ATHENIAN TECH

NEWSLETTER

June 2025

THREAT INTELLIGENCE BY ATHENA

From the Editor's Desk

The previous month i.e. May 2025 witnessed hostilities flare up to reach almost a war like situation between India and Pakistan which forced India to launch Operation Sindoor on 07 May 2025 which ended with a ceasefire on 10 May 2025. Post the killing of innocent tourists in the Pahalgam, on 22 April 2025, Inda took a host of measures, which ultimately culminated in the launch of Operation Sindoor.

IN THIS NEWSLETTER

Issue #04

Thanks largely to the hyper-connected world that we live in, tensions at the border spilled to the virtual space. This spilling of hostilities, into the cyberspace, led to astronomical rise in the number of attacks against Indian institutions. As per media reports, published in early June, it has been learned that India faced at least 10 crore cyberattacks post the killings in Pahalgam.

While the month of May saw hectic action in cyberspace June saw a lull, especially with the ceasefire coming into force. The month of the June however, exposed India to new kinds of risks, something which India is gradually being exposed to more so in the last couple of years. These are largely India's expanding cyber risks in a fragmented digital world order.

In an increasingly digitized and polarized world, India's cyber exposure is rising—not from direct conflict, but from perception. As geopolitical rivalries, like the recent Iran-Israel standoff, move beyond traditional battlefields into cyberspace, countries maintaining neutrality find themselves vulnerable to ideological targeting. India, with longstanding diplomatic ties to both the countries (Iran and Israel), was previously targeted by pro-Palestinian and Islamist hacktivists during the Gaza conflict. These attacks—mostly DDoS and defacements—weren't about damage, but symbolism. India's perceived tilt towards Israel made it a proxy target.

As the Iran-Israel confrontation intensified, India too got dragged into digital crossfire. India's expanding reliance on digital infrastructure—public services, fintech, and cloud networks—makes it an attractive target. The threat isn't purely technical, but ideological. India must move beyond reactive defences and actively assess how it is viewed within global narrative ecosystems.

Further data breaches continued to hold sway, even in June. On June 19, 2025, the the largest credential breach ever cam to light. In the breach over 16 billion usernames, passwords, tokens, and cookies were leaked from a patchwork of data harvested over years. Unlike isolated breaches, this was the product of long-term malware campaigns quietly exfiltrating data through emails, browser extensions, and compromised sites. This leak affected platforms like Google, Apple, Facebook, GitHub, and Telegram. Structured and bundled, the data allows attackers to launch account takeovers, credential stuffing, phishing, and ransomware attacks with ease.

On 09 June 2025, mobility platform Zoomcar confirmed a data breach affecting 8.4 million users. Threat actors initially contacted employees, claiming access to personal information, a claim later verified through forensic investigation. Exposed data includes fields like names, emails, phone numbers, addresses, and car registration details. Although financial credentials were untouched, the hybrid nature of this dataset opens doors to highly targeted fraud and impersonation scams. Zoomcar's operations continue uninterrupted, but the incident highlights the broader vulnerability of app-based consumer platforms in India. As services integrate personal, locational, and transactional data, securing them becomes a public policy imperative.

Digital sovereignty—control over data, infrastructure, and standards—is now central to national policy. The EU leads with landmark regulations like the Digital Markets Act, Digital Services Act, and AI Act, that are aimed at reining in platform dominance and ensuring user protection. India's Digital Personal Data Protection Act, 2023, marks its own step forward in defining consent, accountability, and localization. Countries like Brazil, South Korea, and Kenya are also tightening digital governance. Sovereign cloud models—like GAIA-X and AWS's European Sovereign Cloud—are becoming default architecture in regulated sectors. Meanwhile, governments are investing in local innovation, open-source platforms, and digital skilling to reduce dependency and enhance strategic autonomy.

But sovereignty has limits. Digital systems remain inherently global. As nations assert control, they must reconcile domestic authority with the need for international standards and interoperability.

When it came to events the 30th edition of Infosecurity Europe, held in London, convened over 13,000 professionals to assess the state of cybersecurity amid rising global tensions. AI threats, regulatory shifts, and geopolitical risks shaped the agenda. The AI & Cloud Theatre addressed deepfake detection, large language model (LLM) vulnerabilities, and AI-driven phishing. The event confirmed a new reality: cybersecurity is now foundational to national defence, business continuity, and digital trust. Strategic alignment, cross-border cooperation, and skill-building are essential for future readiness.

