RESOURCE CENTER

World Password Day Survey 2024

Get the full interactive view at
https://bitwarden.com/nl-nl/resources/world-password-day-2024/

bitwarden

Overview

The Bitwarden World Password Day survey, conducted in Spring 2024, gathered insights from 2,400 individuals from the US, UK, Australia, France, Germany, and Japan to delve into current user password practices. The survey examines password security habits at home and in the workplace, assesses the perceived impacts of phishing and AI on online security, and captures user sentiment towards passkey adoption as an emerging authentication method.

View the presentation for a comprehensive exploration of the survey findings.

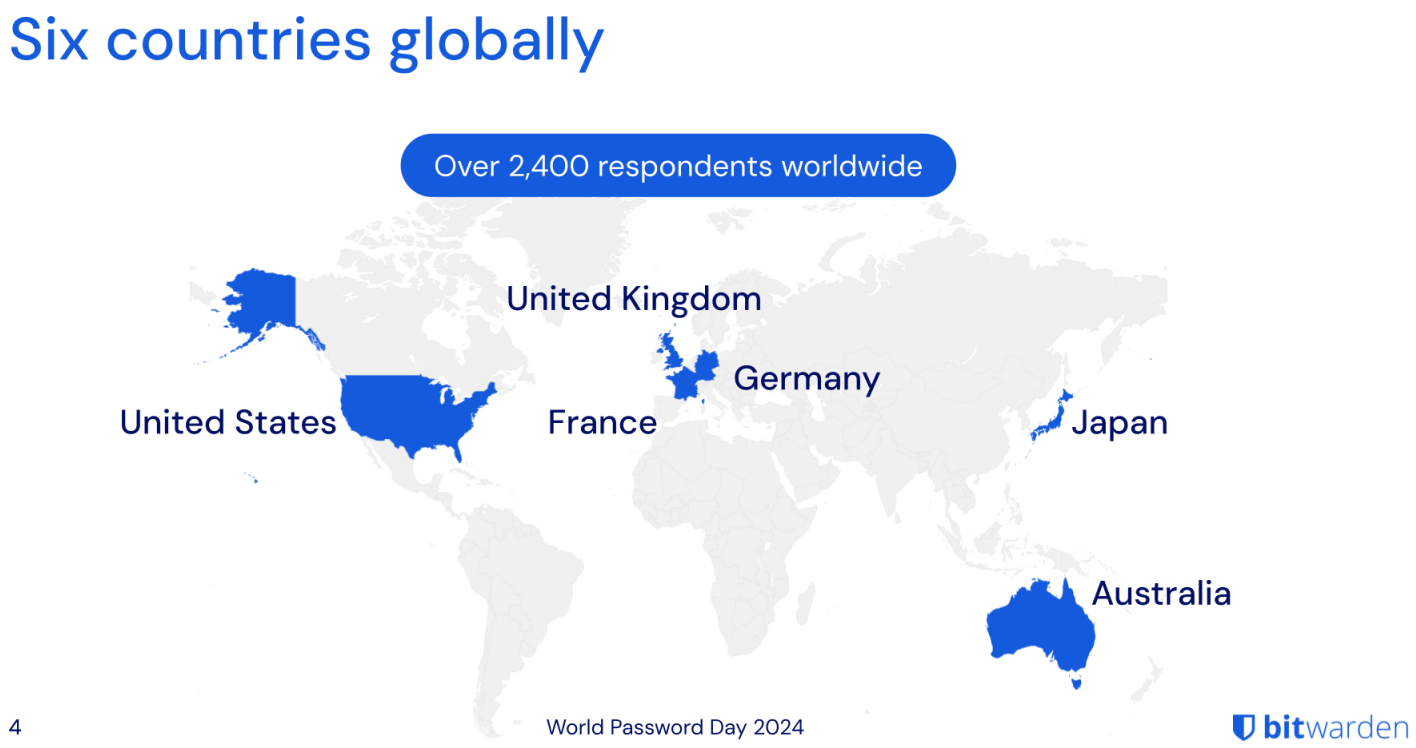


Table of Contents

Progress in passkey adoption

Key takeaways

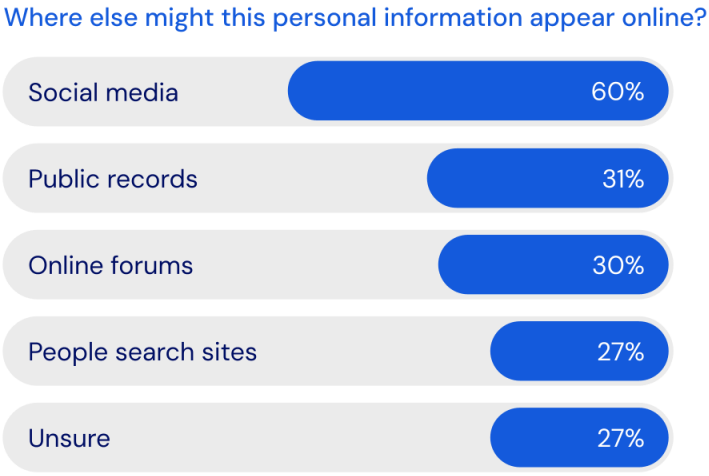
- 25% of global respondents reuse passwords across 11-20+ sites or apps at home, and 36% incorporate personal information into their passwords, raising concerns about password strength and security.
- A majority of respondents continue to use memory (54%) and pen and paper (33%) for password management, underscoring a reliance on outdated and potentially insecure practices.
- Almost a third of respondents (32%) feel unprepared or uncertain about defending against AI-enhanced cyber threats, highlighting a gap in cybersecurity readiness.
- 37% view their workplace security habits as risky, with notable percentages storing passwords insecurely (35%) or using weak credentials (39%), indicating areas for improvement in organizational cybersecurity practices.
