

# Så kollar du om ditt lösenord har läckt



Uppdaterad 13:59 Publicerad 11:00



Foto: Evelien DOosje/Alamy

**Under de senaste dagarna har flera medier rapporterat om en stor läcka av svenskers inloggningsuppgifter som spridits på nätet.**

**DN:s Hugo Ewald svarar på tre frågor om läckan.**



**Hugo Ewald Hurinsky**

Text



## Vad är det som har hänt?

I september 2023 publicerades en stor lista över inloggningsuppgifter på ett internetforum där användare köper och säljer stulna databaser. Filen består av drygt 70 miljoner unika mejladresser.

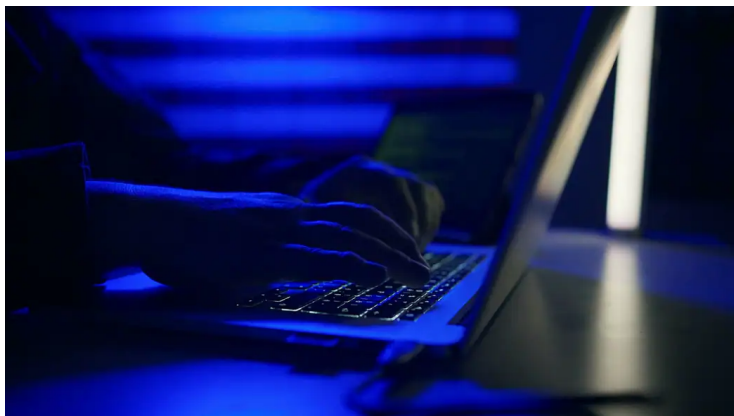
Läckan väckte ingen större uppmärksamhet förrän den 18 januari, när säkerhetsexperten Troy Hunt skrev [ett blogginlägg](#) om lösenordsläckan. Den blev mer känd i Sverige när svenska medier tidigare i veckan uppmärksammade blogginlägget. Förmodligen är själva läckan äldre än från september 2023, då

den i sin tur uppges komma från en nu nedlagd sökmotor för läckt data.

### Bör jag vara orolig?

Nya databasläckor består ofta av sammanslagningar av återanvända, gamla läckor. Ofta är lösenorden många år gamla. I många fall är det inte heller själva lösenorden som är läckta, utan krypterade versioner av lösenorden som inte alltid går att knäcka.

Den här lösenordsläckan är intressant eftersom den innehåller många e-postadresser som inte tidigare återfunnits i läckor. Den är dock betydligt mindre än tidigare stora läckor som i vissa fall innehållit uppgifter till hundratals miljoner konton. Det är som i fallet med många andra större läckor oklart hur gamla inloggningsuppgifterna är och om de ens kommer från sajter som fortfarande finns.



Att använda unika lösenord och byta dessa regelbundet kan hindra obehöriga från att komma åt dina konton. Foto: Jozef Polc/Alamy

Har du använt exakt samma lösenord på en stor mängd sajter kan det finnas en risk att någon skulle kunna använda uppgifterna i läckan för att försöka logga in på tjänster. Men de flesta större sajter använder i dag så kallad tvåfaktorsinloggning; att man använder en extra kod från en app eller ett sms, förutom lösenordet. Sajter som Facebook lägger också i dag ofta märke till om någon försöker logga in på ditt konto från en ny plats, och berättar det för dig.

Det bästa sättet att hålla sig säker från lösenordsläckor är att använda unika lösenord på alla sajter, samt att [aktivera tvåfaktorsinloggning](#) när du har möjlighet att göra det. Du kan också [använda dig av en lösenordshanterare](#).

### Hur vet jag om jag är drabbad?

Det finns i dag flera sajter du som privatperson kan besöka för att se om dina inloggningsuppgifter läckt. Störst är [Haveibeenpwned.com](#), som drivs av ovan nämnda Troy Hunt. Där kan du också se om dina uppgifter finns med i någon tidigare läcka.

Text



**Hugo Ewald Hurinsky**  
hugo.ewald@dn.se

Följ

© Detta material är skyddat enligt lagen om upphovsrätt