RESOURCE CENTER

World Password Day Survey 2024

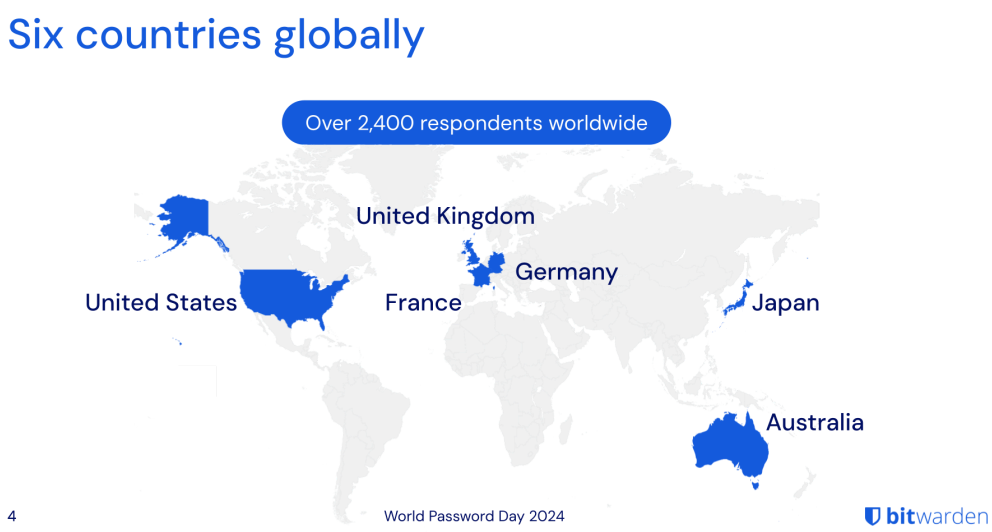
Get the full interactive view at
https://bitwarden.com/sv-se/resources/world-password-day-2024/

bitwarden

Översikt

Bitwarden World Password Day-undersökningen, som genomfördes våren 2024, samlade in insikter från 2 400 individer från USA, Storbritannien, Australien, Frankrike, Tyskland och Japan för att fördjupa sig i nuvarande användarlösenordspraxis. Undersökningen undersöker lösenordssäkerhetsvanor i hemmet och på arbetsplatsen, bedömer de upplevda effekterna av nätfiske och AI på onlinesäkerhet, och fångar användarnas känsla för antagande av lösenord som en framväxande autentiseringsmetod.

> Se presentationen för en omfattande utforskning av undersökningsresultaten.



Nyckel takeaways

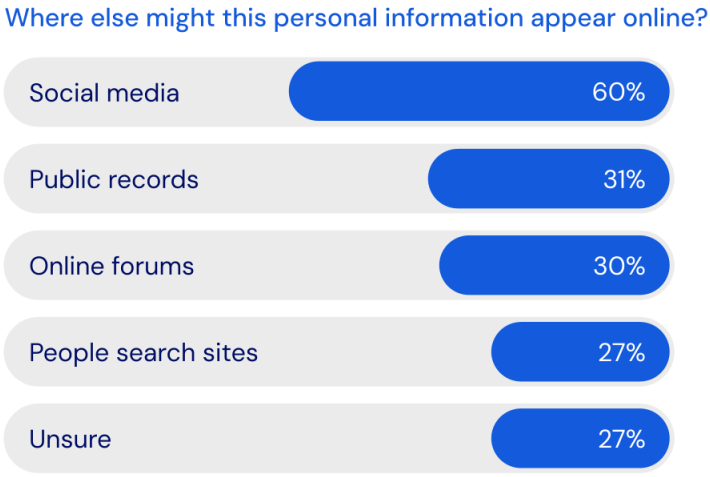
- 25 % av de globala svarandena återanvänder lösenord på 11–20+ webbplatser eller appar hemma, och 36 % införlivar personlig information i sina lösenord, vilket ger upphov till oro för lösenordsstyrka och säkerhet.
- En majoritet av de svarande fortsätter att använda minne (54 %) och penna och papper (33 %) för lösenordshantering, vilket understryker ett beroende av föråldrade och potentiellt osäkra metoder.
- Nästan en tredjedel av de tillfrågade (32 %) känner sig oförberedda eller osäkra på att försvara sig mot AI-förstärkta cyberhot, vilket visar på en lucka i cybersäkerhetsberedskap.
- 37 % ser sina säkerhetsvanor på arbetsplatsen som riskabla, med anmärkningsvärda procentandelar som lagrar lösenord på ett osäkert sätt (35 %) eller använder svaga referenser (39 %), vilket indikerar områden för förbättring av organisatoriska cybersäkerhetsmetoder.
- Även om 45 % av de globala svarandena använder lösenord, finns det en brist på förståelse (41 % är "inte särskilt välinformerade" eller "inte alls") om integritets- och säkerhetsfördelarna med lösenord.