- Although 45% of global respondents are adopting passkeys, there is a lack of understanding (41% are “not very well informed” or “not at all") about the privacy and security benefits of passkeys.

Individuals reveal risky password practices at home

The survey shows that a quarter (25%) of global respondents reuse passwords across 11-20+ accounts, with more than a third (36%) admitting to using personal information in their credentials that is publicly accessible on social media (60%) platforms and online forums (30%). These practices reveal a significant gap between recommended security practices and actual user behavior, highlighting how weak password habits and password reuse significantly heighten cybersecurity risks and identity theft.

Social media poses security risk

Out of the 36% of respondents who use personal information in their passwords, 60% report that this info can be found on their social media accounts.



Discrepancy between cybersecurity confidence and behaviors

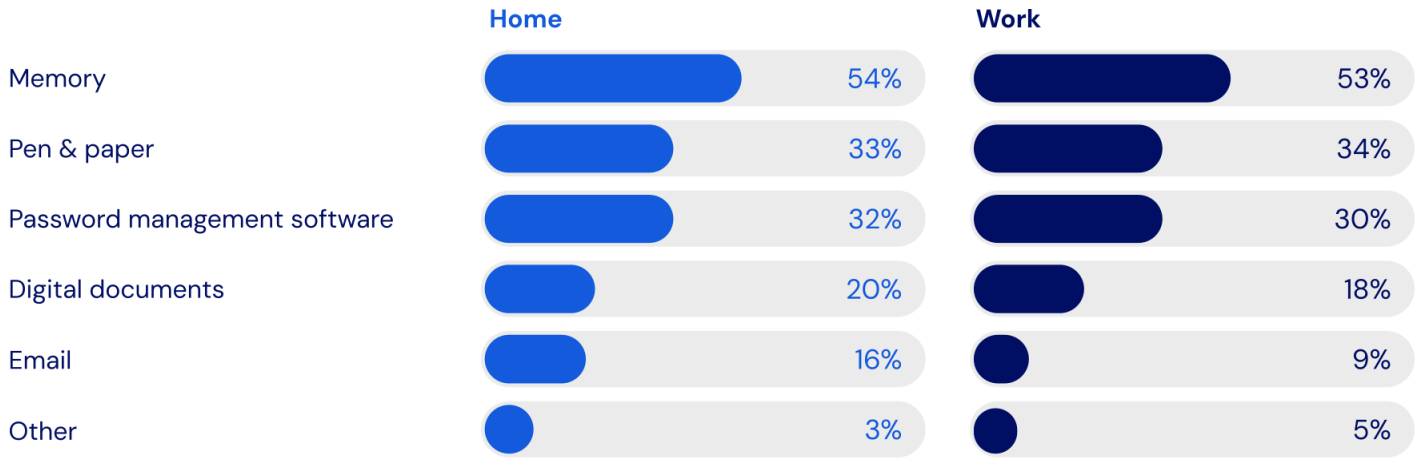
There is a critical need for enhanced awareness and education about better cybersecurity habits at home and at work. Despite 60% of users claiming they feel confident in being able to identify a phishing attack and 68% feeling prepared to identify and mitigate AI-enhanced cyberattacks, a substantial number of respondents still resort to risky password management methods. Fifty-four percent of individuals rely on memory and 33% use pen and paper to manage their passwords at home. Nearly half of respondents (41%) reveal they very frequently or somewhat frequently access personal and work data on public networks, increasing their vulnerability.