As regards the nature of cyber threats phishing remains a dominant cyber threat. By mimicking trusted sources, attackers trick users into sharing sensitive data through fake links, urgent messages, or too-good-to-be-true offers. Protection starts with awareness: verify emails, avoid clicking embedded links, and look for anomalies in sender addresses.

Use strong, unique passwords and enable MFA. Keep devices updated, install antivirus tools and maintain secure backups.

Reporting phishing attempts helps authorities identify trends and issue timely alerts. As attacks grow more personalized, digital literacy becomes as vital as technology in protecting users. Public awareness is our first—and strongest—line of defence.

To sum it all up, India's cyber landscape reflects broader global patterns: ideological spillovers, record-breaking data leaks, and digital services under siege. Its neutrality no longer shields it from becoming a symbolic target in international conflicts. At the same time, its growing digital economy, regulatory evolution, and geopolitical positioning amplify its attractiveness to threat actors.

Cybersecurity is no longer just about protecting networks—it's about safeguarding sovereignty, economic stability, and public trust. From policy and regulation to education and technology, India must adopt a whole-of-nation approach.

Anticipating threats, reinforcing resilience, investing in local capacity, and fostering global cooperation are not optional—they are now core to securing India's digital future.

As we walk this path together to make this world cyber safe, this is our third attempt at reaching out to you. Do let us know about what you feel about our attempts at reaching out to you. We will be more than happy to incorporate your views. Feel free to share your questions and views on the matter at pankaj.toppo@atheniantech.com .Till we meet again, happy reading.

Pankaj Anup Toppo

India’s Exposure in the Iran-Israel Conflict

For decades, the Iran-Israel rivalry has shaped the geopolitical landscape of West Asia. India, while maintaining strategic neutrality, has fostered constructive bilateral relations with both nations, balancing energy cooperation with Iran and defence engagement with Israel. This stance of neutrality has traditionally kept India on the sidelines of regional flare-ups, diplomatically engaged but largely uninvolved.

However, the nature of conflict has changed over time. The Israel-Iran escalation is no longer just a regional or kinetic issue. It has become a digitally driven confrontation, highlighting cyber hostilities. Unlike before, the spillover effects now impact third-party nations, not for their actions, but for their perceived alliances.

This context is particularly important for India. During the last round of hostilities in Gaza, between Israel and Palestine, India was targeted by pro-Palestinian and Islamist hacktivist groups. The reason was perception-based: India’s diplomatic stance and open engagement with Israel were perceived as indirect support for Israel. The attacks, ranging from DDoS operations to website defacements, were mainly symbolic, but they demonstrated how qu ickly geopolitical alignments can be weaponised in digital space.

Now, as the Israel-Iran conflict escalates, similar patterns are re-emerging. With global narratives becoming more polarised and cyber actors aligning ideologically, India again faces the risk of being drawn into the digital crossfire. The threat is real, not just hypothetical. It stems from a well-known pattern: perceived links to Western or Israeli interests can make India a proxy target.

As Iran and Israel face each other across both physical and cyber spheres, India's digital infrastructure—government services, fintech systems, and cloud networks—remains exposed. The vulnerabilities may not yet have been exploited extensively, but their purpose is evident. In a time when perception influences targeting, India must expect that it could once again be caught in the ideological fallout of a conflict that is neither of its making nor within its control.

India in the Crosshairs of Ideological Cyber Campaign

India had become involved in the digital consequences of geopolitical conflicts not because of its own doing. An instance of this was apparent during the recent Gaza conflict, where pro-Palestinian and Islamist hacktivist groups launched coordinated cyber operations against Indian digital assets. Their reasoning was based on perception: India's diplomatic ties with Israel were viewed as implicit support, positioning it in ideological opposition to their cause.

These operations were not sophisticated cyber intrusions. Instead, they largely Distributed Denial of Service (DDoS) attacks, website defacements, and public claims of breaches targeting symbolic platforms — from government websites to visa service portals. Despite their limited technical complexity, these acts aimed to serve a broader purpose: expressing dissent, demonstrating affiliation, and testing the resilience of public-facing systems.

The concern now extends beyond repetition to escalation. As the Iran-Israel conflict grew intense and ideological alliances become clearer, India was drawn into another wave of cyber hostility. The pattern is already well-known: geopolitical crises often spark narrative-driven cyber campaigns, and countries perceived as aligned with the West serve as convenient symbolic targets. India's strategic stance, coupled with its reliance on digital infrastructure, makes it particularly vulnerable.

