

RESOURCE CENTER

World Password Day Survey 2024

Hur påverkar lösenordspraxis hemma på arbetsplatsen?

Get the full interactive view at

<https://bitwarden.com/sv-se/resources/world-password-day/>



Översikt

Denna årliga globala undersökning av över 2 300 anställda vuxna i USA, Australien, Storbritannien, Tyskland, Frankrike och Japan belyser generationstrender i lösenordsvanor.

Se presentationen för en omfattande utforskning av undersökningsresultaten.

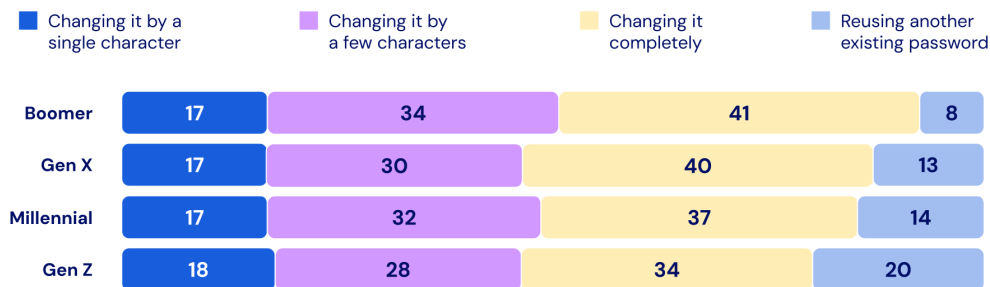
Lösenordströtthet leder till lösenordsåteranvändning

Gen Z är den första generationen som har vuxit upp helt online, men deras status som digitala infödda har inte gjort dem i sig säkerhetsmedvetna. Enligt undersökningen har omfattningen av deras onlineexponering sannolikt bidragit till lösenordströtthet. 35 % av Gen Z-respondenterna avslöjade att de aldrig eller sällan uppdaterar lösenord efter ett dataintrång hos ett företag som de har ett konto hos. Endast 10 % rapporterade att de alltid uppdaterar utsatta lösenord. När du uppmanas att uppdatera en inloggning ändrar 38 % av Gen Z och 31 % av Millennials bara ett enda tecken eller återvinner helt enkelt ett befintligt lösenord.

Lösenordsåteranvändningen är skenande, med 72 % av Gen Z återanvänder lösenord, i kontrast till endast 42 % av Boomers – en betydande generationskoppling. Men trots deras beteende, tror 79% av Gen Z-respondenterna att lösenordsåteranvändning är riskabelt. 59 % av Gen Z återanvänder också befintliga lösenord när de uppdaterar ett konto hos ett företag som har upplevt ett dataintrång, jämfört med bara 23 % av Boomers. Ännu mer avslöjande, 55 % av de tillfrågade har övergett ett konto eller skapat ett nytt helt enkelt för att slippa gå igenom processen för återställning av lösenord, medan 30 % av Gen Z ofta eller alltid glömmer lösenord till viktiga konton.

Gen Z could learn a thing or two from Boomers – 41% completely change their passwords when prompted, versus just 34% of Gen Z. Still, 62% across all generations opt for less secure updates or reused passwords.

Q: When prompted to change my password, I often alter my password by...



6 

Yngre generationer förlitar sig på multifaktorautentisering (MFA) när de använder svaga lösenord

Mer än 80 % av de yngre generationerna är åtminstone något sannolikt att möjliggöra MFA även när det inte krävs, jämfört med endast 51 % av Boomers. Detta tyder på att Gen Z och

Innehållsförteckning

Resultat från World Password Day 2025

- Lösenordströtthet leder till lösenordsåteranvändning
- Yngre generationer förlitar sig på multifaktorautentisering (MFA) när de använder svaga lösenord
- Lösenordsstress
- Lösenordsdelning över generationer
- Gen X: Möjligheter för aktivering

Resultat från World Password Day 2024

2023 års resultat för World Password Day

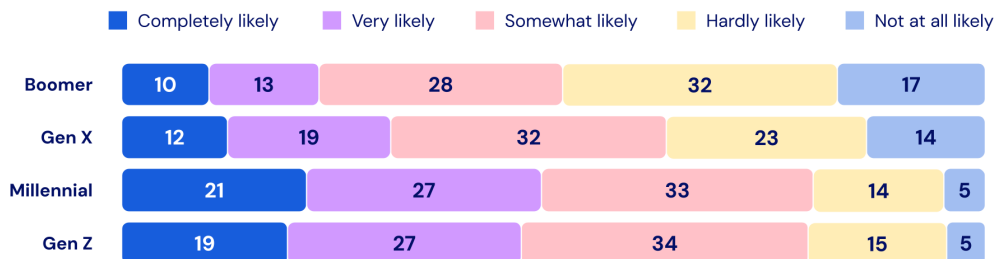
2022 års resultat för World Password Day

