



Webel[®]
opportunities infinite



CyberPeace

WORLD SOCIAL MEDIA DAY 2025

Unlocking the Power of Protection

30th June – A Day to Rethink Safety

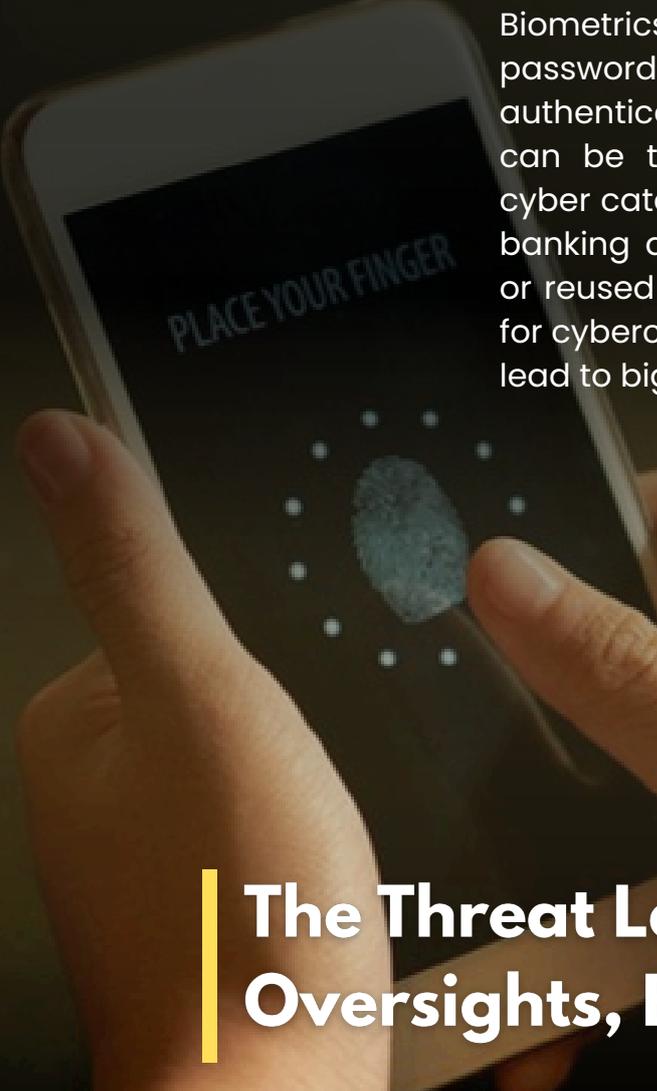


Rethinking Digital Safety in a Hyperconnected World

World Social Media Day is more than a calendar date; it's a collective call to action. A reminder to evaluate and strengthen our social media accounts and lead a balanced digital life. The safeguarding of our digital persona and space is of prime importance as that will enable us to lead a productive and positive digital life.

A major tool in our cybersecurity arsenal is the **PASSWORD**. Passwords constitute the first line of defence in most digital systems. They are the keys to our identity, privacy, and digital safety.

Why Do Passwords Still Matter in the Age of Biometrics and AI?



Biometrics and AI offer convenience, but passwords still underpin the majority of authentication systems. A strong password can be the fine line between safety and cyber catastrophe, from email accounts and banking apps to government portals. Weak or reused passwords are the easiest targets for cybercriminals, a small oversight that can lead to big consequences.

The Threat Landscape: Small Oversights, Big Consequences

With phishing, credential stuffing, data breaches, and SIM swap attacks on the rise, even tech-savvy users fall prey to sophisticated traps. Many users continue to use passwords like "123456" or "password," unaware of how easily they can be cracked. The reality is: our password can either be our greatest vulnerability or our personal cyber armour.



Passwords: Our Digital Body Armour

A strong password is thus essential and creating one doesn't have to be complicated. The trick is to aim for longer passwords (12 to 16 characters) to boost their strength. The second tip is that we need to make them unpredictable by mixing uppercase and lowercase letters, numbers, and special characters.

The third tip is to avoid obvious choices like **names, birthdays, or commonly used passwords** such as "admin123." Instead, we need to opt for unique and memorable passphrases that are easy for us to remember but difficult for others to guess, something as simple as **CalcutA@_2045#** can do the trick.

