

Sikker lagring av passord på PC og mobiltelefon

Beskytt personlig informasjon med
effektive metoder



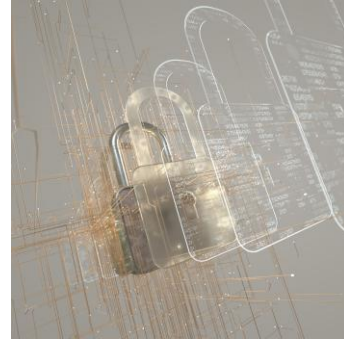
Agenda for Presentasjonen

- Introduksjon til passordsikkerhet
- Metoder for lagring av passord
- Passordbehandlere: Funksjoner og fordeler
- Sikkerhetspraksis for PC og mobiltelefon
- Anbefalinger og beste praksis



Introduksjon til passord sikkerhet

Hvorfor er passordsikkerhet viktig?



Beskyttelse av sensitiv informasjon

Sikre passord er nødvendig for å beskytte sensitiv informasjon som bankdetaljer og private e-poster fra uautorisert tilgang.



Risiko for identitetstyveri

Svake passord kan føre til identitetstyveri, noe som kan resultere i betydelige økonomiske tap og skade på ens rykte.



Hackertrusler

Hackere bruker avanserte verktøy for å knekke svake passord, derfor er det viktig å bruke sterke og unike passord.





Vanlige trusler og risikoer

Phishing

Phishing er en type svindel der angriperen prøver å lure brukere til å gi fra seg sensitiv informasjon, som passord.

Brute-force angrep

Brute-force angrep involverer å forsøke å gjette passord ved å bruke mange kombinasjoner til man finner riktig passord.

Malware

Malware er skadelig programvare som kan infisere enhetene dine og forårsake skade eller tap av data.





Konsekvenser hvis passord kommer på avveie

Identitetstyveri

Det kan føre til identitetstyveri, hvor angripere kan misbruke din personlige informasjon til urettmessige formål.

Brudd på personvern

Det kan også føre til brudd på personvernet, der sensitiv informasjon blir eksponert for tredjeparter.

Økonomiske tap

Tap av økonomiske midler kan skje som følge av svindel og uautorisert tilgang til bankkontoer og kredittkort.



Her er noen eksempler



- Noen kan få tilgang til din nettbank og stjele penger
- E-posten din kan brukes til å sende svindel til venner
- Kontoer hos nettbutikker kan misbrukes til å handle i ditt navn
- Private bilder og dokumenter kan bli åpnet og delt
- Du kan få falske regninger eller bli utsatt for ID-tyveri



Metoder for lagring av passord



gnistr.net Sponset ·

«Passordboken» – Aldri mist et passord igjen!
I en verden full av koder og kontoer, gjør «Passordboken» livet enklere. Med alfabetiske faner og praktiske seksjoner, har du alltid kontroll på passordene dine – og andre viktige detaljer.



gnistr.net
Pengene-tilbake-garanti – Test «Passordboken» uten risiko! [Finn ut mer](#)

11 6 kommentarer

Liker Kommenter Del

Afentaler Sára Handball · Følg

Startside Video Venner Marketplace Vars



Tradisjonelle metoder: Notater og dokumenter

Fysiske notater for passord

Mange brukere lagrer passordene sine i fysiske notater, noe som kan virke praktisk.

Sikkerhetsrisikoer

Lagring av passord på papir kan være usikkert, da de kan bli funnet av andre.

Alternative lagringsmetoder

Det finnes sikrere metoder for passordlagring, som digitale passordbehandlere, som anbefales.



Moderne metoder: Passordbehandlere !

Sikker lagring av passord

Passordbehandlere gir en sikker løsning for å lagre passordene dine **ved hjelp av kryptering** for å beskytte dataene.

Enkel tilgang til passord

Med en passordbehandler får du enkel tilgang til passordene dine, noe som gjør håndteringen mer praktisk og effektiv.

Anbefalt sikkerhetspraksis

Bruk av passordbehandlere er en anbefalt praksis for sikker passordlagring og for å forhindre datainnbrudd.

Sikkerhet i nettlelere



Passordlagring i nettlelere

Nettlelere tilbyr ofte innebygde funksjoner for lagring av passord, noe som gir brukerne praktisk tilgang til sine kontoer.

Risiko ved passordlagring

Selv om det er praktisk å lagre passord i nettleseren, kan det medføre sikkerhetsrisikoer dersom uvedkommende får tilgang til nettleseren, eller hvis enheten mistes..

Sikker bruk av funksjoner

Det er viktig å bruke passordlagrings funksjoner på en sikker måte, for eksempel ved å aktivere to-faktor autentisering og holde programvaren oppdatert.



Du bør ikke lagre passord i nettleseren!

- Lagring av passord i nettleseren kan være praktisk, men det kan være svært risikabelt.
- Kort fortalt har alle som har tilgang til enheten og nettleseren din enkel tilgang til passordene dine.
- Nettkriminelle kan få ekstern tilgang til enheten din via malware og andre typer nettangrep, og det er også en fare for at noen stjeler enheten din.



Passordbehandlere: Funksjoner og fordeler

Hvordan fungerer passordbehandlere?