This emerging reality requires more than just reactive containment. It calls for proactive mapping of India's position in global ideological narratives. If past campaigns are any guide, the next phase may not aim to inflict significant infrastructural damage but will seek to fracture trust, manipulate perception, and exploit symbolic vulnerabilities. For India, recognising this pattern early is not only wise—it is essential.

The attacks

The month of June witnessed a resurgence of cyber offensives against Indian digital platforms, echoing earlier incidents during the 2023 G20 Summit. These attacks, though somewhat limited in scope, carry symbolic importance and reflect a growing pattern of ideological cyber groups targeting India not because of its direct involvement in a conflict, but due to its perceived stance within the geopolitical narrative. Against this background, several incidents took place, in June, each showcasing different facets of this wider digital campaign.

1. Defacement of Educational Website by Garuda Error System

A website linked to Delhi Public School Bachhol, Jajpur, Odisha, was defaced by "Garuda Error System." The compromised page displayed politically charged slogans supporting Gaza and condemning Israel, along with references to a broader digital alliance under hashtags such as #OpIndia and #OpIsrael. Although the institution is not a government- entity, targeting a school portal underscores the adversaries' tactic: selecting publicly visible, easily accessible domains to maximise attention and spread their message. It needs to be noted that while this defacement does not have any mention of the Iran Israel conflict but only states that it will target countries which support Israel. The i=only reason why this incident finds mention here is because it happened on 14 June 2025 when the Israel Iran conflict was on n full swing.

***Figure 1**:The school's homepage was defaced with pro-Palestinian, anti-Israel slogans by the Garuda Error System, warning of further attacks on nations seen supporting Israel.*

2. DDoS Against Indian Financial Agencies

In a recent post shared within a Telegram channel called Sons of Anarchy—a group known for spreading ideologically motivated cyber messages—a threat actor using the alias "R3VOXANONYMOUS" claimed responsibility for launching Distributed Denial of Service (DDoS) attacks on two major financial agencies in India. The targets included the Income Tax Department and the Central Board of Indirect Taxes and Customs (CBIC), previously known as the Central Board of Excise and Customs, both divisions under the Ministry of Finance, Government of India.

The post, accompanied by a graphic "DDoS Alert" visual and check-host links, alleged disruptions to the official websites of these institutions. The attack was positioned as part of broader campaign under banners such as #OpIndia and #OpIsrael, reflecting increasing ideological polarisation in cyber narratives. By targeting prominent fiscal institutions of the Indian state, the attackers aimed not only to disrupt but also to symbolically align, framing India's financial systems as legitimate targets within an evolving digital theatre of dissent.

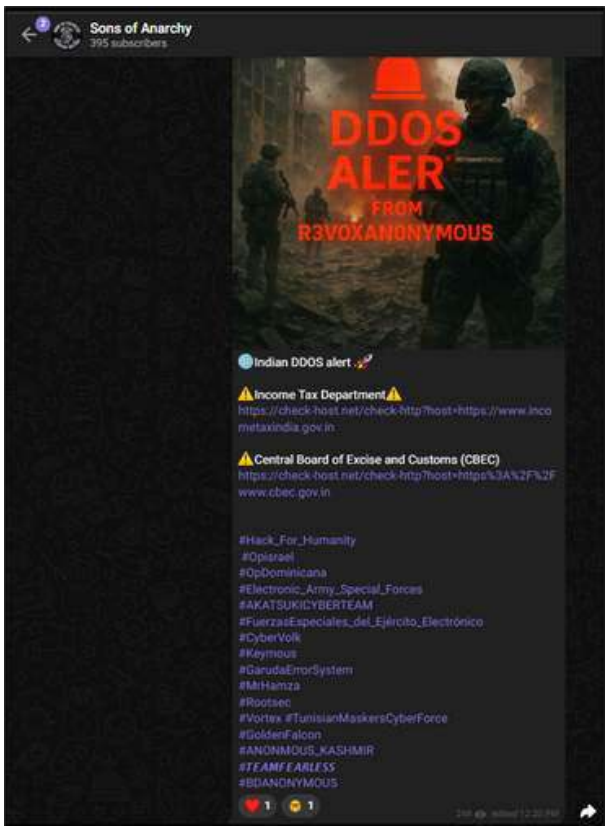

***Figure 2**:Telegram post from "Sons of Anarchy" claimed DDoS attacks on India's key financial agencies as part of broader ideological cyber offensives.*

3. Messaging Escalation and Threat Declaration

In a recent Telegram post from the channel "Obscurion", pro-Palestinian and pro-Iranian cyber actors claimed a "leaked data attack" on India. Framed with slogans like "It's Time to Strike the Indian Sites," the post listed hashtags such as #OpIndia, #Save_Gaza, and #Pro_Iran, while naming groups like Garuda Error System, APT_404, and Team Fearless as part of an ideological alliance.