These behaviors have clear consequences, with nearly a fifth (19%) of global users admitting to experiencing security breaches, and 23% confirming their passwords have been stolen or compromised in the past. This underscores the cognitive dissonance between users' security postures and their actual practices.

Password manager use at home inching up

54% of respondents still rely on memory to manage passwords at home.
32% use password management software at home - up from 30% the previous year.

How do you manage your passwords for sites and services?



6 World Password Day 2024 bitwarden

Weak personal password habits compromise workplace security

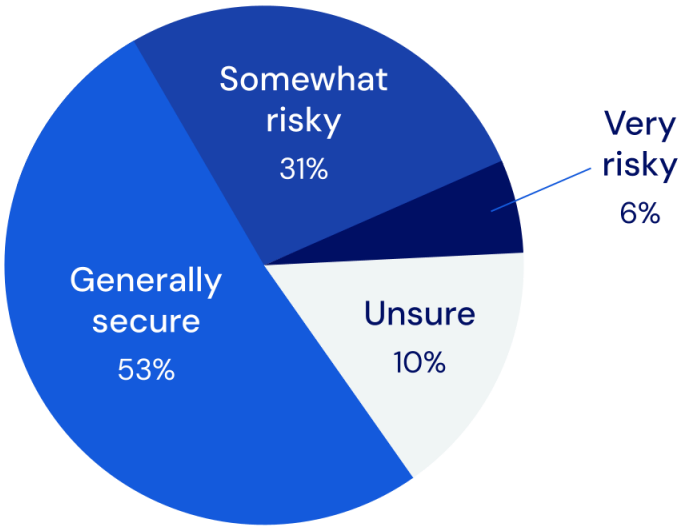
The survey's findings illustrate that individual password habits at work mirror those at home. The majority of respondents admit to relying on memory (53%) and pen and paper (34%) for their workplace accounts. Almost half (48%) reveal that they somewhat frequently or very frequently reuse passwords across workplace platforms or accounts.

Additionally, 48% of respondents say they receive regular security training focused on safeguarding login credentials against common threats, citing that they are confident (43%) or somewhat confident (50%) in counteracting those threats. Their behavior, however, paints a different picture with more than a third (37%) classifying their workplace security habits as somewhat or very risky. Though the global average is higher than the US percentage (23%) of respondents classifying their workplace security habits as risky, US users persist in using weak or personal-info based passwords (44%), storing work passwords insecurely (45%), not using 2FA (23%), and sharing passwords insecurely (32%).

Workplace security habits need some work

Although 53% classify their workplace security habits as generally secure, risky security habits such as using weak or personal info-based passwords are still common.

How would you classify your workplace security habits?



