
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: 1luvb$g$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:

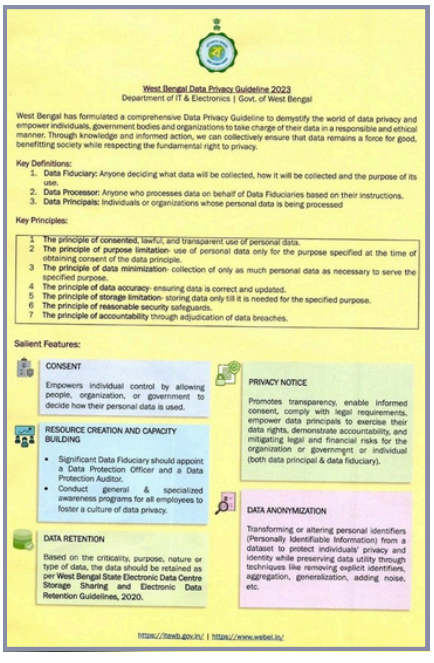
Cyber Hypnosis comics.

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.



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.