

# Global Mega-Breach:

## *16 Billion Passwords Leaked*

Is your organisation **breach-resilient**?

---

# The Breach that Shook the Internet

- 16 Billion Login Credentials Leaked
- Credentials from Apple, Google, Facebook, Telegram & more found on dark web
- One of the largest fresh breaches, not recycled data
- Likely result of malware, infostealers, and credential stuffing attacks
- Enterprise security is under threat

# Legal Fallout Under India's DPDPA

- Credentials means personal data; this triggers legal obligations even if leak originated outside India
- Under DPDPA, breaches of personal data must be reported to Data Protection Board & affected users
- Incident Response Management plan should be in place to tackle situations like these

# Key Takeaways for Corporates

- Activate breach response playbook
- Implement 2FA / passkeys across systems
- Conduct immediate malware & device hygiene checks
- Update vendor contracts & data processing terms
- Begin Data Protection Impact Assessments (DPIAs)

# Strategic Advantage *via* Global Compliance

- Harmonize DPDPA with GDPR, CCPA, etc. for multi-jurisdictional operations
- Build Zero Trust Architecture
- Appoint DPOs with breach notification powers
- Integrate legal & IT for continuous monitoring
- Embed privacy-by-design into all workflows

# Time to Act, Not React

Is your organisation breach-resilient?

Review your:

- Credential security protocols
- Data breach/incident response plan
- Employee training modules
- Insider risks

In the era of DPDPA, privacy is not optional.

# Get Started.

---

Have Something Else To Add?

We are only an e-mail away  
[dataprivacy@amlegals.com](mailto:dataprivacy@amlegals.com)

#RespectData

[www.amlegals.com](http://www.amlegals.com)