No actual data samples were provided, nor was any breach independently confirmed. Nonetheless, the messaging demonstrates a recurring tactic: employing aggressive narratives and digital theatrics to signal dissent and instil perception-based fear—an approach that is increasingly common in cyber campaigns connected to geopolitical flashpoints.

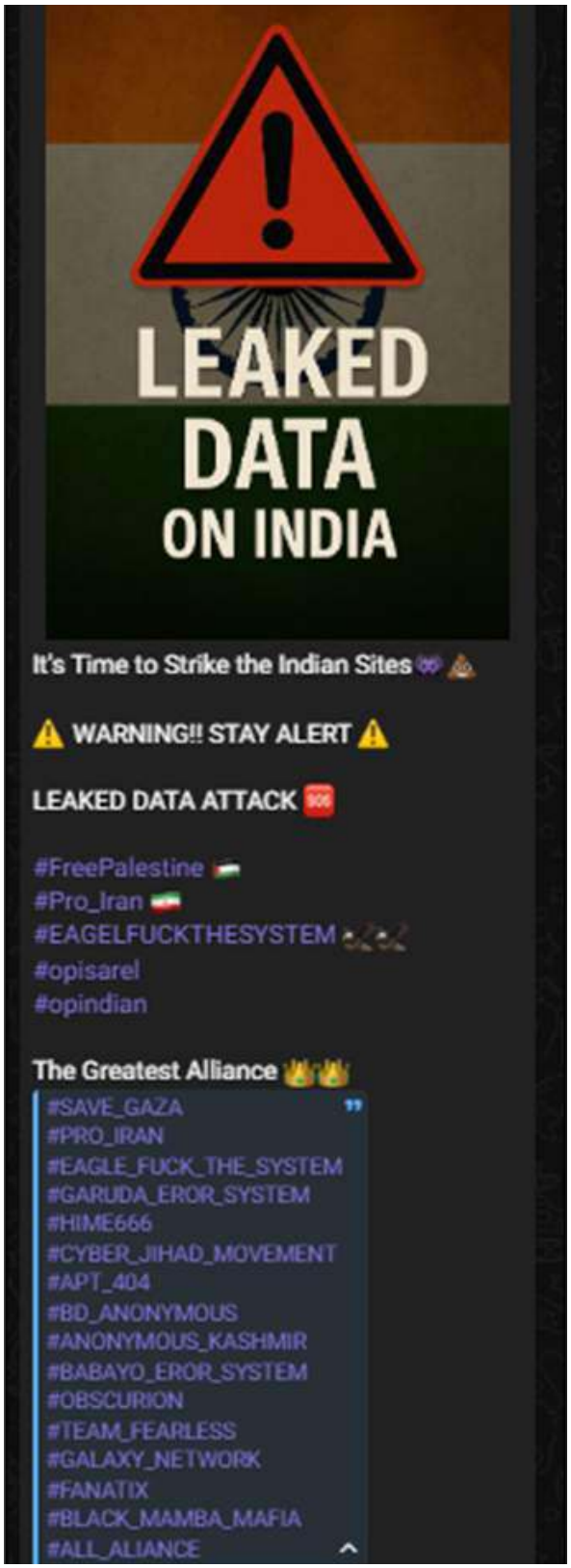

***Figure 3**:Telegram post from "Obscurion" threatening a leaked data attack on India, amplifying pro-Iran and pro-Palestinian cyber rhetoric.*

4. Multi-Target Website Defacements

In a recent wave of cyber defacements, the Telegram group “Fredens of Security” claimed responsibility for attacks on Indian digital infrastructure. The defacement itself was carried out by a threat actor operating under the handle “./noobiezta”, who targeted multiple platforms, displaying anti-India and anti-Western messages referencing campaigns such as #OpIndia, #OpNATO, and #OpG7Countries, #IranJustDoIt, #FckIndia, #FckIsrael.