Resultat från World Password Day 2021

Millennials kan kompensera för dåliga lösenordsvanor genom att förlita sig på MFA som ett säkerhetsnät. MFA är förvisso ett värdefullt lager av skydd, men det är inte en ersättning för unika, starka lösenord. Om lösenordet – den första faktorn – äventyras eller svagt, kommer kontot att förbli sårbart, särskilt när MFA är aktiverat med SMS, vilket är känsligt för SIM-bytesattacker.

Multifactor authentication is more popular than expected – 70% say they're likely to enable it, even when not required

Q: If MFA is not required, how likely are you to enable it?



19



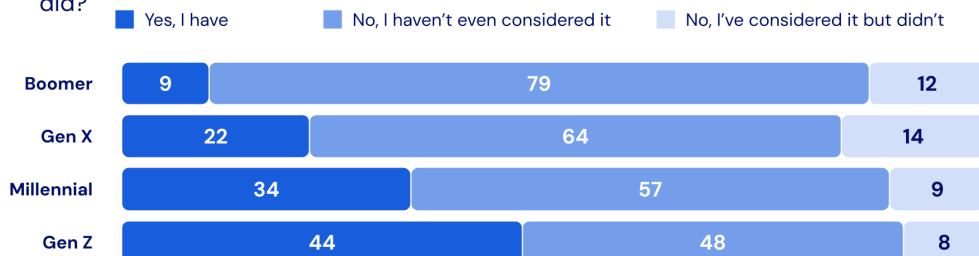
Lösenordsstress

Lösenord kan avslöja karaktären av interpersonella beteenden. 44 % av Gen Z säger att de har ändrat ett lösenord för en streamingtjänst för att ta bort åtkomst från en familjemedlem eller vän som ett känslomässigt svar på något de sa eller gjorde. Behörighetsägande och digitala gränser formas i allt högre grad av personliga beslut och relationer, särskilt bland Gen Z och Millennials, som är mer benägna att dela kontoåtkomst till onlineplattformar.

Lösenordsstress varierar mellan åldersgrupper. 62 % av Gen Z rapporterar en viss grad av stress kring hantering av lösenord trots att de vuxit upp online. När säkerhetsvanor måste upprätthållas på dussintals konton känner även digitala infödda påfrestningen.

New vector for emotional revenge: 44% of Gen Z and 34% of Millennials admit to changing a streaming password to lock out a friend or family member

Q: Have you changed a streaming service password to remove shared account access for a friend or family member as an emotional response to something they did?



16 

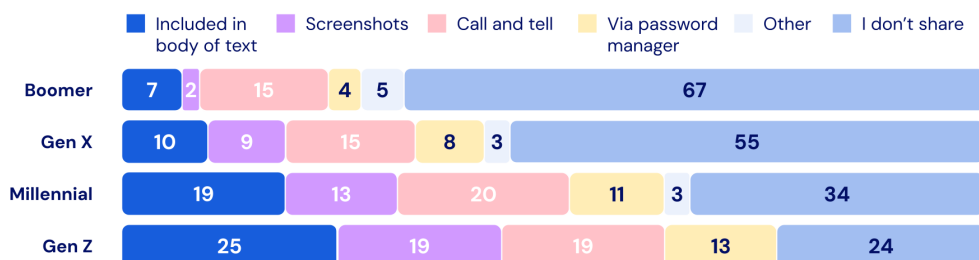
Lösenordsdelning över generationer

Med 46 % är det mest sannolikt att Gen Z använder programvara för lösenordshantering. Ändå fortsätter osäkra delningsvanor. 25 % av Gen Z delar lösenord via text, 19 % delar skärmdumpar och 19 % delar verbalt. Bara 13 % av de tillfrågade rapporterar att de använder en lösenordshanterare för att dela autentiseringsuppgifter på ett säkert sätt, vilket visar på en bristande anpassning mellan hur lösenord lagras och delas.

I andra änden av spektrumet säger 67 % av Boomers att de inte delar lösenord och bara 7 % delar via textmeddelande. Även om yngre generationer trendar mot modern lösenordshantering och MFA-verktyg, undergräver riskfyllda beteenden bästa praxis.

Gen Z and Millennials are the most likely to share passwords, but only 13% and 11% respectively, use a password manager for secure sharing when they do

Q: What is the primary means you use for sharing a password with a friend, colleague or family member?



