

Effektiv lösenordshantering

László Mocsáry

2026-11-24

Vad är en ’inloggningsuppgift’ ???

Består av <u>minst 2 delar</u>:

- En **’Användaridentitet’** som talar om **<u>vem</u>** du är:
  - t.ex. ditt personnummer
  - t.ex. en e-mail-adress (helst riktig e-mail-adress, dit man kan skicka e-post)
  - t.ex. ett av dig påhittat namn (t.ex. Nisse123)

- Ett **’Lösenord’** som utgör själva ’**<u>nyckeln</u>**’ till det lås som du försöker öppna t.ex. vid en inloggning.

Några exempel på ’inloggningsuppgift’

AnvID = Användaridentitet

AnvID
Lösenord

AnvID
PIN-kod

AnvID
Fingeravtryck

AnvID
Ansiktsigenkänning

AnvID
Engångskod (som SMS eller e-mail)

AnvID (personnummer)
Mobilt BankID
(med BankID-kod /ansiktsigenkänning)

2FA:

AnvID
1) Lösenord
2) Kod skickad till mobilen (SMS)

3FA:

AnvID
1) Kod skickad som e-mail
2) Kod skickad till mobilen (SMS)
3) Mobilt BankID

2FA = tvåfaktorsauktorisering

3FA = trefaktorsauktorisering

En annan säker inloggningsmetod

Lösenordsnyckel (passkey):

- **Ett nyckelpar skapas:** När du registrerar dig på en webbplats skapas två digitala nycklar. En **offentlig nyckel** som skickas till webbplatsens server, och en **privat nyckel** som sparas helt dolt och säkert på din enhet (t.ex. din mobil eller dator).

- **Verifiering med biometri:** När du ska logga in ber webbplatsen din enhet att bevisa att den har den privata nyckeln. Du godkänner detta genom att låsa upp din enhet med **ansiktsigenkänning (FaceID), fingeravtryck eller din enhets PIN-kod**.

- **Säker matchning:** Din enhet signerar en digital utmaning från webbplatsen med din privata nyckel. Webbplatsen kontrollerar signaturen med sin offentliga nyckel och släpper in dig. **Ditt faktiska fingeravtryck eller din PIN-kod skickas aldrig över internet.**

Apples Keychain (iCloud nyckelring) fungerar exakt så på **iPhone, iPad och Mac,** och synkroniseras mellan alla Apple-enheter. Det är Apple har utvecklat denna standard och byggt in den i sina operativsystem (iOS, iPadOS och macOS).

Var förvarar man sina inloggningsuppgifter ?

1) Den allra enklaste metoden:



OBS:

- Glöm inte att stryka över ’gamla’ inloggningsuppgifter t.ex. när du byter/återställer ett lösenord.
- Förvara anteckningsboken på ett ställe som du alltid kommer ihåg, t.ex. en bestämd plats i en bokhylla.
- Ibland är det bra att du har antecknings-boken med dig, när du är ute och rör på dig.
- Tappa inte bort den !!! Och glöm inte kvar den på en kursgård… 🤔

Var förvarar man sina inloggningsuppgifter ?

2) ’Anteckningar’ på någon av dina enheter

Här är några lösryckta exempel:

Smartphone	**Google Keep** (app både iPhone och Android) **Word**-dokument / **Excel**-kalkylark
Surfplatta	**Google Keep** (app både iPhone och Android) **Word**-dokument / **Excel**-kalkylark
Dator/laptop	**Google Keep** (via en web-läsare) **Word**-dokument / **Excel**-kalkylark

Det finns alla möjliga appar för ’Anteckningar’ både i Android- och Apple-världen (t.ex. Inkpad, Notepad, MS To Do, MS OneNote, ….).

OBS: Google Keep kräver att du är inloggad på ditt Google-konto.

Var förvarar man sina inloggningsuppgifter ?