Subsequently, the same actor defaced over 30 regional web portals, including domains under “payunitsecnsk.in”. These attacks were showcased through Fredens of Security’s Telegram channel, reinforcing their ideological messaging. Though technically unsophisticated, the incidents serve a symbolic purpose, project dissent and align with broader anti-Israel and anti-West narratives emerging amid the ongoing geopolitical friction.

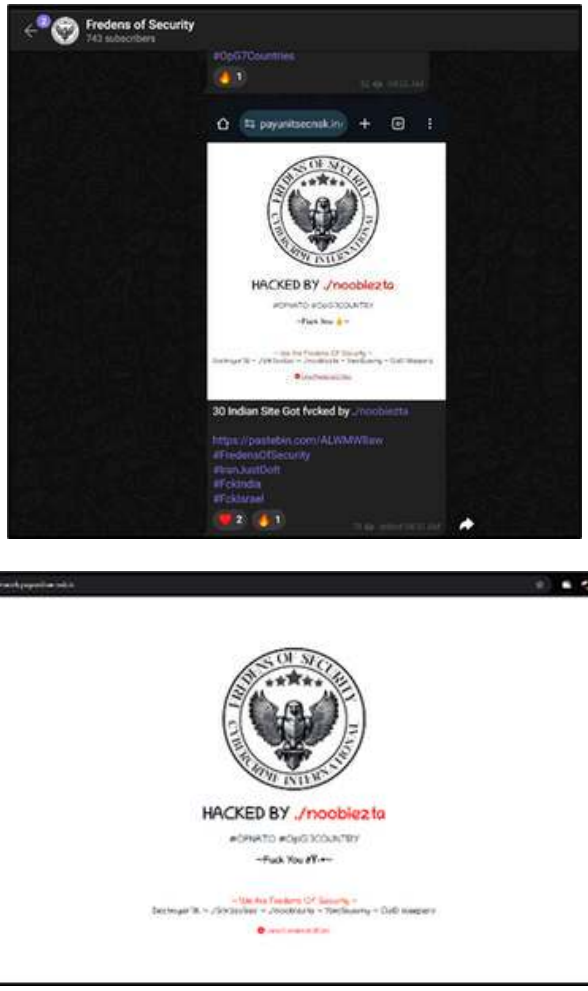

***Figure 3**:Screenshot of a defaced domains, accompanied by a Telegram post from “Fredens of Security,” claiming credit for hacking over 30 Indian sites as part of an anti-West cyber campaign led by threat actor “./noobiezta.”.*

Strengthening India's Cyber Posture Amid Perception-Driven Threats

India's foreign policy stance—characterised by strategic autonomy and balanced diplomacy—has traditionally kept itself away from direct involvement in regional conflicts. However, as recent cyber incidents reveal, perception in the digital age often takes precedence over declared neutrality. Whether seen as favouring Israel or maintaining relations with Iran, India increasingly finds itself vulnerable, not because of its actions, but due to how ideologically motivated cyber actors interpret those actions.

The wave of defacements, DDoS operations, and narrative-rich messaging campaigns signifies a wider shift: conflicts that were once limited to geographical borders now spread rapidly through cyberspace. In this environment, India's vulnerability is not just technical—it is also symbolic. Its prominence on the global stage, defence and technology partnerships, and digital infrastructure collectively make it a high-value target.

To mitigate this evolving risk, India must adapt its cybersecurity posture. This involves not only enhancing institutional capabilities through agencies like The Indian Computer Emergency Response Team (CERT-In) and the National Critical Information Infrastructure Centre (NCIIPC) but also preparing for perception-driven campaigns that blur the fine line between dissent and disruption. Proactive monitoring, coordinated response frameworks, and narrative risk assessment should become central components of the national cyber strategy.

As geopolitical crosswinds grow stronger, India's readiness can no longer be reactive. The future of cybersecurity depends not only on firewalls and patches but also on foresight—and on recognising that in today's conflicts, silence or neutrality provide no refuge from digital hostility.

The Largest Credential Data Leak in History

Researchers at cybernews, news portal covering news on maters related to cyber security have unearthed what is now being considered as the most extensive exposure of digital credentials ever documented, in human history. The discovery which came to light on 19 June 2025, threw open a treasure trove of containing over 16 billion unique login entries, distributed across 30 separate archives, representing a significant escalation in the scope and structure of credential-based cyber risks.

Unlike prior incidents, which were rooted in a singular breach event, this leak is notably composite in nature. Analysts at cybernews believe that the breach is the result of years of credential theft, quietly facilitated by infostealer malware campaigns. These malicious programmes—often embedded within email attachments, browser extensions, or compromised websites—exfiltrate sensitive login details from user devices in real time, often without raising detection alarms.