Evaluating a Sample Password: **Kangaroo@2025**

Total Length: 13 characters

Uppercase Letters: 1

Numerical Digits: 4

Special Characters: 1

Guessability: ⚠️ High includes repeated letters and the current year

Tip: Swap out certain letters with symbols or unexpected characters for extra strength





How to Store & Manage Passwords Like a Pro

Use a Password Manager (Open and paid softwares available)

Enable 2FA (Google Authenticator, Authy)

Update passwords every 3–6 months

Never reuse passwords across accounts

Why an Authenticator App Can Enhance Digital Safety

An authenticator app adds a vital second layer of defence to our online accounts, making it significantly harder for attackers to gain access even if our password is compromised. Unlike SMS-based OTPs, which can be vulnerable to interception through methods like SIM-swapping, authenticator apps generate secure, device-based codes that are far more reliable. Trusted options such as Google Authenticator, Microsoft Authenticator, Authy, and Duo Mobile offer robust protection and are highly recommended for anyone looking to strengthen their digital security.





The Growing Importance of Passwords

In today's digital landscape, our password is more crucial than ever. Our smartphone holds personal information that defines our identity. Our email account acts as the central hub for accessing nearly all our online services. Social media platforms reflect our thoughts, opinions, and digital presence, while banking apps protect our hard-earned money. At the heart of securing all these critical aspects of our life lies one simple yet powerful tool: a strong password.



Password Rules to Live by

- Use **Passphrases**, not simple passwords. Eg: 1luv\$b\$g\$r@MD(I love burger from McDonald).
- **Children & Teens:** Share passwords only with guardians
- **Never reuse** passwords
- Use a **Password Manager**
- Use **MFA** wherever possible; if not, then **2FA** has to be activated

More Safety Tips We Wish We Had Followed Sooner:

- Check if our data has been breached at haveibeenpwned.com
- Never click on suspicious "Reset Password" links
- Use privacy screens in public
- Handhold children and seniors into the world of digital safety
- Avoid shared/public devices and networks for login
- Not to jot down passwords on sticky notes or in phone
- Carry out a monthly digital hygiene check

A Thought to Remember:

**"Our password is not just a key.
It's the firewall between our
Digital Security and a hack."**



Government Initiatives

The Cyber Security Centre of Excellence (CS-CoE) under the aegis of Department of IT&E has published various advisories, posters, booklets, comics to stress the importance of cyber hygiene practices.

A Few prominent ones are listed below:

Cyber Hypnosis comics.

Cyber Hygiene Handbooks.

Cyber Security Guidelines for Government Employees.

Cyber Security- A knowledge for Safer tomorrow.

Additionally **"Data Privacy Guidelines"** were published to empower individuals, government agencies to take charge of their data responsibly and ethically. **"The Anonymiser Hackathon"** was conducted to invite useful solutions to anonymize personally identifiable information. Moreover, capacity building through training and awareness events remains a regular activity of CS-CoE.

THE ANONYMISER HACKATHON
Supported by
Department of Information Technology and Electronics
Government of West Bengal

An anonymiser can anonymise personally identifiable information from given sets of data, in a way that any combination of auxiliary datasets cannot deanonymise the same, where personally identifiable information includes a person, entity, or even an incident. This anonymiser can change the way we see and experience the current data revolution. **Department of IT & Electronics, Government of West Bengal** invites academicians, students, and technologists from across the globe, to participate in **The Anonymiser Hackathon** and develop India's first data anonymiser.

Phase 1 Ideathon
16th March - 15th April
Round table discussion in hybrid mode on various use cases and problem statements and shortlisting the problem statements

Phase 2 Solution development
16th April - 15th May
A 30-day exercise, where the participants will work with relevant support from various mentors on creating a live model of the proposed anonymiser.

Phase 3 Grand Finale
Last week of May
A half-day grand event where evaluations of submitted projects shall be done under the expert evaluation committee. Post the same, the winners shall be awarded.

3 Consolation Prizes of ₹25k Each

1st ₹2.5 Lacs
2nd ₹1.75 Lacs
3rd ₹1 Lacs

West Bengal Data Privacy Guideline 2023
Department of IT & Electronics | Govt. of West Bengal

West Bengal has formulated a comprehensive Data Privacy Guideline to demystify the world of data privacy and empower individuals, government bodies and organizations to take charge of their data in a responsible and ethical manner. Through knowledge and informed action, we can collectively ensure that data remains a force for good, benefitting society while respecting the fundamental right to privacy.

Key Definitions:

1. Data Fiduciary: Anyone deciding what data will be collected, how it will be collected and the purpose of its use.
2. Data Processor: Anyone who processes data on behalf of Data Fiduciaries based on their instructions.
3. Data Principals: Individuals or organizations whose personal data is being processed

Key Principles:

1. The principle of consented, lawful, and transparent use of personal data.
2. The principle of purpose limitation- use of personal data only for the purpose specified at the time of obtaining consent of the data principal.
3. The principle of data minimisation- collection of only as much personal data as necessary to serve the specified purpose.
4. The principle of data accuracy- ensuring data is correct and updated.
5. The principle of storage limitation- storing data only till it is needed for the specified purpose.
6. The principle of reasonable security safeguards.
7. The principle of accountability through adjudication of data breaches.