Individer avslöjar riskabla lösenordspraxis hemma

Undersökningen visar att en fjärdedel (25 %) av de globala svarandena återanvänder lösenord på 11-20+ konton, och mer än en tredjedel (36 %) erkänner att de använder personlig information i sina autentiseringsuppgifter som är offentligt tillgänglig på sociala medier (60 %) plattformar och onlineforum (30 %). Dessa metoder avslöjar en betydande klyfta mellan rekommenderade säkerhetspraxis och faktiska användarbeteende, och belyser hur svaga lösenordsvanor och lösenordsåteranvändning avsevärt ökar riskerna för cybersäkerhet och identitetsstöld.

Social media poses security risk

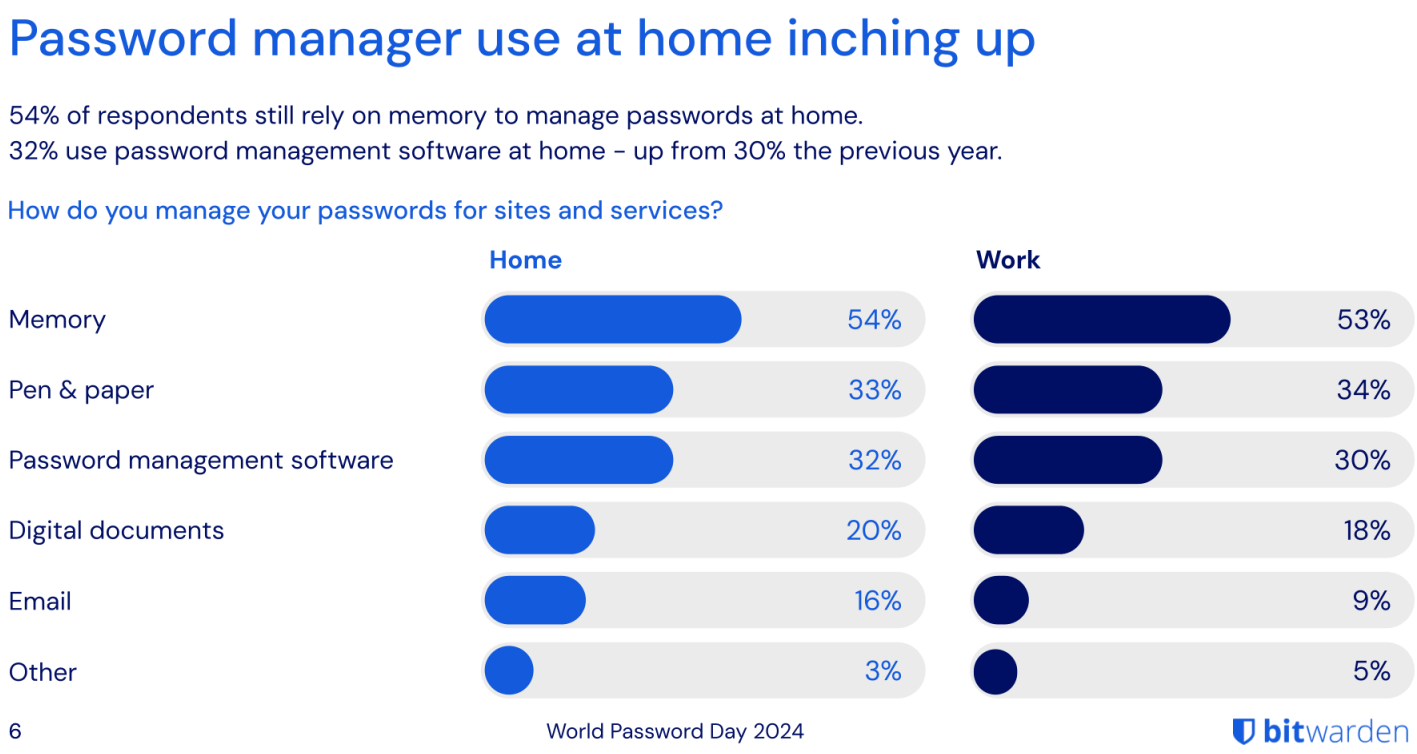
Out of the 36% of respondents who use personal information in their passwords, 60% report that this info can be found on their social media accounts.