Each dataset uncovered by the researchers varied in size, with the smallest containing over 16 million records and the largest exceeding 3.5 billion records. The sources spanned nearly every major online platform, including Google, Apple, Facebook, GitHub, and Telegram. Notably, one particularly large subset, reportedly tied to Portuguese-speaking users, suggests patterns of regional targeting.

Each dataset uncovered by the researchers varied in size, with the smallest containing over 16 million records and the largest exceeding 3.5 billion records. The sources spanned nearly every major online platform, including Google, Apple, Facebook, GitHub, and Telegram. Notably, one particularly large subset, reportedly tied to Portuguese-speaking users, suggests patterns of regional targeting.

Cybersecurity analysts note that these records do not solely stem from recent incidents. Instead, they represent a fusion of historical breach data, malware-extracted credentials, and recycled dumps previously circulated in the cyber underground. This patchwork, repackaged and redistributed over time by multiple actors, creates not only volume, but volatility. The same credentials may appear across several datasets, making precise impact assessment difficult.

While headlines often focus on numerical magnitude, industry observers suggest the more critical concern lies in the leak's structure. This is not just data, it is an actively weaponised resource. With usernames, passwords, tokens, and cookies all bundled together, the leak provides threat actors with ready-to-use pathways for account takeovers, credential stuffing, and lateral phishing attacks. In some cases, these footholds can be leveraged further into ransomware deployments or deeper network intrusions.

Security professionals have responded with urgency. Users are advised to immediately reset passwords for critical accounts, especially those reused across multiple services, and to enable multi-factor authentication where possible. Equally vital is the practice of monitoring for unauthorised logins or behavioural anomalies that may signal account compromise.

Looking ahead, the incident reinforces a key tenet of cybersecurity that remains as relevant today as it was a decade ago: access credentials, when mishandled, represent one of the most persistent and exploitable vulnerabilities in the digital ecosystem. In this case, it is not merely the theft of data that is concerning, but the slow, structural accumulation of risk over time.

Zoomcar Data Breach

On 09 June 2025, mobility platform Zoomcar fell victim to a significant cyber incident, one that not only disrupted its internal operations but also raised deeper concerns about the security of personal-vehicle linked data in India's rapidly digitising ecosystem. Several employees reportedly received direct messages from an unidentified threat actor, who claimed to possess access to sensitive consumer records. These communications, described as both threatening and specific, marked the onset of a data breach that has since drawn nationwide attention.

The company initiated an immediate internal investigation, supported by external cybersecurity specialists. Preliminary findings confirmed that the breach had exposed personal information of approximately 8.4 million users. The compromised dataset included field names like full names, contact numbers, email IDs, residential addresses and car registration details. While no financial data or user credentials appear to have been accessed, experts warn that the exposed combination of personal and vehicular data still presents material risks.

The exact method of infiltration remains unclear, though the attackers' calculated approach, particularly their outreach to internal personnel, suggests a deliberate and potentially coordinated campaign. Industry analysts believe the breach is consistent with recent regional trends involving credential-harvesting malware and socially engineered intrusions targeting consumer tech firms.

Zoomcar has confirmed that its operational platforms remain intact and that user services continue without disruption. However, the breach's implications extend well beyond operational continuity. Cybersecurity professionals note that pairing user contact details with identifiable vehicle registration numbers creates new opportunities for targeted fraud. Threat actors may exploit this dataset to orchestrate highly customised phishing attempts or impersonation schemes that appear credible at first glance.

For end-users, the advisory is clear: remain alert to unsolicited messages, particularly those referencing Zoomcar, vehicle ownership, or location-linked services. Experts emphasise that even in the absence of passwords or banking data, sophisticated attackers can exploit contextual personal information to induce trust and gain further access.

From a corporate standpoint, Zoomcar now faces a multi-dimensional challenge. Alongside forensic containment, the company is managing potential legal exposure and reputational damage, both of which will likely evolve as authorities continue to investigate the matter. Company officials have stated that they are working closely with law enforcement agencies and are reviewing internal data protection protocols in response.

As application-based services increasingly consolidate personal, locational, and transactional data into singular user profiles, ensuring their protection becomes not just a technical challenge but a policy imperative. The Zoomcar breach, though significant in itself, may ultimately serve as a precursor to broader reforms—prompting a re-evaluation of how digital services handle hybrid datasets, and what role institutional oversight must play in that process.

