and the carbon footprint caused by large-scale data centres.

The rise of offline AI represents a subtle yet powerful transformation in how humans interact with machines. It is redefining what "smart" truly means, not just intelligence that learns, but intelligence that respects privacy, works independently, and remains always accessible, even when the world around it is disconnected.

Satellite Internet Expands the Connected World

In a world where connectivity defines opportunity, billions of people still remain offline. Villages in rural areas, remote islands and even in mountainous regions continue to struggle with limited or no Internet connection. But that reality is changing, thanks to a new technological revolution unfolding, satellite-based Internet.

Unlike traditional broadband or mobile networks that rely on ground infrastructure, Low Earth Orbit (LEO) satellites operate much closer to the planet, reducing signal delay and providing high-speed connectivity even in isolated areas. Companies like Starlink(SpaceX), OneWeb, and Amazon's ProjectKuiper are at the forefront of this transformation, launching thousands of satellites to build global coverage networks.

For communities that have long been left behind, the impact is profound. Schools in remote regions can now access online learning, farmers can monitor weather data and market prices in real-time, and doctors can provide telemedicine consultations to remote villages. During natural disasters, satellite networks also serve as emergency communication lifelines when traditional infrastructure collapses, as seen recently during cyclones and earthquakes in the Asia-Pacific region.

In India, the Department of Telecommunications (DoT) and IN-SPACe have begun collaborating with global satellite operators to accelerate rural connectivity under the government's Digital India initiative. With regulatory clearances easing and satellite terminals becoming smaller and cheaper, millions could soon be connected where fibre cables may never reach.

However, this connectivity boom comes with new challenges. Space debris, orbital congestion, and the need for international coordination are emerging as serious concerns. Moreover, maintaining cybersecurity for thousands of orbiting systems remains a crucial task. Experts believe global cooperation will be essential to ensure that the promise of universal Internet access does not lead to digital or orbital chaos.

Despite these hurdles, satellite Internet stands as one of the most significant equalisers of the modern era. It has the power to close the global digital divide and bring every corner of the world into the same online conversation.

DIY Guide: Staying Safe on Public Wi-Fi

We truly live in a digital world, and it is manifest in the alacrity with which each of us remains connected 24/7. It's a different matter that the intensity of remaining connected can vary depending on one's nature, likes, and, of course, the generation to which one belongs. Although telecom companies have almost covered the entire country, there are still areas with low connectivity. If you are travelling to offbeat locations, you will have noticed that one of the USPs that the properties in the said locality flaunt is free Wi-Fi. While it's a good idea to access those services in such locations, more often than not, public places like cafes, restaurants, airports and even aeroplanes offer free public Wi-Fi. So, should you bite the bullet as the free data in a digital world is way too sumptuous to resist, even at a time when Internet connectivity comes as a default with a live mobile connection?

Before delving into those details, it is advisable to gain an understanding of the nature of Wi-Fi networks available today.

In today's fast-paced digital world, staying connected has become a daily necessity rather than a luxury. Whether we are at an airport, cafe, or hotel lobby, our first instinct is often to look for a free Wi-Fi connection. While older generations may not feel the same pull toward constant connectivity, for the younger generation, being online is almost second nature. Social media, instant updates, and the fear of missing out have created a strong need to remain connected to the digital world at all times. For many, a place with weak mobile data or no signal feels incomplete unless there's Wi-Fi to bridge the gap. Free Wi-Fi, in such moments, becomes more than a convenience; it becomes an attraction. The promise of staying updated, posting regularly, or simply not missing what's happening around the world is often enough to make people connect without a second thought.

In today's times, we are surrounded by two kinds of Wi-Fi networks. The first is the private network, which we have in our respective homes, where we use it at home, in a secure and familiar environment, and entry into that closed group is controlled. shared only with family members. This is a trusted space,where you control who connects and what devices are allowed in. The other is public Wi-Fi, which is available in places like cafes, hotels, airports, and even paying guest accommodations. Unlike your home network, these connections are open to everyone, friends, strangers, and at times, even cybercriminals. While they appear friendly and convenient, they lack the same level of safety and control that a private network in your home offers.