Diskrepans mellan cybersäkerhetsförtroende och beteenden

Det finns ett stort behov av ökad medvetenhet och utbildning om bättre cybersäkerhetsvanor hemma och på jobbet. Trots att 60 % av användarna hävdar att de känner sig säkra på att kunna identifiera en nätfiskeattack och 68 % känner sig beredda att identifiera och mildra AI-förbättrade cyberattacker, tar ett stort antal svarande fortfarande till riskfyllda lösenordshanteringsmetoder. Femtiofyra procent av individerna förlitar sig på minne och 33 % använder penna och papper för att hantera sina lösenord hemma. Nästan hälften av de tillfrågade (41 %) avslöjar att de mycket ofta eller något ofta har tillgång till person- och arbetsdata på offentliga nätverk, vilket ökar deras sårbarhet.

Dessa beteenden har tydliga konsekvenser, med nästan en femtedel (19 %) av globala användare som erkänner att de har upplevt säkerhetsintrång, och 23 % bekräftar att deras lösenord har stulits eller äventyrats tidigare. Detta understryker den kognitiva dissonansen mellan användarnas säkerhetsställningar och deras faktiska metoder.



Svaga personliga lösenordsvanor äventyrar säkerheten på arbetsplatsen

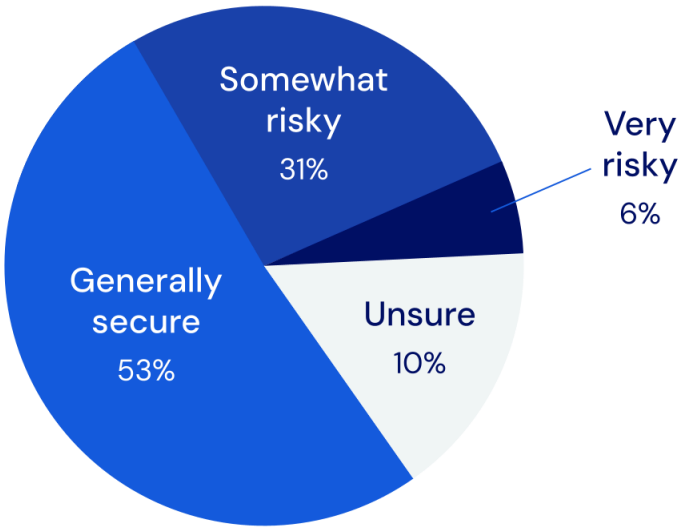
Undersökningens resultat illustrerar att individuella lösenordsvanor på jobbet speglar dem hemma. Majoriteten av de svarande medger att de förlitar sig på minne (53 %) och penna och papper (34 %) för sina arbetsplatskonton. Nästan hälften (48%) avslöjar att de något ofta eller mycket ofta återanvänder lösenord på arbetsplatsplattformar eller konton.

Dessutom säger 48 % av de tillfrågade att de får regelbunden säkerhetsutbildning med fokus på att skydda inloggningsuppgifter mot vanliga hot, med hänvisning till att de är säkra (43 %) eller något säkra (50 %) på att motverka dessa hot. Deras beteende målar dock upp en annan bild med mer än en tredjedel (37 %) som klassificerar sina säkerhetsvanor på arbetsplatsen som något eller mycket riskfyllda. Även om det globala genomsnittet är högre än procentandelen i USA (23 %) av de svarande som klassificerar sina säkerhetsvanor på arbetsplatsen som riskfyllda, fortsätter amerikanska användare att använda svaga eller personliga informationsbaserade lösenord (44 %), lagra arbetslösenord på ett osäkert sätt (45 %), inte använda 2FA (23 %) och att dela lösenord på ett osäkert sätt (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%