Identify the risky security habits you practice at work

Using weak or personal info-based passwords	39%
Storing work passwords insecurely	35%
Not using 2FA	33%
Sharing passwords insecurely	32%

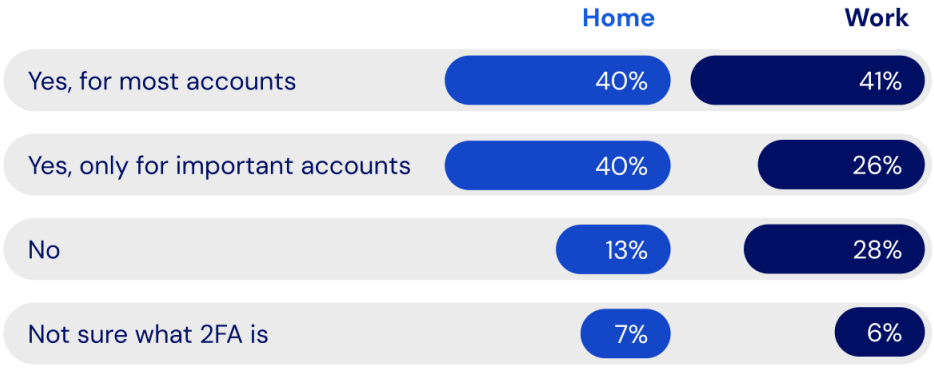
Stronger cybersecurity habits on the rise

Despite password security challenges, the survey reveals encouraging trends, demonstrating that users are increasingly adopting more responsible cybersecurity behaviors. Fifty-one percent of respondents globally (and 56% of US individuals) that have adopted a password manager at home report becoming more security conscious at work, and 45% say they reuse passwords less frequently. This extends beyond personal use, with 28% sharing the benefits of password management software within the workplace. The positive influence of using password managers at work is evident in respondents' personal lives, with 52% acknowledging increased security awareness at home, alongside a reduced frequency of password reuse (41%).

Adoption of two-factor authentication (2FA) is on the rise, with 40% of global respondents using it for most personal accounts and a similar percentage (41%) for most workplace accounts. There is growing awareness of its importance as a secondary security layer, with 57% of all respondents using 2FA to enhance their security posture as a result of an increase in phishing attacks. The growing frequency of cyberattacks targeting employees' credentials has not gone unnoticed either. Sixty-five percent of respondents have made some improvements or have increased safeguards to enhance security posture, showcasing a commitment to stronger cybersecurity practices across personal and professional settings.

Two-factor authentication gaining in popularity

Do you use two-factor authentication (2FA)?



80% of respondents say they use 2FA for personal accounts, compared to only 66% the previous year.

Just 7% say they are not sure what 2FA is - a substantial decrease from 22% last year.

Progress in passkey adoption

Forty-five percent of global survey respondents have adopted passkeys, indicating a continued shift toward passwordless authentication. However, more than forty percent of respondents still lack a full understanding of their security advantages, signaling a need for more education on the security benefits of passkeys over traditional passwords. Despite growing adoption, concerns about privacy and security persist. Users express apprehensions regarding data misuse (31%), monitoring uncertainties (31%), unauthorized access (31%), and secure storage doubts (29%). Transparent communication and strong security assurances are essential to address these issues, boost user confidence, and promote broader acceptance of passkeys.

If organizations adopted passkeys, 62% of respondents feel their trust in their company's security resilience would increase, and 66% would be more inclined to use passkeys personally if their workplace implemented them. Fifty-one percent of respondents foresee passkeys and passwords coexisting and 17% anticipate passkeys will make passwords obsolete. Regardless of individuals' outlook on the future of passkeys, a majority (56%) feel the industry needs to enhance its efforts in educating the public about the benefits of passkey technology.

More education needed to drive passkey adoption

While 45% of respondents use passkeys to log in to some accounts,
another 49% say they don't understand the security benefits of passkeys over traditional passwords.

How well do you understand the security benefits of passkeys over traditional passwords?