Lösenordsguiden

1. Varför lösenordshanterare behövs

Varje konto och tjänst kräver ett unikt lösenord. Om samma lösenord används på flera ställen innebär en dataläcka hos en enskild tjänst att alla dina konton blir sårbara.

Eftersom det är mänskligt omöjligt att memorera dussintals unika och komplexa lösenord, är den generella rekommendationen att använda en lösenordshanterare. Verktyget sparar och krypterar dina uppgifter så att du endast behöver komma ihåg ett enda huvudlösenord.

Webbläsarens inbyggda hanterar

Det är vanligt att webbläsare (som Chrome, Edge eller Firefox) erbjuder sig att spara lösenord automatiskt. Dessa är ofta sämre skyddade. Om någon får tillgång till din dator eller ditt synkroniserade Google/Microsoft-konto, får de ofta direkt tillgång till alla sparade lösenord i klartext. Stäng därför av funktionen "Erbjud att spara lösenord" i webbläsaren och låt en dedikerad

lösenordshanterare sköta all lagring.

2. Tre typer av lösenord – Välj rätt efter syfte

Vilken typ av lösenord du ska välja beror helt på hur det ska användas. Lösenord kan delas in i tre kategorier:

Kategori A: Genererade lösenord (För webbtjänster och appar)

Används för alla konton på internet och lokala tjänster (t.ex. Nextcloud, Baserow, e-post).

- **Björknets rekommenderade standard:** 20 tecken. Ska bestå av en helt slumpmässig blandning av stora och små bokstäver, siffror och specialtecken.
- **Undvik:** Tvetydiga tecken som kan förväxlas (exempelvis stort I, litet l och siffran 1).
- **Hantering**: Låt lösenordshanteraren generera och fylla i dessa automatiskt. Du ska inte memorera dem.

Kategori B: Huvudlösenord (För memorering)

Används till själva lösenordshanteraren (t.ex. Vaultwarden) eller för att låsa upp krypterade diskar.

- **Björknets rekommenderade standard:** Minst 12 tecken. Ska bestå av ord som uppfattas som slumpmässiga för utomstående, men som är möjliga för dig att memorera. Kombineras med siffror och specialtecken.
  Exempel på struktur: "f*ED|k.m@5rId¤gU&k@-135" (Fredrik Madrid Gurka)
- **Hantering:** Måste kommas ihåg utantill. Skriv aldrig ner detta digitalt.

Kategori C: Lokala lösenord (För snabb enhetsåtkomst)

Används för fysiska enheter som du har direkt tillgång till, exempelvis för att logga in på din personliga dator eller mobil.

- **Björknets rekommenderade standard:** 8–12 tecken med en blandning av stora och små bokstäver, siffror och specialtecken.

- **Hantering:** Kan hållas något kortare för att tillåta snabb inmatning, eftersom säkerheten här primärt skyddas av att enheten blockerar inloggningsförsök efter ett visst antal felaktiga inmatningar.

3. Säker hantering och delning

Ett starkt lösenord förlorar sitt värde om det hanteras oaktsamt. Följ dessa fasta regler för hantering:

Skicka aldrig lösenord i klartext: Lösenord ska aldrig skrivas direkt i chattar (såsom Nextcloud-chatt) eller i vanliga e-postmeddelanden.

Använd säkra delningsverktyg: Björknet rekommenderar och tillhandahåller verktyg för säker delning. Använd Password Pusher eller de inbyggda delningsfunktionerna i Vaultwarden när du behöver skicka ett lösenord till någon annan.

Begränsa livslängden: När du genererar en delningslänk för ett lösenord, ställ alltid in en kort giltighetstid (t.ex. några timmar) samt ett lågt maximalt antal öppningar (förslagsvis att länken raderas efter att den har öppnats en gång).

Fysisk omgivning: Var uppmärksam på din omgivning så att ingen ser när du skriver in känsliga lösenord.

Lånade enheter: Logga aldrig in på känsliga konton från publika eller lånade datorer, då du inte kan kontrollera om enheten är övervakad eller infekterad med skadlig programvara.

4. Tvåfaktorsautentisering (2FA) – Det extra skyddet

Ett lösenord – oavsett hur starkt det är – utgör bara en enda försvarslinje. Björknet rekommenderar att du alltid aktiverar tvåfaktorsautentisering (2FA) på de tjänster där det är möjligt, särskilt för kritiska konton som Nextcloud och din lösenordshanterare.

- **Så fungerar det:** Vid inloggning krävs både ditt lösenord och en tidsbegränsad engångskod (ofta 6 siffror) som genereras i en app på din telefon.
- **Varför det behövs:** Om ditt lösenord skulle läcka kan en obehörig person ändå inte logga in, eftersom de saknar den fysiska enhet som genererar koderna.

- **Rekommenderade verktyg:** Använd en dedikerad autentiseringsapp för att hantera dina koder, till exempel den inbyggda funktionen i Vaultwarden, Aegis eller Proton Authenitcatior.

5. Hantering vid misstänkt läcka

Om du misstänker att ett lösenord har kommit på avvägar måste du agera omedelbart:

- **Byt lösenord direkt:** Om ett lösenord har läckt, eller om du av misstag råkat skicka det i en öppen chatt, ska det bytas ut direkt i den berörda tjänsten.
- **Kontrollera läckor:** Du kan använda tjänster som Have I Been Pwned (vilket finns integrerat direkt i Vaultwarden) för att kontrollera om dina e-postadresser eller lösenord har förekommit i kända publika dataläckor på internet.

> “
>
> Komplexitet är säkerhetens fiende.
>
> Gary McGraw

Björknet - Infrastruktur på mänskliga villkor.

"*Humanism i digital gestaltning.*"

Magnifica Humanitas - Påven Leo XIV

Revision #3
Created 2026-06-14 05:42:01 UTC by Samuel
Updated 2026-06-14 06:46:18 UTC by Samuel