In an era where digital identity extends well beyond logins and passwords, this incident serves as both a cautionary tale and a call to strengthen the foundational pillars of cybersecurity, from platform governance to user awareness, and from sector-specific standards to national regulation.

Digital Sovereignty: From Abstract to Concrete

Digital sovereignty refers to a nation's ability to control and govern its digital infrastructure, data flows, and technology standards. It emphasizes local jurisdiction over data storage, cybersecurity, and platform regulation. By mid-2025, digital sovereignty has moved from rhetoric to structured implementation. Governments are legislating it, institutionalising it, and increasingly, linking it to national competitiveness and security.

Expanding Regulation in a Fragmented Legal Landscape

The European Union continues to anchor global momentum with the Digital Markets Act (DMA), Digital Services Act (DSA), and the Artificial Intelligence Act (AI Act)—collectively designed to safeguard user rights and establish boundaries around platform power and emerging technologies. Regulatory analysts describe this shift as a deliberate move towards "rule-based digital order." Beyond Europe, countries such as India have introduced the Digital Personal Data Protection Act, 2023 (DPDP Act). Countries like Brazil, South Korea, and Kenya are also tightening their data governance frameworks.

Strategic Autonomy in a Multipolar Digital Order

This assertiveness is not merely legal, it is geopolitical. The U.S., EU, and China are advancing distinct digital governance models, each seeking to shape global standards and reduce dependence on rival infrastructure. Observers believe that these policies reflect deeper structural goals: developing local capacity, protecting strategic assets, and asserting influence over the rules that govern cross-border data flows.

Cloud Infrastructure and the Rise of Sovereign Architectures

One of the most visible manifestations of sovereignty is the sovereign cloud. Public institutions and regulated industries are deploying cloud infrastructures built to meet local residency and legal requirements. Initiatives like GAIA-X and the AWS European Sovereign Cloud are shaping a new standard—one that blends scale with jurisdictional clarity. For many governments, this architecture is no longer optional. It is becoming a baseline requirement in sectors where data sensitivity intersects with national oversight.

Cybersecurity: From IT Function to National Strategy

Rising geopolitical tensions have underscored the security dimension of digital sovereignty. Cyberattacks targeting energy grids, telecom systems, and election infrastructure have pushed governments to treat cybersecurity as integral to national defence. Countries are responding by investing in domestic semiconductor capabilities, funding AI and quantum research, and limiting exposure to foreign vendors. Incidents like SolarWinds and the Colonial Pipeline attack have become case studies in why digital infrastructure must now be protected as critical infrastructure.

Innovation, Open Source, and Local Capability Building

Across Europe and parts of Asia, governments are actively investing in homegrown platforms, open-source technologies, and digital skilling initiatives. Denmark's pilot of open-source software in government and India's expansion of open digital public infrastructure reflect a broader movement towards self-reliant technology ecosystems. These efforts, analysts argue, are essential to long-term strategic autonomy—not simply a hedge against foreign dependency.

Public Sentiment and Digital Self-Determination

At the citizen level, the conversation is shifting. Grassroots campaigns in Europe are calling for community-based data governance, while voices from the Global South are increasingly vocal about digital colonialism. Rising citizen awareness is influencing national digital strategies, and in some cases, shaping how public institutions approach platform governance.

Digital sovereignty is no longer theoretical, it is becoming the foundation of modern digital policymaking. Yet, as states assert control, they must navigate a fundamental tension: sovereignty demands national authority, but digital systems remain inherently global.

Infosecurity Europe: Securing the Next Digital Decade

Infosecurity Europe 2025, held from 03-05 June, 2025 at the ExCeL Centre in London, United Kingdom marked its 30th edition. With over 13,000 professionals in attendance, the gathering served as a testament to the maturity and urgency of cybersecurity dialogue across Europe and beyond.

This year's event unfolded at a time of considerable flux in the sector. Generative AI, regulatory turbulence, and the deepening nexus between geopolitics and cyber policy have collectively sharpened the stakes. Against this backdrop, the conference's theme, blending high-level strategic clarity with applied technological insight, felt not only timely but essential.

The programme was structured across eight curated stages, each examining distinct threads of the cybersecurity fabric. At its core remained the Keynote Stage, where a diverse set of voices, from senior CISOs and government advisors to academic researchers, shared lessons from frontline defence and long-view policy evolution. A particularly thought-provoking opening address by Professor Brian Cox explored the implications of quantum computing and cosmic uncertainty for information integrity.