In recent years, public Wi-Fi has also become a marketing tool. Businesses have realised that free internet access attracts customers faster than any other perk. Almost every cafe, restaurant, and hotel now proudly displays a “Free Wi-Fi” sign at the entrance. Even travel platforms like MakeMyTrip, Airbnb and resort chains highlight complimentary Wi-Fi as one of their top amenities. After all, if two hotels offer the same price, the one with free Wi-Fi will always seem more appealing. The result is that people naturally choose convenience over caution.

However, beneath this layer of comfort lies a risk that often goes unnoticed. Public Wi-Fi networks, while appearing safe and convenient, are in fact one of the easiest ways for cybercriminals to reach you. These open networks act as digital crossroads, where dozens of users share the same connection, making it effortless for attackers to slip in unnoticed. The same connection that helps you check a bank balance, access office mail, or make an online payment can also allow an attacker to quietly intercept your personal data.

The danger lies not in the technology itself, but in how casually we trust it. A familiar cafe name or airport logo on a Wi-Fi screen gives us a false sense of security. Many people are unaware that connecting to a network without verifying its source can expose sensitive information, such as passwords, card details, and personal messages, in mere seconds. In an era where data is as valuable as currency, it is crucial to recognise that not all free connections come without a cost. Public Wi-Fi may seem like a small everyday convenience, but one careless connection can open the door to serious digital trouble for you and transform you from a prince to a pauper in seconds. If you don't want to be that unlucky individual, follow some of the tips mentioned below to make good use of public Wi-Fi without losing sleep over the thought that you should have held back your emotions that one time.

How Hackers Exploit Public Wi-FixFi Networks?

When you connect to a public Wi-Fi network, your device shares the same connection with several other users. Attackers exploit this shared access by creating fake Wi-Fi networks that closely resemble official ones. For instance, if the café's network name is "CoffeeHouse," a hacker might create a clone called "CoffeeHouse_Free." Once you connect to the fake network, every online action you take, from logging into social media to checking your email, can be silently monitored.

Sometimes, even genuine public Wi-Fi networks are not secure. Hackers sitting on the same network can intercept unencrypted data, view your browsing history, and even capture your login details. They can also trick users into visiting fake websites that appear to be legitimate banking or shopping portals. What makes these attacks dangerous is that users often don't realise anything unusual has happened until it is too late or shortly after they have been conned.

Safe Habits When Using Public Wi-Fi

The easiest way to stay protected is to avoid using public Wi-Fi for any financial transactions or sensitive work. Always verify the network name with the staff before connecting; even a small spelling difference could mean the network is fake. If you need to browse, stick to websites that start with "https", which stands for Hypertext Transfer Protocol Secure, as they provide an additional layer of protection by encrypting your connection.

If you frequently use public Wi-Fi, consider installing a Virtual Private Network (VPN). A VPN ensures that all your online activity is encrypted, even if the network itself is not secure. Keep your device software and security applications updated at all times. Once you have finished using the public network, disconnect and select "Forget this Network" to prevent your phone or laptop from reconnecting automatically in the future.

Common Mistakes to Avoid

Most problems on public Wi-Fi are not caused by complex hacking but by small mistakes people make without realising it. One such mistake is leaving Bluetooth turned on in public places. When Bluetooth is left active, nearby devices can sometimes detect your phone or laptop and attempt to connect or send files without permission. Attackers can misuse this to access shared data or send malicious files. Another common mistake is clicking on pop-up messages that appear right after connecting to a Wi-Fi network. These messages often claim to offer “security updates” or “faster connection” options, but are usually fake. They install harmful software that can steal information or slow down your device. The safest approach is to keep Bluetooth turned off when not in use, avoid clicking on unexpected pop-ups, and never share personal details, passwords, or OTPs while using public Wi-Fi. Genuine banks or financial services will never ask for such information online.

The Smarter Choice

Public Wi-Fi’s Wi-Fi may make life easier, but it is not always safe. Whenever possible, use your mobile data or a personal hotspot instead of public Wi-Fi networks. The small amount of data used for work or browsing is a fair price to pay for keeping your private information secure.

Cybersecurity begins with awareness. A few careful steps, such as verifying connections, using secure websites, and disconnecting after use, can go a long way in keeping your data safe. The next time you see a free Wi-Fi sign, think twice before connecting; the convenience it offers could come at a cost far greater than you expect.

Athenian Tech

Contact Us

www.atheniantech.com

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