

Think your password is safe? It might be easier to crack than you think

From reusing the same login across various platforms to relying on '123456' as the sole line of defence, poor password practices continue to leave billions vulnerable. In this week's edition of The Safe Side, we explore how weak passwords could be the biggest security risk.



In 2022, NordPass, the password management tool from the team behind NordVPN, released its list of the 200 most common passwords. The most common password in the world that year was “password”, the second and third most common passwords were: ‘123456’ and ‘123456789’. In 2025, ‘123456’ was still on the list and used by over 76 lakh (7.6 million) people. In 2025, a single weak password led to the collapse of a 158-year-old UK transport company, highlighting the devastating real-world impact of poor cybersecurity practices. Hackers were able to guess an employee’s weak password, gain access to the company’s systems, and launch a ransomware attack that locked critical data and operations.

With no way to recover systems and mounting financial losses, the company was ultimately forced to shut down, leaving around 700 employees jobless. The incident underscores how even

basic security failures — like weak or reused passwords — can escalate into full-scale business disasters, especially when organisations lack robust cyber defences or recovery mechanisms. Cracking weak passwords is often alarmingly easy for cybercriminals, thanks to automated tools and vast databases of leaked credentials. Simple passwords like '123456', common words, or predictable patterns can be guessed in seconds using brute-force attacks (a trial-and-error hacking method), where software rapidly tries millions of combinations, or dictionary attacks that rely on frequently used terms.

If a password has been reused across multiple sites, a single data breach can give attackers access to several accounts at once. Even adding slight variations — like 'Password@123' — offers little protection as such patterns are widely anticipated. In many cases, hackers don't need advanced skills at all; weak passwords do most of the work for them, leaving personal, financial, and professional data exposed with minimal effort, making it easy to hack into your systems and even bank accounts.

Amit Relan, CEO and co-founder of mFilterIt, says, "Password hygiene plays an important role in digital security, but it's not the complete picture. Modern cyber fraud operates through a combination of compromised credentials, behavioral manipulation, and systemic gaps. Strengthening security will require both user awareness and more intelligent, ecosystem-level safeguards."

Prakash Ravindran, CEO and Director, InstiFi, said, "The growing concern is the interconnected nature of digital identities. A single compromised password from a data breach can be exploited through credential stuffing to access financial accounts, especially when users rely on the same login details across apps. With UPI and mobile-first transactions becoming the norm, these risks are amplified."

No longer a technology problem

Quick Heal's India Cyber Threat Report 2026 reveals that cyberattacks are increasingly driven by human and behavioural vulnerabilities, with Trojans accounting for 43 per cent and infectors 35 per cent of threats, largely exploiting user actions such as clicking malicious links or reusing credentials, he informed.

Dr Sanjay Katkar, Joint Managing Director, Quick Heal Technologies Ltd, told indianexpress.com, “Once the password is compromised, these credentials are systematically tested across banking apps, UPI platforms, email accounts, and social media, enabling attackers to move laterally and execute financial fraud at scale. This is how a single weak password can quickly translate into unauthorised transactions, identity misuse, and account takeovers.”

Vijender Yadav, CEO and co-founder of Accops, told indianexpress.com, “The fact that weak passwords still top global breach reports tells us this is no longer a technology problem alone, it is a behaviour and design problem. If a single password unlocks multiple banking, social and work apps, one compromise can cascade into full-blown financial fraud.”

Ravindran said, “We are increasingly seeing fraud shift from system-level attacks to user-level exploitation, where cybercriminals take advantage of weak digital habits rather than technical vulnerabilities. This makes user awareness and digital hygiene critical.”

Kaushal Bheda, Director at Pelorus Technologies, said, “Security professionals issue the exact same password guidelines every year, yet individuals consistently recycle identical credentials across their digital lives. An average person lacks a personal security posture. People do not even know what might be out there about them, especially on the dark web, operating unaware that their past passwords and email addresses are probably already indexed in public breach databases. Attackers feed this existing data into automated software to test against multiple platforms simultaneously.”

Bypassing two-factor authentication

Bheda said that even when secondary defenses are active, attackers bypass two-factor authentication through social engineering and other means.

“People don’t treat OTPs (One-Time Passwords) with the same caution as regular passwords — even though they are, quite literally, ‘passwords’. Because an OTP feels temporary and comes via SMS or app, users often assume it’s safe to share, especially in urgent or convincing situations (like a fake bank call),” he pointed out.

Shedding more light on OTPs, Amit Relan said, “An OTP is often seen as the final safeguard, but in many cases, it is also becoming a point of vulnerability. Once credentials are compromised,

attackers are increasingly able to bypass OTP layers through techniques like social engineering, SIM swaps, or rerouting authentication via virtual numbers. This effectively turns a simple password breach into a full account takeover, enabling unauthorized transactions and deeper access across linked platforms.”

Strengthening Your Digital Security

- ✚ Avoid using the same password across multiple platforms, especially for financial accounts
- ✚ Never reuse a password from a low-security site on critical platforms like banking or work accounts
- ✚ Stay away from predictable passwords such as “password”, “abcd123”, or “password@123”
- ✚ Treat alarming messages (like SMS alerts claiming your bank account is locked) as potential scams
- ✚ Do not share OTPs under any circumstances — they are as sensitive as passwords
- ✚ Prefer app-based authenticators over SMS-based OTPs for better security
- ✚ Be alert to unusual signs like sudden loss of network connectivity, which may indicate an ongoing attack
- ✚ Use strong multi-factor authentication (MFA) wherever available
- ✚ Move towards password-less authentication for critical accounts when possible
- ✚ Platforms should adopt behavioural intelligence and real-time risk detection to flag suspicious activity, even when login details seem correct
- ✚ Use of biometric authentication, facial recognition, or authenticator tokens significantly reduces risk

“From a regulatory standpoint, the DPDP Act has made safeguarding personal data a compliance requirement for businesses. This makes strong credential security an essential, something that cannot be achieved without due diligence from customers. This makes adopting a stronger security framework all the more important. Advanced security solutions such as Quick Heal Total Security and AntiFraud.AI help strengthen protection by identifying suspicious behaviour patterns and blocking fraud attempts before damage occurs,” Dr Sanjay Katkar added.

How to frame a strong password?

- ✚ Use longer passwords, at least 12–16 characters; these are hard to crack.
- ✚ Combine uppercase letters, lowercase letters, numbers, and special characters to get a stronger password.
- ✚ Avoid common words, names, birthdays, or predictable patterns (like “abcd123”).
- ✚ Don’t use easily guessable substitutions, for example: P@ssw0rd.
- ✚ Create a passphrase, a random combination of unrelated words, for example:
WhiteCat!Yamunasector18.
- ✚ Create a complete sentence and use the first letter for each word or use small spellings, “I have one Dog and two parrots,” which leads to “IHoneD@2P”.
- ✚ Consider using a password manager to generate and store complex passwords securely.
- ✚ Change passwords immediately if you suspect a breach or unusual activity.

The Safe Side

As the world evolves, the digital landscape does too, bringing new opportunities—and new risks. Scammers are becoming more sophisticated, exploiting vulnerabilities to their advantage. In our special feature series, we delve into the latest cybercrime trends and provide practical tips to help you stay informed, secure, and vigilant online.