3) Lösenordshanterare

Välrenommerade exempel:

1. **Proton Pass** (**gratis**, synk till alla sorters enheter)
2. **Bitwarden** (**gratis**, obegränsat antal enheter)
3. **Nordpass** (**gratis**, 1 enhet åt gången)
4. **DashLane** (**gratis**, 25 lösenord, 1 enhet bara)
5. **mSecure** (**inte gratis**, Android-tfn & surfplattor)
6. **Norton Password Manager** (**inte gratis**, synk till alla sorters enheter)
7. **Samsung Pass** (för t.ex. anteckningar, inloggningar till webplatser, kreditkortsuppgifter)

Var skall man helst inte förvara sina inloggningsuppgifter ?

Sparade i en web-läsare

(Chrome, Edge, Firefox, Vivaldi, Brave,…. osv)

Problem:

- Visserligen förvaras lösenord krypterade i en lokal databas på datorn.
- Men skyddet av krypteringsnyckeln är t.ex. beroende av t.ex. Windows inbyggda säkerhetsfunktioner.
- Om man kommer över inloggningsuppgifterna till t.ex. Windows 11, så kan krypteringsnyckeln vara kompromitterad.
- Om flera personer använder samma Windows-konto kan den ene använda den andres sparade lösenord.
- Det är riskfyllt att slentrianmässigt (åter)använda samma lösenord på olika web-platser!
- Det är alldeles för enkelt att ta bort (= tappa bort) sparade lösenord från web-läsarens lokala databas.

Min slutsats:

- Svara **NEJ** om web-läsaren frågar dig om du vill spara lösenordet när du loggar in på en web-plats.

Vad är en lösenordshanterare ???

1. En **förvaringsplats** (kassavalv, krypterad) för dina inloggningsuppgifter (det s.k. **Valvet**).

2. **Valvet** öppnas med ett **Huvudlösenord** (’Master Password’).

3. **Valvet** är **åtkomligt** på alla sorters enheter (smartphone, surfplatta, laptop, stationär dator).

4. Kan **fylla i** inloggningsuppgifter på web-sidor med en simpel knapptryckning. Kan också skapa ’**svår-knäckta**’ lösenord, som du inte behöver komma ihåg.

Hur bra är ett lösenord ???

Antal tecken	Bara tal	Bara gemener	Stora och små bokstäver	Tal, stora och små bokstäver	Tal, stora och små bokstäver samt symboler
4	Ögonblickligen	Ögonblickligen	Ögonblickligen	Ögonblickligen	Ögonblickligen
5	Ögonblickligen	Ögonblickligen	57 minuter	2 timmar	4 timmar
6	Ögonblickligen	46 minuter	2 dagar	6 dagar	2 veckor
7	Ögonblickligen	20 timmar	4 månader	1 år	2 år
8	Ögonblickligen	3 veckor	15 år	62 år	164 år
9	2 timmar	2 år	791 år	3 000 år	11 000 år
10	1 dag	40 år	41 000 år	238 000 år	803 000 år
11	En vecka	1 000 år	2 miljoner år	4 miljoner år	56 miljoner år
12	3 månader	27 000 år	111 miljoner år	917 miljoner år	3 miljarder år
13	3 år	705 000 år	5 miljarder år	56 miljarder år	275 miljarder år
14	28 år	18 miljoner år	300 miljarder år	3 biljoner år	19 biljoner år
15	284 år	477 miljoner år	15 biljoner år	218 biljoner år	1 kvadriljon år
16	2 000 år	12 miljarder år	812 biljoner år	13 kvadriljon år	94 kvadriljoner år
17	28 000 år	322 miljarder år	42 kvadriljoner år	840 kvadriljoner år	6 kvintiljoner år
18	284 000 år	8 biljoner år	2 kvintiljoner år	52 kvintiljoner år	463 kvintiljoner år

Vi ska titta lite närmare på…

Proton Pass
(gratis)
Man öppnar ett gratis Proton-konto.

resp.

Norton Password Manager
(ej gratis)
Ingår i Norton 360-säkerhetspaketet.

Slutligen…

Fortsatt diskussion och fler frågor ?!?

The End

Tack för idag! 