The Tutors Academy The Tutors Academy The Tutors Academy The Tutors Academy The Tutors Academy The Tutors Academy The Tutors Academy The Tutors Academy The Tutors Academy The Tutors Academy

Cyber Hygiene in India:

Growing Digital Security Risks and Solutions

Cyber Hygiene in India Latest News

COVID-19's effects still linger in the physical world. In a similar way, a "digital pathogen" has spread across cyberspace. This pathogen is poor cyber hygiene. It has touched almost every sector, even authentication agencies.

The term "cyber hygiene" is often called the first line of defence against cybercrime. It has gained attention after serious security scares hit financial institutions and public bodies.

India's digital economy is expanding fast. Because of this, cyber hygiene is no longer just an optional practice. It has become a critical pillar of economic stability.

What Is Cyber Hygiene?

- *Coined by Internet pioneer Vinton Cerf in 2000, during his testimony before the US Congress' Joint Economic Committee.*
- *Refers to routine practices that keep digital systems, devices, and data secure.*
- *Operates on a principle similar to public health: prevention is invariably cheaper than the cure.*

Neglecting basic cyber hygiene can be as costly as ignoring an epidemic — the damage extends beyond money lost to disrupted businesses, compromised identities, regulatory liabilities, and eroded public trust.

The Rising Cost of Data Breaches

Globally, the average cost of a data breach declined 9% YoY to $4.44 million (IBM 2025 report).

In India, however, costs are rising:

IBM 2026 report (August 2026): Average breach cost in India reached ₹25.5 crore, up 15.9% YoY.

Average breach compromised 39,500 records, up from 38,200 the previous year.

Financial services sector faced an even steeper average cost: ₹40.9 crore per breach.

These IBM figures capture the total organisational cost, including detection, investigation, recovery, business disruption, and reputational damage.

No Sector Is Immune

Recent incidents highlight the breadth of exposure: reported/suspected data exposures at State Bank of India and HDFC Bank (banking sector); issues at the Central Board of Film Certification (CBFC) (government body); and the eMudhra incident (digital-certification company).

Why This Matters: Banks hold financial/identity data; sovereign bodies manage sensitive public records; certification bodies underpin digital trust itself. A vulnerability in any one of these can have far-reaching consequences — security must extend across the entire technology supply chain.

The eMudhra incident specifically showed the danger wasn't just data theft, but the potential undermining of the trust mechanisms that secure online communications — underlining why digital-certification infrastructure needs rigorous testing and verification.

The Tutors Academy The Tutors Academy The Tutors Academy The Tutors Academy The Tutors Academy The Tutors Academy The Tutors Academy The Tutors Academy The Tutors Academy The Tutors Academy

India's Mounting Cyber-Fraud Losses

As per the Union Home Ministry's Parliament reply, financial cyber-fraud losses have surged dramatically:

2021: ₹551 crore

2022: ₹2,290 crore

2023: ₹7,465 crore

2024: ₹22,848 crore

2025: ₹22,495 crore (a marginal dip)

RBI Data (FY2023-24): Banks reported 36,075 fraud cases involving ₹13,930 crore; of these, 29,082 cases related to cards/internet banking, accounting for ₹1,457 crore.

Why Digital Growth Amplifies Risk

India's Integrated Financial Ecosystem — UPI, mobile banking, internet banking, digital lending — creates a complex, interconnected architecture where a vulnerability at one point can have consequences far beyond it.

Scale Indicator: As per NPCI data, UPI processed ~186 billion transactions in 2024-25 — underscoring the massive scale of India's digital payments infrastructure, and correspondingly, the scale of potential exposure.

Building Cyber Resilience: A Multi-Level Approach

Individual Level:

Use unique, strong passwords/password managers.

Enable multi-factor authentication.

Install software updates promptly.

Avoid clicking suspicious links.

Corporate Level:

Embed security into operations via timely patching, encryption, secure software.

Conduct phishing simulations, independent penetration testing, and regular incident-response exercises.

Sovereign/regulatory Level:

RBI has issued cybersecurity and IT-governance requirements for regulated entities.

CERT-In coordinates responses to cybersecurity incidents nationally.

Conclusion

As India accelerates toward a digitally empowered economy, the data makes clear that cyber hygiene can no longer be treated as a peripheral compliance checkbox — it must become embedded institutional culture.

With breach costs in India rising even as global averages decline, and fraud losses having grown more than 40-fold between 2021 and 2024, the stakes extend far beyond individual financial loss to the broader credibility of India's digital finance ecosystem.

The Tutors Academy The Tutors Academy The Tutors Academy The Tutors Academy The Tutors Academy The Tutors Academy The Tutors Academy The Tutors Academy The Tutors Academy The Tutors Academy

Topic For Group Discussion (GD) And Lecturette For SSB Interview

Since absolute security remains unattainable in practice, the realistic goal — across individuals, corporations, and regulators alike — must be minimising risk, detecting threats early, containing damage swiftly, and recovering fast, ensuring that the pace of India's digital transactions is matched by the integrity of the systems and institutions underpinning them.

