New study exposes a quiet truth: the internet is built on weak password rules

Monday 10 November, 2025

Related Sectors:

Computing & Telecoms :: Consumer Technology :: Media & Marketing ::

Scan Me:

New study exposes a quiet truth: the internet is built on weak password rules

Which came first, the weak passwords or the lax security requirements?

New research from NordPass reveals that the world's most popular websites quietly encourage bad password habits - not by what they say, but by what they don't require.

After analyzing the 1,000 most visited websites globally, NordPass researchers found that most websites still make it far too easy to create weak passwords. From shopping platforms to government portals, even the internet's biggest names often skip the basic principles of creating strong passwords.

"The internet teaches us how to log in and for decades, it's been teaching us the wrong lessons. If a site accepts "password123", users learn that's enough and it's not. People normalized minimal effort for maximum risk," says Karolis Arba?iauskas, head of product at NordPass.

The password paradox

When it comes to basic security, most websites still fall short. NordPass found widespread inconsistency in how platforms handle password protection. Some websites enforce a few basic requirements, while others have none at all, and only a small number follow a clear, standardized approach.

As a result, users face completely different expectations from one platform to another. On one website, they might need to create a long and complex password; on another, something as simple as "123456" would still be accepted. This inconsistency doesn't just confuse users - it quietly lowers the global standard for online safety.

- 61 % of websites require a password - yet none fully meet NIST or NordPass security standards.
- 58 % don't require special characters, and 42 % don't enforce any minimum length.
- 11 % have no password requirements at all.
- Only 1 % of websites included in the study require all the right elements: long, complex passwords with uppercase letters, symbols, and numbers.

Sectors that handle some of the most sensitive data - government, health, and food & drink - performed the worst.

"It's not just about telling users to 'be more careful'. Security needs to be a partnership. Websites can shape safer habits by guiding users through better design like clear rules, visual indicators, or even modern authentication like passkeys," Arbaciauskas continues.

A closer look at the digital landscape

Beyond passwords, the research also examined how websites approach authentication overall and the numbers reveal how slowly innovation spreads.

- 39 % of sites let users sign in with single sign-on (SSO), mostly via Google.
- Only 2 % support passkeys, the modern passwordless technology backed by the FIDO Alliance.
- Just five websites - bahn.de, cuisineaz.com, fedex.com, interia.pl, and ups.com - met the strictest password criteria defined by NordPass and NIST.

While a few websites stand out as examples of strong password enforcement, most still prioritize convenience over security.

"Password carelessness didn't appear out of nowhere. When websites stop demanding strong

credentials, users stop creating them. What we're really looking at is a cultural shift in both internet users and internet developers - one we urgently need to reverse," says Arba?iauskas.

Why this matters

In an era of growing data breaches and automated hacking tools, password quality is no longer a minor detail - it's a first line of defense. Weak enforcement creates a ripple effect: if even the biggest websites don't set high standards, smaller ones rarely follow.

Weak password enforcement doesn't just put individuals at risk - it scales up to companies, industries, and governments. Every time a major platform accepts a weak password, it slows down implementation of the global standard for online security.

Cybercriminals exploit that gap. Simple passwords in combination with rising technologies like artificial intelligence make brute force and credential stuffing attacks easier than ever, putting millions of user accounts at risk across industries.

Methodology

A total of 1,000 of the most visited websites were selected based on the Top 1000 Most Visited Websites in the World by Ahrefs, according to organic search traffic estimates from February 2025. The ranking reflects the estimated number of monthly visits each website receives from organic search. We then checked what authentication methods and password requirements each of them had at the time. The data reflects the period from February 26 to March 6, 2025.

ABOUT NORDPASS

NordPass is a password manager for both business and consumer clients. It's powered by the latest technology for the utmost security. Developed with affordability, simplicity, and ease of use in mind, NordPass allows users to access passwords securely on desktop, mobile, and browsers. All passwords are encrypted on the device, so only the user can access them. NordPass was created by the experts behind NordVPN — the advanced security and privacy app. For more information: nordpass.com.

Company Contact:

NordPass

E. press@nordpassmedia.com
W. https://nordpass.com/

View Online

Newsroom: Visit our Newsroom for all the latest stories:
https://www.nordpass.pressat.co.uk