Salient Features:

- CONSENT**
Empowers individual control by allowing people, organization, or government to decide how their personal data is used.
- RESOURCE CREATION AND CAPACITY BUILDING**
• Significant Data Fiduciary should appoint a Data Protection Officer and a Data Protection Auditor.
• Conduct general & specialized awareness programs for all employees to foster a culture of data privacy.
- DATA RETENTION**
Based on the criticality, purpose, nature or type of data, the data should be retained as per West Bengal State Electronic Data Centre Storage, Sharing and Electronic Data Retention Guidelines, 2020.
- PRIVACY NOTICE**
Promotes transparency, enable informed consent, comply with legal requirements, empower data principals to exercise their data rights, demonstrate accountability, and mitigating legal and financial risks for the organization or government or individual (both data principal & data fiduciary).
- DATA ANONYMIZATION**
Transforming or altering personal identifiers (Personally identifiable information) from a dataset to protect individuals' privacy and identity while preserving data utility through techniques like removing explicit identifiers, aggregation, generalization, adding noise, etc.

<https://web.gov.in/> | <https://www.webel.in/>



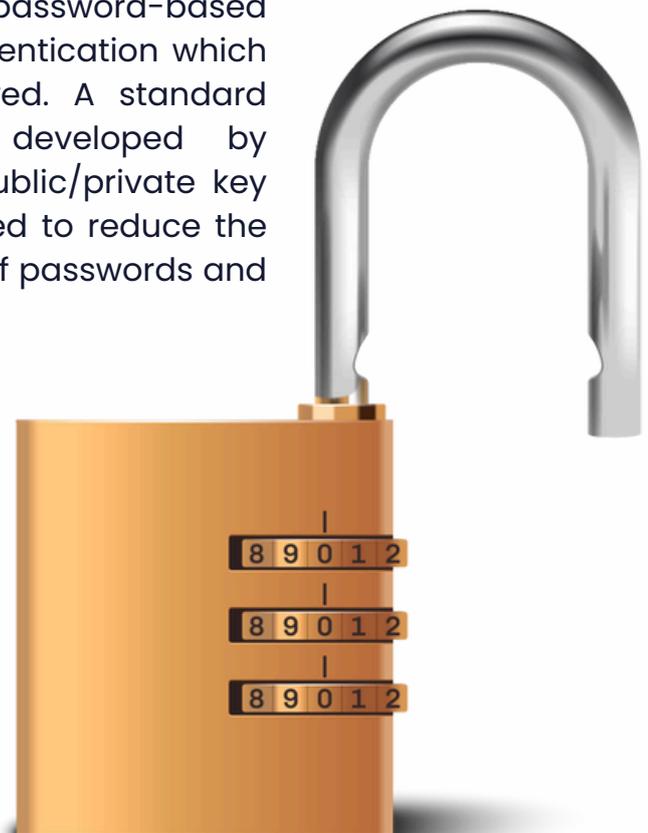
Future Ahead : Towards A Cyberspace With Less And Safe Passwords

The usage of passwords hinges on two basic principles: **Uniqueness and Complexity.**

However, due to the increase in e-services and social networking, it becomes increasingly difficult to use unique passwords on multiple platforms. This results in an unintentional violation of the **“uniqueness”** of a password making it redundant and vulnerable.

Additionally, as all passwords have to follow the set password policy (a mix of capital letters, small letters, numerals and special characters), every netizen creates a password, that, although complex, is simpler to remember, which violates the “complexity” principle. Lastly, the continual data breaches and cyber-attacks may expose even the most difficult passwords.

Given the inherent weakness of password-based authentication, the shift to key-based authentication which is entirely password less may be followed. A standard namely FIDO (Fast Identity Online) developed by international forums which is based on public/private key pairs instead of passwords may be adopted to reduce the risks associated with the conventional use of passwords and eliminate the risk of cyber-attacks.





Conclusion: Share Knowledge, Not Access

This **#WorldSocialMediaDay**, let us pledge to raise awareness about the importance of strong password practices. Whether it's our friends, family members, colleagues, or students, everyone can benefit from better digital hygiene. By sharing these simple yet powerful tips, we can collectively build stronger defences against cyber threats and protect our online identities, one secure password at a time.