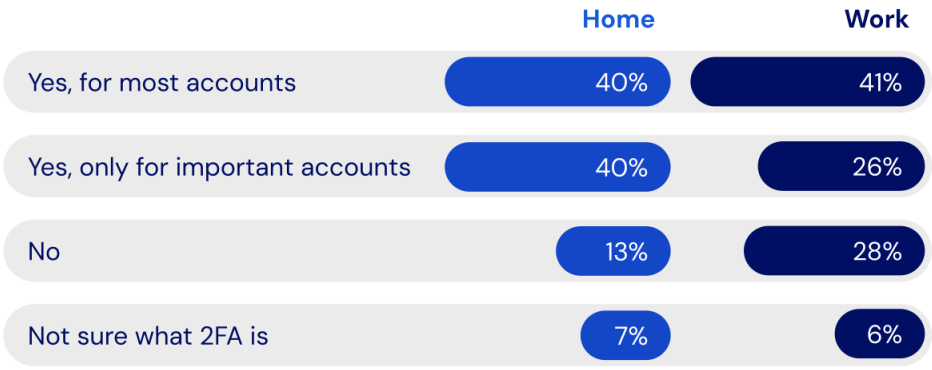
Starkare cybersäkerhetsvanor ökar

Trots utmaningar med lösenordssäkerhet avslöjar undersökningen uppmuntrande trender som visar att användare i allt högre grad anammar mer ansvarsfulla beteenden inom cybersäkerhet. 51 procent av de tillfrågade globalt (och 56 % av amerikanska individer) som har antagit en lösenordshanterare hemma rapporterar att de blir mer säkerhetsmedvetna på jobbet, och 45 % säger att de återanvänder lösenord mer sällan. Detta sträcker sig bortom personligt bruk, med 28 % som delar fördelarna med programvara för lösenordshantering på arbetsplatsen. Det positiva inflytandet av att använda lösenordshanterare på jobbet är uppenbart i respondenternas personliga liv, där 52 % erkänner ökad säkerhetsmedvetenhet i hemmet, tillsammans med en minskad frekvens av lösenordsåteranvändning (41 %).

Antagandet av tvåfaktorsautentisering (2FA) ökar, med 40 % av de globala respondenterna som använder det för de flesta personliga konton och en liknande andel (41 %) för de flesta arbetsplatskonton. Det finns en växande medvetenhet om dess betydelse som ett sekundärt säkerhetslager, där 57 % av alla svarande använder 2FA för att förbättra sin säkerhetsställning som ett resultat av en ökning av nätfiskeattacker. Den ökande frekvensen av cyberattacker riktade mot anställdas referenser har inte heller gått obemärkt förbi. Sextiofem procent av de tillfrågade har gjort vissa förbättringar eller har ökat säkerhetsåtgärder för att förbättra säkerhetsställningen, vilket visar ett engagemang för starkare cybersäkerhetspraxis i personliga och professionella miljöer.

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.

Framsteg i antagandet av lösenord

Fyrtiofem procent av de globala undersökningsrespondenterna har antagit lösenord, vilket indikerar en fortsatt förändring mot lösenordslös autentisering. Men mer än fyrtio procent av de svarande saknar fortfarande en fullständig förståelse för sina säkerhetsfördelar, vilket signalerar ett behov av mer utbildning om säkerhetsfördelarna med lösenord framför traditionella lösenord. Trots växande användning kvarstår oron för integritet och säkerhet. Användare uttrycker farhågor om datamissbruk (31 %), osäkerheter vid övervakning (31 %), obehörig åtkomst (31 %) och tvivel om säker lagring (29 %). Transparent kommunikation och starka säkerhetsgarantier är avgörande för att lösa dessa problem, öka användarnas förtroende och främja en bredare acceptans av lösenord.

Om organisationer antog lösenord, känner 62 % av de tillfrågade att deras förtroende för deras företags säkerhetstålighet skulle öka, och 66 % skulle vara mer benägna att använda lösenord personligen om deras arbetsplats implementerade dem. 51 procent av de tillfrågade förutser att lösenord och lösenord existerar samtidigt och 17 % förväntar sig att lösenord kommer att bli föråldrade. Oavsett individers syn på framtiden för lösenord, anser en majoritet (56 %) att branschen behöver förbättra sina ansträngningar för att utbilda allmänheten om fördelarna med nyckelteknologi.