HKIT SECURITY SOLUTIONS

HKIT
CYBER EXCELLENCE

JULY - 2025

NEWSLETTER

Latest Updates in Security

At HKIT Security Solutions, we specialize in providing cutting-edge cybersecurity services and data protection strategies tailored for modern digital threats. Our team of experts brings deep technical knowledge, regulatory insight, and industry best practices to secure your infrastructure, applications, and data. From vulnerability assessments and penetration testing to compliance consulting and SOC support, we deliver end-to-end security solutions to organizations of all sizes. With a strong focus on proactive defense and risk mitigation, we empower businesses to stay ahead of evolving cyber threats. Trusted by clients across sectors, HKIT Security is committed to building a safer digital ecosystem.

Need Expert Security Services?

Looking for professional support in strengthening your organization's cybersecurity posture? HKIT Security Solutions offers a full suite of services, including:

- ISO 27001 / 27701 Implementation & Consulting
- Phishing Simulation Services
- Advance Anomaly Detection Services
- Vulnerability Assessment & Penetration Testing (VAPT)
- Security Infrastructure Audits & Gap Analysis
- Data Privacy Compliance (DPDP, GDPR)
- Cybersecurity Policy & Governance Consulting

Visit us at: www.hkitsecurity.com

Security Basics for Everyone

Think before you click—phishing scams often look like real emails or messages. Use a strong password that's hard to guess, and never reuse the same password on different sites. Keep your devices updated so you're protected against the latest threats. Don't install apps or software from unknown sources. Always back up important data in case of accidental loss or ransomware. Remember, staying secure online starts with small daily habits.

CYBER CRIME NEWS

- A 57-year-old South Mumbai businessman lost ₹4.21 crore in an online investment scam run via a fake WhatsApp group posing as SBI Caps Securities.
- Fraudsters used a counterfeit trading app to show fake profits and lured the victim through an Instagram ad and manipulated communications.
- The scam was exposed when the victim was asked to pay a hefty “service management fee” to withdraw fictitious returns of ₹52.88 crore. The case is under South Cyber Police investigation.

timesofindia.indiatimes.com

- On July 6 in Lucknow, four fraudsters were arrested for scamming retired IVRI scientist Shukdev Nandi out of ₹1.29 crore.
- The criminals impersonated CBI and Bengaluru Police officials via WhatsApp, using official logos and false allegations about Aadhaar misuse.
- Through psychological coercion over three days, they convinced the victim to transfer funds to multiple accounts under the pretense of an “audit.”

www.coastaldigest.com

Data Privacy (DPDP Act) Developments

- By July 2025, India finalized the Digital Personal Data Protection (DPDP) Rules 2025, strengthening the country’s data privacy framework.
- Key provisions include registered consent managers and mandatory parental consent for processing children’s data.
- The rules aim to align with global standards like GDPR while addressing India-specific data protection needs.
- Google Pay, PhonePe, Amazon Pay, and the NPCI have jointly appealed for an exemption from DPDP Act’s consent mandate for every digital transaction.
- The companies argue that requiring explicit user consent per transaction could disrupt operational workflows and degrade the user experience.
- This move highlights industry concerns over balancing privacy compliance with practical usability in India’s fast-growing digital payments sector.

www.privacyworld.blog
www.uprootsecurity.com

GDPR & Global Compliance News

- In July 2025, the European Data Protection Board (EDPB) announced enhanced GDPR support for SMEs, promoting scalable compliance and inter-regulatory collaboration across the EU.
- Regulators have shortened breach reporting deadlines to 48 hours (especially in healthcare) and updated rules for cross-border data transfers and cloud provider agreements.
- With GDPR fines exceeding €3 billion in 2025, these updates highlight stricter enforcement and a growing focus on both data protection and business feasibility.

Chrome Attacked, CoinDCX Breached – July 2025's Top Cybersecurity Incidents

On July 19, 2025, leading Indian crypto exchange CoinDCX suffered a massive security breach, with ₹378 crore (~$44.2 million) siphoned from an internal operational account. The attack was traced to compromised credentials from a Bengaluru-based engineer's laptop.

- Authorities suspect involvement of the North Korean Lazarus Group; one arrest has been made.
- Customer wallets remain unaffected, with assets stored in segregated cold wallets.
- CoinDCX has pledged to cover all losses through its treasury reserves.
- A recovery bounty program has been launched to track stolen assets.
- This incident ranks among India's largest crypto-related breaches to date.

www.hindustantimes.com

In mid-July 2025, Google patched a critical zero-day vulnerability—CVE-2025-6558—in Chrome, which was actively exploited in the wild.

- The flaw, identified by Google's Threat Analysis Group, involved improper input validation in Chrome's ANGLE and GPU components.
- Attackers leveraged malicious HTML pages to potentially escape the browser sandbox.
- Google issued an emergency security update and strongly urged users to patch immediatel

thehackernews.com