The digital pathogen: Why cyber hygiene is no longer optional | Explained

The term cyber hygiene, the first line of defence against cybercrime, increasingly got into the vocabulary after financial institutions and public bodies suffered serious security scares

Updated - October 30, 2026 12:45 pm IST

SANTOSH V. PERUMAL



Image used for representation purpose only. | Photo Credit: Getty Images/iStockphoto

Even as the stains of Covid-19 has yet to recede entirely in the physical world, the pathogen in the digital age — poor cyber hygiene — has found its foothold across the sectors that it has not even spared authenticating agency.

The term cyber hygiene, the first line of defence against cybercrime, increasingly got into the vocabulary after financial institutions and public bodies suffered serious security scares.

In cyberspace, neglecting basic hygiene can be as deadly as ignoring an epidemic, the opportunity cost of which is not merely in money lost, but disrupted businesses, compromised identities, regulatory liabilities and above all eroded public trust.

Digital trust, like public health, depends upon a simple principle: prevention is invariably cheaper than the cure.

It was Internet pioneer Vinton Cerf, who coined the term cyber hygiene in 2000, when he used it in his testimony before the US Congress' Joint Economic Committee.

"Good cyber hygiene is essential for staying safe in today's digital world. Simple and responsible online practices can go a long way in protecting your personal and financial information," says a mail from a nationalised bank to a customer.

Global average cost of a data breach declined to $4.44 million, down 9% year-on-year (YoY), while it rose in India, an IBM 2025 report said.

The IBM's 2026 report, released in August, puts average cost of a data breach in India at ₹25.5 crore, up 15.9% YoY. The breach compromised 39,500 records against 38,200 in the previous year. The financial services sector faced an even higher average cost of ₹40.9 crore per breach.

The IBM report measures the average total organisational cost of a breach, including detection, investigation, recovery, business disruption and reputational damage.

The data assumes importance especially in the country's systemically important banking sector, as compromised information can lead to identity theft, financial fraud and further attacks on customers.

Against this backdrop, reported or suspected data exposures involving State Bank of India and HDFC Bank highlight the country's rising and sophisticated cybersecurity challenge.

Cyber risks do not discriminate sectors as seen from reported issues involving in the Central Board of Film Certification (CBFC) and digital-certification company eMudhra.

Banks hold financial and identity data, sovereign bodies manage sensitive public records and certification bodies underpin digital trust. Hence, vulnerability in any of these could lead to far-reaching consequences. Security must therefore extend across the entire technology supply chain.

In a reply to the Parliament, the Union Home Ministry reported increasing financial cyber-fraud losses from ₹551 crore in 2021 to ₹2,290 crore in 2022, ₹7,465 crore in 2023, ₹22,848 crore in 2024 and marginally dipping to ₹22,495 crore in 2025.

Per Reserve Bank of India (RBI) data, in FY2023–24, banks reported 36,075 fraud cases involving ₹13,930 crore. Of these, 29,082 cases related to cards or internet banking, which accounted for ₹1,457 crore.

However, the central bank data comes with a caveat that the amount involved in reported frauds is not equivalent to actual loss incurred. Recoveries may reduce the loss, and frauds reported in one financial year may have occurred years earlier.

Notable international historical cases such as Equifax (2017) and Capital One (2019) illustrate the potential financial consequences in terms of settlements and other judiciary costs.

Even as India's rapid digital transformation has widened and deepened the reach of the banking industry, it has exposed the sector more to cyber risks.

The integrated financial ecosystem — comprising UPI, mobile banking, internet banking and digital lending — complicated the complex architecture that the vulnerabilities at one point can have dire consequences far beyond it.

The National Payments Corporation of India data suggest that UPI processed around 186 billion transactions during 2024–25, illustrating the scale of digital payments infrastructure.

This growth makes cyber hygiene — the routine practices to keep digital systems, devices and data secure — indispensable for all stakeholders alike — banks, customers, technology vendors, payment intermediaries and regulators.

In view of this, campaigns have already been strengthened on the need for effective cyber hygiene action at various levels.

Individual level cyber hygiene calls for employing unique, strong passwords/password managers, enabling multifactor authentication, installing software updates and avoid clicking suspicious links.

Corporate level measures suggest embedding security into operations with timely patching, encryption, secure software, phishing simulations, independent penetration testing and regular incident-response exercises.

The eMudhra incident highlighted that the near danger was not simply the theft of information but the likely undermining of trust mechanism to secure online communications. It rather showed

why trusted digital-certification infrastructure needs rigorous testing and verification.

The sovereign and regulator level cyber hygiene looks at collective resilience. In this regard, RBI has issued cybersecurity and IT-governance requirements for regulated entities, while CERT-In coordinates responses to cybersecurity incidents.

And finally...

Just as the pace of transactions is important, the integrity of systems and institutions behind it is integral to the credibility of digital finance.

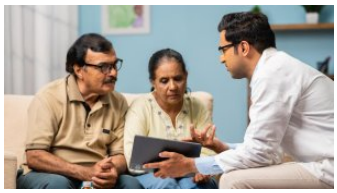
Absolute security is seldom achievable in a real world; aim should rather be minimising risk, detecting threats early, containing damage, and recovering fast.

Cyber hygiene, which is no longer an individual option or corporate compliance, has become a critical pillar of collective economic stability.

As India moves towards a digitally empowered economy, cyber hygiene must become more than a compliance checkbox — it must be a culture.

Published - October 30, 2026 11:46 am IST

In Case You Missed It



Educated but illiterate? How Indians have little health,...



India set to simplify visa forms



SBI Q2 profit rises 14.3% to ₹23,038 crore; eyes NIM abo...



Anthropic says revenue surged 1100% ahead of IPO



Experts call for cross-sector collaboration to implement On...



Playbook to overcome inflation



The worm that broke the internet



How AI training models could compromise privacy