

Lista på lämpliga lösenordshanterare för mobiltelefoner m.m.

Lösenord till program och annat man har på sin smartphone är ett ständigt bekymmer för de flesta. Man skall komma ihåg lösenordet och helst ha olika lösenord till olika program. Detta är ett bekymmer för alla oavsett ålder. Bästa sättet att lösa detta bekymmer är att installera en lösenordshanterare där man på ett säkert sätt kan förvara alla sina lösenord och en del annat.

Nedan finns en lista på olika program på marknaden. Självt använder jag Bitwarden som jag tycker är utmärkt enkel att hantera. Detta program är dessutom gratis vilket inte alltid är fallet.

Här är en lista över några av de mest lämpliga och populära lösenordshanterarna för mobiltelefoner 2025, med fokus på säkerhet, användarvänlighet och funktioner som stöd för biometrisk inloggning och kryptering:

Toppval för mobiltelefoner

- **1Password**
Mycket säker, med 256-bitars AES-kryptering, stöd för tvåfaktorsautentisering (2FA), biometrisk inloggning och reseläge för att dölja valv. Appen finns på svenska och erbjuder **14 dagars gratisprov**.
- **Dashlane**
Stark säkerhet, 256-bitars AES-kryptering, noll-kunskapsarkitektur, biometrisk inloggning och extrafunktioner som VPN och dark web-övervakning. **Gratis provperiod på 30 dagar**.
- **Keeper**
Hög säkerhetsnivå med 256-bitars AES-kryptering, flera alternativ för flerfaktorsautentisering och biometrisk inloggning. Appen erbjuder även krypterad meddelandetjänst och dark web-bevakning.
- **LastPass**
Enkel och snabb, stöd för 2FA och biometrisk inloggning. Fungerar bra på både Android och iOS.
- **Bitwarden**
Gratis och öppen källkod, stöd för 2FA och biometrisk inloggning. Lämplig för användare som vill ha full kontroll över sina data.
- **RoboForm**
Bra säkerhet, kraftfull formuläryfyllning och låga kostnader. Stöd för 2FA och biometrisk inloggning.
- **Enpass**
Gratis version tillgänglig, stöd för 2FA och biometrisk inloggning. Enkel att använda på både mobil och dator.
- **KeePass**
Klassisk, säker och med öppen källkod. Stöd för 2FA och biometrisk inloggning via olika appar.
- **Google Lösenordshantering**
Integrerad i Android och Chrome, enkel att använda och erbjuder automatisk lagring och generering av lösenord. Stöd för biometrisk inloggning.
- **iPhone och Mac**
Även i dessa enheter finns en lösenordshanterare inbyggd.

Lista på lämpliga lösenordshanterare för mobiltelefoner m.m.

Lösenordshanterare	Säkerhet	Biometrisk inloggning	Gratisversion	2FA	Plattformer
1Password	Mycket hög	Ja	Nej	Ja	iOS, Android
Dashlane	Mycket hög	Ja	Ja (prov)	Ja	iOS, Android
Keeper	Mycket hög	Ja	Ja (prov)	Ja	iOS, Android
LastPass	Hög	Ja	Ja	Ja	iOS, Android
Bitwarden	Hög	Ja	Ja	Ja	iOS, Android
RoboForm	Hög	Ja	Ja (prov)	Ja	iOS, Android
Enpass	Hög	Ja	Ja	Ja	iOS, Android
KeePass	Hög	Ja (via appar)	Ja	Ja	iOS, Android
Google Lösenordshantering	Hög	Ja	Ja	Ja	Android, iOS

Lista på lämpliga lösenordshanterare för mobiltelefoner m.m.

Lämpliga lösenordskombinationer bör vara långa, unika, och använda både versaler, gemener, siffror och specialtecken för bästa säkerhet.

Exempel på säkra lösenordskombinationer

En lösenfras: "Tomtenärledigpåpåskén" kan göras ännu säkrare med några teckenbyten, till exempel "T0mténär!3dgpåpåsk3n".

En kombination av ord och tecken: "ShyL!0nS33S@w-p00l".

Unik ordkombination: "Anew-Slather-Unseated-Farbror-Sandy".

Slumpmässigt genererat: "jG7!xPmLk#1sQ2zT" – här blandas små och stora bokstäver, siffror och specialtecken.

Egen minnesfras med variationer: "JagGillarK4tt!MatR3cept".

Principer för starka lösenord

Minst 12–14 tecken rekommenderas, gärna fler.

Undvik vanliga ord, mönster eller personlig information som kan hittas i en ordlista.

Använd inte samma lösenord på flera ställen.

Tips för att skapa lösenord

Blanda både stora och små bokstäver, siffror och symboler.

Skapa gärna lösenord genom att sätta ihop flera slumpmässigt valda ord.

Använd gärna en lösenordshanterare, till exempel Bitwarden, 1Password eller Proton Pass, för att skapa och spara starka lösenord.

Dessa exempel och tips ger ett starkt skydd mot både enkla gissningar och automatiserade attacker

Lista på lämpliga lösenordshanterare för mobiltelefoner m.m.

Vad kännetecknar ett bra lösenord?

Ett lösenord bör vara minst 12 tecken långt (helst 16 tecken eller mer). Vår lösenordsrelaterade forskning har visat att 45 procent av amerikanerna använder lösenord på åtta tecken eller färre, vilka inte är lika säkra som längre lösenord

- Ett lösenord bör innehålla en kombination av bokstäver (både versaler och gemener), siffror och tecken.
- Du måste ha ett unikt lösenord för varje onlinekonto.
- Ett lösenord bör inte innehålla någon personlig information som din födelsedag eller adress, eftersom identitetsstöld och dataintrång kan äventyra sådan information. Det är också bäst att inte inkludera information som kan nås på sociala medier, som barns eller husdjurs namn.
- Ett lösenord bör inte innehålla några efterföljande bokstäver eller siffror (t.ex. ABCD, 1234, etc.).
- Ett lösenord bör inte bestå av ordet "lösenord" eller samma bokstav eller siffra upprepad.

Varför är lösenordssäkerhet viktigt?

Att inte ha säkra lösenord har sina konsekvenser, vilka inkluderar men inte är begränsade till:

- Efter att ha fått tillgång till en användares inloggningsuppgifter kommer många hackare att logga in på deras konton för att stjäla mer av deras personligt identifierbara information (PII) som deras namn, adresser och bankkontoinformation.
- De kommer att använda denna information antingen för att stjäla pengar direkt från användaren eller för att stjäla deras identitet. Identitetsstöld kan leda till ytterligare ekonomiska förluster eller svårigheter att få lån eller anställning.
- En hackare som bryter sig in på dina konton på grund av ett svagt lösenord kan äventyra din integritet. Om du till exempel inte ändrar standardlösenordet för dina IP-säkerhetskameror kan hackare logga in på ditt användarkonto och övervaka dig i ditt eget hem.
- För företag kan hackare starta desinformationskampanjer mot företag, dela sina data med konkurrenter och lagra dem mot en lösensumma¹.

Effekten av stulna lösenord

Komprometterade lösenord orsakade 80 procent av alla dataintrång under 2019², vilket resulterade i ekonomiska förluster för både företag och konsumenter.

Kontrollera hur starkt ett lösenord är

Med hjälp av länken <https://www.security.org/how-secure-is-my-password/> kan man kolla hur pass starkt ett lösenord är.