Newly introduced this year, the AI & Cloud Theatre quickly became a locus of attention. Here, discussions ranged from the rising risk of AI-powered phishing and deepfakes to the security of large language models and cloud-native architectures. Industry analysts observed that the session mix reflected a sector grappling with scale, complexity, and regulatory readiness, particularly as the EU and UK continue to refine AI governance frameworks.

In contrast, the Cyber Strategies zone—developed in collaboration with leading CISOs—offered a more grounded perspective. Discussions emphasized board-level engagement, risk governance, and operational resilience. Observers noted a growing convergence between security and business continuity planning, suggesting a more integrated approach to enterprise risk in years ahead.

Skill-building remained a key priority. SANS Institute masterclasses focused on strengthening cloud security practices and embedding security culture at scale. Hands-on workshops provided attendees with a space to experiment with AI-driven automation tools, though some participants quietly noted that critical domains, such as operational technology (OT) security, received less visibility than warranted, given rising threats to industrial systems.

Notably, the event's celebratory undertones, the 30th anniversary party and private executive gatherings, never distracted from the seriousness of its content. If anything, the mood reflected a sector that is aware of its growing relevance and responsibilities. As state-sponsored threats escalate and cybersecurity moves higher on the political agenda, gatherings like Infosecurity Europe are becoming as much about cross-border collaboration as they are about product innovation.

DIY Defence: Outsmarting Phishing Attacks

In the domain of cybersecurity, phishing continues to stand as one of the most pervasive and mutating threats. Phishing is a type of cyberattack where attackers impersonate a trustworthy entity through email, text, or calls to trick individuals into revealing sensitive information about them like their passwords or financial details. These attacks typically hinge on deception, with perpetrators posing as credible institutions or individuals to coax recipients into divulging sensitive information

Verify Before You Click

Cybersecurity professionals advocate a simple yet often overlooked habit, verifying sources independently before interacting with links or attachments. This involves navigating directly to a website via a browser rather than following embedded URLs. A frequent tactic among cybercriminals is to replicate legitimate domains with slight variations, extra hyphens, character swaps, or deceptive domain endings, to entrap the unsuspecting.

If It Sounds Too Good to Be True, It Probably Is

Phishing often leverages human psychology, luring users with promises of windfall gains, unclaimed prizes, or urgent refunds. These offers typically demand swift action, preying on curiosity and impulsiveness. Cybersecurity experts reiterate well-worn yet crucial advice, if a deal seems too generous or urgent to be true, it likely isn't. The prudent approach is to verify any such claims through official channels rather than through links embedded in suspicious messages.

Strengthen Your Digital Defence

Cyber resilience begins with strong digital hygiene. You should keep your devices and applications updated, as it addresses known vulnerabilities that threat actors frequently exploit. Creating unique, complex passwords for each account further narrows the attack surface. Crucially, enabling multi-factor authentication (MFA) adds an additional safeguard, one that can thwart attackers even if passwords are compromised.

Strengthen Your Digital Defence

Cyber resilience begins with strong digital hygiene. You should keep your devices and applications updated, as it addresses known vulnerabilities that threat actors frequently exploit. Creating unique, complex passwords for each account further narrows the attack surface. Crucially, enabling multi-factor authentication (MFA) adds an additional safeguard, one that can thwart attackers even if passwords are compromised.

Use Security Tools and Filters

While no security tool offers absolute protection, you should deploy trusted antivirus software and enable spam filters to significantly reduce exposure to phishing and other cyber threats. Additionally, maintaining regular backups, ideally stored on encrypted cloud services or isolated external drives, ensures a viable path to recovery in the event of ransomware attacks or data breaches.

Report Incidents to Strengthen Collective Defence

Timely reporting of phishing attempts is not merely a defensive measure but is a civic responsibility. Whether within organisational frameworks or through national cyber response portals, reporting helps in mapping threat patterns, raising public alerts, and pre-empting further harm.

As phishing tactics become more sophisticated, ranging from impersonating tax departments to mimicking popular e-commerce platforms—awareness must evolve at the same pace. Recent campaigns have even invoked the likeness of public figures to build false credibility. Experts note that fostering digital literacy within families, workplaces, and communities is the most sustainable form of defence. In a hyper-connected world, knowledge may well be the most effective firewall.

Athenian Tech

Contact Us

www.atheniantech.com

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