11 

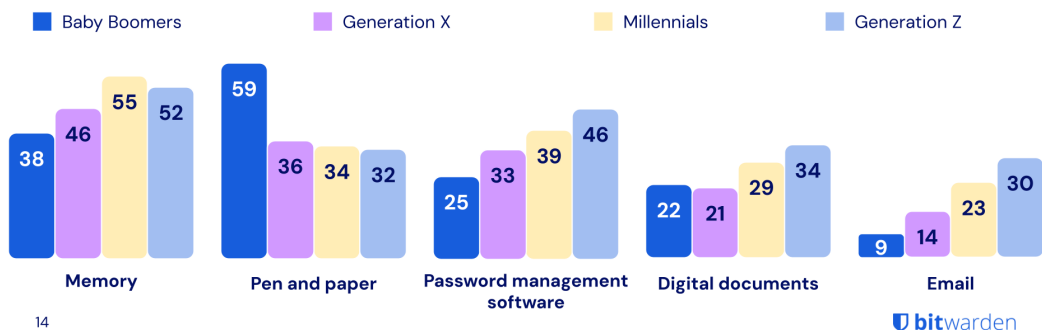
Gen X: Möjligheter för aktivering

Medan Gen Z visar tecken på risktagande och lösenordströtthet, avslöjar Gen X en annan utmaning: en brist på förtroende för lösenordshanterare. Endast 33 % av Gen X använder en lösenordshanterare, släpar efter 39 % av Millennials och 46 % av Gen Z.

21 % av Gen X erkänner att de inte vet hur man ställer in eller litar inte på en lösenordshanterare, även om de ofta innehar ledarroller och är i början av sina karriärer. Även om de flesta har allmän medvetenhet om säkerhetsrisker, framhäver kontrasten mellan säkerhetsvanor av Gen X en möjlighet till möjlighet till möjlighet och utbildning, särskilt för en generation ledare som påverkar säkerhetspolicyer och beteenden för både arbetsplatsen och hemma.

Insecure habits vary: More than half (55%) of Millennials still rely on memory to manage their passwords and 59% of Boomers use pen and paper; meanwhile, Gen Z is most likely to use a password manager

Q: How do you manage your passwords at home?



[Läs hela rapporten.](#)

Resultat från World Password Day 2024

Undersökningen 2024 Bitwarden World Password Day samlade in insikter från 2 400 individer från USA, Storbritannien, Australien, Frankrike, Tyskland och Japan för att fördjupa sig i nuvarande rutiner för användarlösenord. Undersökningen undersökte lösenordssäkerhetsvanor i hemmet och på arbetsplatsen, bedömde de upplevda effekterna av nätfiske och AI på onlinesäkerhet, och fångade användarnas känsla för antagande av lösenord som en framväxande autentiseringsmetod.

Se de [fullständiga resultaten](#) av World Password Day Global Survey för 2024.

Viktiga resultat:

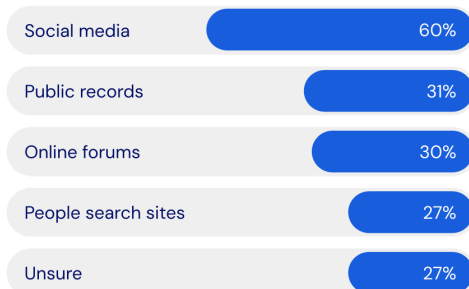
- 36 % av de globala svarandena införlivar personlig information i sina lösenord
- Nästan en tredjedel av de tillfrågade (32 %) känner sig oförberedda eller osäkra på att försvara sig mot AI-förbättrade cyberhot
- 37 % ser sina säkerhetsvanor på arbetsplatsen som riskabla, med anmärkningsvärda procentandelar som lagrar lösenord på ett osäkert sätt (35 %) eller använder svaga referenser (39 %)
- Även om 45 % av de globala svarandena använder lösenord, finns det en brist på förståelse (41 % är "inte särskilt välinformerade" eller "inte alls") om deras integritets- och säkerhetsfördelar

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.



Where else might this personal information appear online?



Resultat från World Password Day 2023

För den tredje årliga World Password Day Survey undersökte Bitwarden över 2 000 internetanvändare globalt (USA, Storbritannien, Australien, Tyskland, Frankrike och Japan) om deras rutiner för lösenordssäkerhet. Dessutom inkluderade 2023 års undersökning frågor om lösenordslös teknologi.

Se de [fullständiga resultaten](#) av World Password Day Global Survey för 2023.

