

RESOURCE CENTER

Hur man skapar starka lösenordsidéer för bättre säkerhet

Get the full interactive view at
<https://bitwarden.com/sv-se/resources/how-to-create-strong-password-ideas-for-better-security/>



Starka lösenordsidéer är viktiga för att skydda dina konton och personliga data. Den här guiden täcker praktiska och effektiva strategier för onlinekontosäkerhet för att hjälpa dig skapa starka lösenordsidéer och förbättra din övergripande digitala säkerhet.

Varför starka lösenordsidéer är viktiga

Med den genomsnittliga användaren som hanterar hundratals konton är det avgörande att använda ett unikt, starkt lösenord för vart och ett. Ett svagt eller återanvänt lösenord kan äventyra flera konton om ett bryts, så det är viktigt att använda starka lösenord för att skydda dina konton från brute force-attacker.

En brute force attack är en metod som används av illvilliga aktörer som distribuerar programvara för att systematiskt prova alla möjliga lösenordskombinationer tills det rätta hittas. Dessa attacker kan knäcka enkla lösenord på några minuter, vilket understryker vikten av att skapa starka och unika lösenord för att förbättra säkerheten.

Att använda säkra lösenord hjälper till att skydda känsliga inloggningar och den data de skyddar, som bankkonton, e-post och personnummer.

Vad gör ett lösenord starkt?

En idé med starkt lösenord bör vara:

- **Lång** – Minst 14 tecken.
- **Varierad** – Använder en kombination av bokstäver, siffror och symboler.
- **Slumpmässigt** – Inkluderar inte ord, mönster eller personlig information i lexikon.
- **Unikt** – Återanvänds inte på andra konton.

Nyckelkomponenter i ett starkt lösenordsidé

1. Längd

Längre lösenord är säkrare. Ett 8-teckens lösenord kan knäckas på några minuter. Ett lösenord på 16 tecken kan ta miljarder år.

2. Karaktärsvariation

Använd en kombination av:

- Stora och små bokstäver
- Tal
- Symboler

Denna variation gör lösenord mer komplexa och svårare att gissa.

3. Slumpmässighet

Undvik förutsägbara mönster, vanliga lösenord eller personliga uppgifter, som namn eller födelsedatum. Slumpmässiga, maskingenererade lösenord är betydligt säkrare.

4. Unikt

Varje lösenord ska vara unikt, vilket innebär att det inte används för något annat konto. Den ska inte heller ha någon personlig information, som datum, namn eller användarens favoritbil. Ett unikt lösenord ska inte kopplas till användaren.

Svaga referenser står för 46 % av obehörig åtkomst till molnmiljöer.

“Password length is a primary factor in characterizing password strength.”

National Institute of Standards and Technology (NIST)

Try it: Use the [Bitwarden Password Strength Checker](#) to assess your current passwords.

Hur man skapar starka lösenord

Att memorera säkra lösenord kan vara en utmaning. Enligt en [global undersökning](#):

- 25 % av människorna återanvänder lösenord på 11–20+ konton.
- 36 % använder personlig information i sina lösenord som kan hittas på sociala medier eller offentliga forum.

Regelbunden uppdatering av skapade lösenord är avgörande för att förbättra säkerheten mot föränderliga cyberhot. Här är två enkla metoder för att skapa starka lösenordsidéer.

Alternativ 1: Använd en lösenfras

En lösenfras kombinerar orelaterade ord till en enda, minnesvärd sträng.

- **Exempel:** Anew-Slather-Unseated-Farbror-Sandy
- Lägg till karaktärstransformationer för extra styrka: ShyL!OnS33S@w-p00l

Du kan också anpassa fraser du kommer ihåg:

- "Jag älskar att äta pizza på fredagar!" → lLoEaPiOnFr!

Alternativ 2: Använd en lösenordsgenerator

Lösenordshanterare inkluderar ofta inbyggda lösenords- eller lösenfrasgeneratorer. Dessa verktyg skapar säkra, slumpmässiga referenser direkt.

Prova det: Använd [Bitwarden Password Generator](#) för starka, säkra förslag.

Vanliga lösenordsfel att undvika

Det finns flera vanliga misstag att undvika när man skapar starka lösenordsidéer.

Misstag	Varför det är riskabelt	Vad ska man göra istället
Återanvända lösenord	Ett intrång på ett konto sätter alla återanvända konton i fara.	Använd unika lösenord för varje konto.
Använder personlig information	Namn, födelsedagar och adresser är lätta för hackare att hitta och gissa.	Håll lösenord slumpmässiga och orelaterade till ditt liv.
Använda vanliga ord eller mönster	Lösenord som 123456 eller qwerty är bland de första som hackare försöker.	Använd lösenordsgeneratorer och undvik förutsägbara mönster.

Tips: Granska och uppdatera regelbundet [svaga](#) eller [återanvända](#) lösenord.

Att identifiera ett svagt lösenord är avgörande. De är ofta korta, förutsägbara eller baserade på personlig information, vilket allt gör dem till enkla måltavlor för dåliga skådespelare.

Använd en lösenordshanterare för bättre säkerhet

En lösenordshanterare gör det enkelt att skapa, lagra och hantera alla dina lösenord på ett säkert sätt, vilket säkerställer att de är starka och unika för varje konto.

Läs mer om hur [Bitwarden](#) håller din data säker.

Viktiga fördelar

- **Autofyll inloggningsinformation:** Spara tid och minska antalet fel.
- **Nätfiskeskydd: Kommer inte att fylla i** autentiseringsuppgifter automatiskt på misstänkta eller falska webbplatser.
- **Inbyggd lösenordsgenerator:** Skapa omedelbart säkra lösenord eller lösenordsfraser.
- **Anpassningsbara alternativ:** Justera längd och teckentyper för att möta kontokraven.
- **End-to-end-kryptering:** Data krypteras innan de lämnar enheten.
- **Lösenordsgranskningar:** Identifiera svaga, återanvända eller kränkta lösenord.
- **Säker delning:** Dela autentiseringsuppgifter på ett säkert sätt med familj eller kollegor.
- Stöd för tvåfaktorsautentisering (2FA): Lägger till ett extra lager av säkerhet.

Aktivera tvåfaktorsautentisering (2FA)

Att lägga till 2FA till dina konton är ett enkelt sätt att avsevärt öka säkerheten när ett starkt lösenord är på plats. Många onlinekonton, inklusive de med känslig information som onlinebanker, erbjuder vanligtvis detta extra säkerhetslager för att skydda användare från obehörig åtkomst. Det kräver en andra form av verifiering, till exempel en kod från en app, förutom lösenordet.

Många lösenordshanterare stöder 2FA direkt eller integreras med autentiseringsappar för bekvämlighet.

Gör säkerheten enklare

Starka lösenordsidéer behöver inte vara svårt. En pålitlig lösenordshanterare kan minska mental belastning, förenkla ditt arbetsflöde och förbättra din övergripande digitala hygien.

- Förvara allt säkert i ett krypterat valv.
- Skapa starka lösenord med ett klick.
- Få aviseringar om svaga eller komprometterade autentiseringsuppgifter.
- Synkronisera dina data mellan enheter.

Kom igång idag! Håll [enkelt reda på lösenord med Bitwarden](#).