Viktiga resultat:

- 56 % är glada över lösenordslösa autentiseringsalternativ som biometri, lösenord eller säkerhetsnycklar
- Bästa praxis späds fortfarande av dåliga vanor, med 85 % återanvänder lösenord på flera webbplatser och 58 % förlitar sig på minne för sina lösenord
- 52 % använder lätt identifierbar information i sina lösenord, såsom företags-/varumärken, välkända sångtexter, husdjursnamn och namn på nära och kära

Netflix and Spill [Your Password]

Over one-third (36%) share passwords for TV streaming services.



World Password Day 2023

2022 års resultat för World Password Day

Bitwarden samarbetade med Propeller Insights för att göra en undersökning av över 2 000 konsumenter i USA, Storbritannien, Tyskland, Japan och Australien. Även om de är mottagliga för vikten av säkerhet, fortsätter individer att kämpa med att omfamna vanor som bättre skulle kunna skydda deras data.

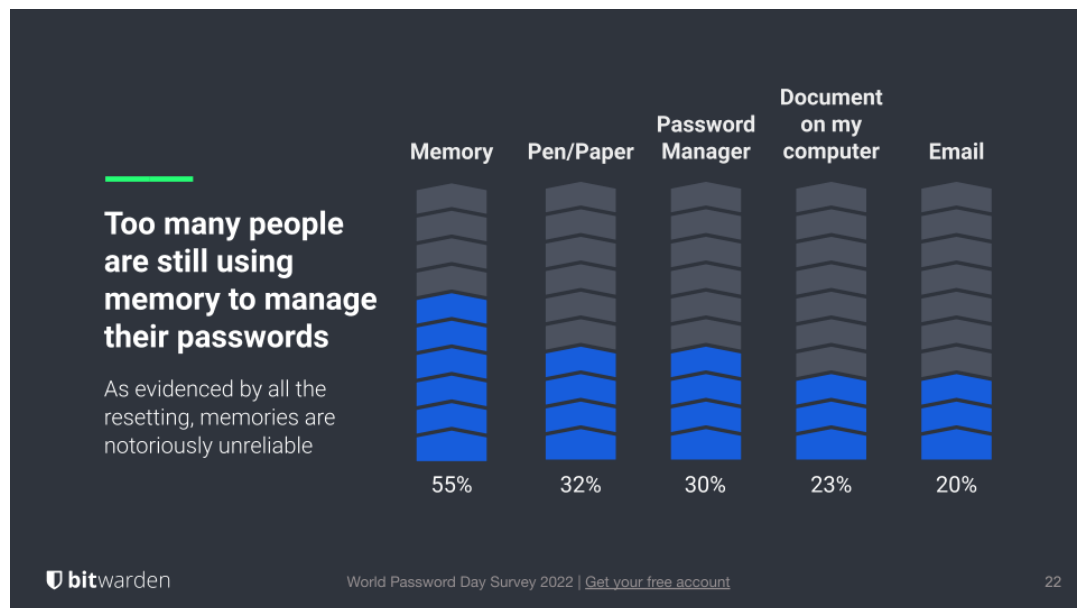
Nästan alla (90 %) av de globala svarspersonerna är "något" eller "mycket" bekanta med bästa praxis för lösenordssäkerhet – men betyder det att vara bekant att omsättas i praktiken? Inte helt.

- En majoritet av globala svarande (84 %) återanvänder lösenord på mer än 1 webbplats
- Nästan en femtedel (21 %) av respondenterna återställer sina lösenord varje dag eller flera gånger i veckan
- Över hälften (55 %) av de globala svarandena förlitar sig på sina minnen för att hantera lösenord

Ytterligare resurser

Se fullständiga resultat från World Password Day Global Survey för 2022 [här](#) eller öppna presentationen för nedladdningsalternativ [här](#).

Läs hela rapporten från World Password Day 2022 [här](#).



Resultat från World Password Day 2021

Bitwarden genomförde sin första World Password Day globala undersökning 2021 för att bedöma tillståndet för lösenordshantering och säkerhetsvanor. Över 1600 internetanvändare tillfrågades i USA, Storbritannien, Japan och Australien.

Viktiga resultat:

- Dataintrång florerar: en fjärdedel globalt (24 %) rapporterar att ha blivit offer för ett dataintrång under de senaste 18 månaderna, med USA som rapporterar den högsta andelen (33 %)
- Minnet har sina nackdelar: majoriteten (59 %) litar på sitt minne för att komma ihåg lösenord, och 56 % återställer sina lösenord från så ofta som varje dag till en gång i månaden
- Mer än hälften delar aldrig lösenord för personligt bruk eller arbete

Se fullständiga resultat från World Password Day Global Survey för 2021 [här](#) eller läs bloggen [här](#).