Kryptert datalagring

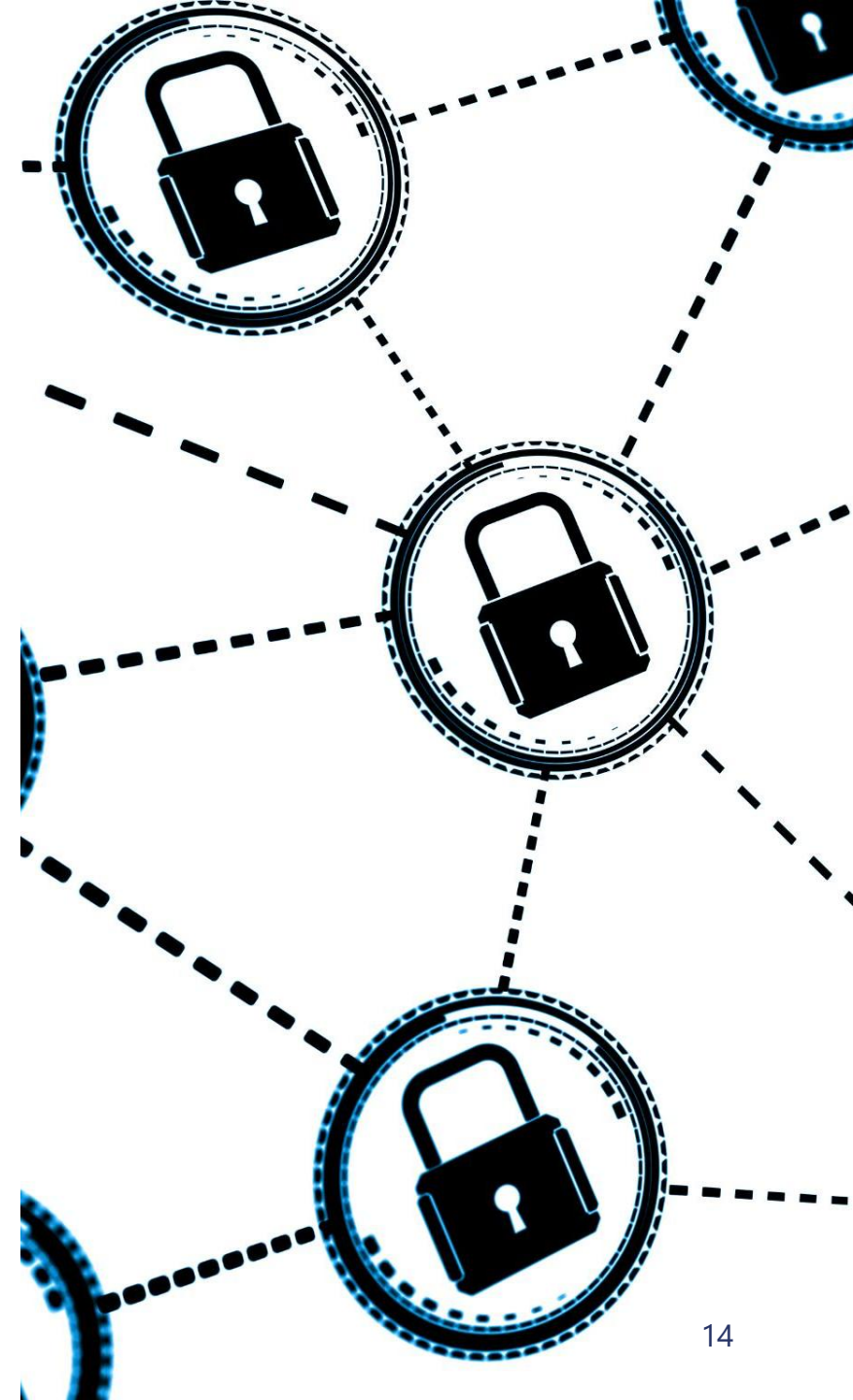
Passordbehandlere lagrer passordene dine sikkert i en kryptert database for å forhindre uautorisert tilgang.

Hovedpassord og autentisering

Bruk av ett hovedpassord eller biometrisk autentisering gir sikker tilgang til lagrede passord.

Generering av sterke passord

Passordbehandlere hjelper deg med å generere sterke og unike passord for dine kontoer, som øker sikkerheten.





Eksempler på populære passordbehandlere

LastPass

LastPass er en av de mest populære passordbehandlerne, kjent for brukervennlighet og sikkerhetsfunksjoner.

1Password







1Password tilbyr avanserte sikkerhetsfunksjoner, inkludert tofaktor autentisering og sikker deling av passord.

Bitwarden

Bitwarden er en åpen kildekode passordbehandler som er kostnadseffektiv og har et sterkt fokus på sikkerhet.



Flere eksempler på passordbehandlere

-
- [KEEPER](#)  (ca. kr 400 pr år)
 - LastPass  (ca. kr 400 pr år)
 - DASHLANE  (\$60 pr år)
 - Bitwarden  (\$10 pr år)
 - 1Password  (\$36 pr år)
 - RoboForm  (\$24 pr år)



Test utført av nettstedet "WIRED" konkluderer:

- I. Best for folk flest : **Bitwarden** (Premium \$10 pr år)
- II. Beste oppgradering : **1Password** (Single \$36 pr år)
- III. Beste fullfunksjonelle : **Dashlane** (Single \$60 pr år)
- IV. Best for pakketjenester : **NordPass** (Premium \$40 pr år)

Fordeler ved bruk av passordbehandlere

Økt sikkerhet

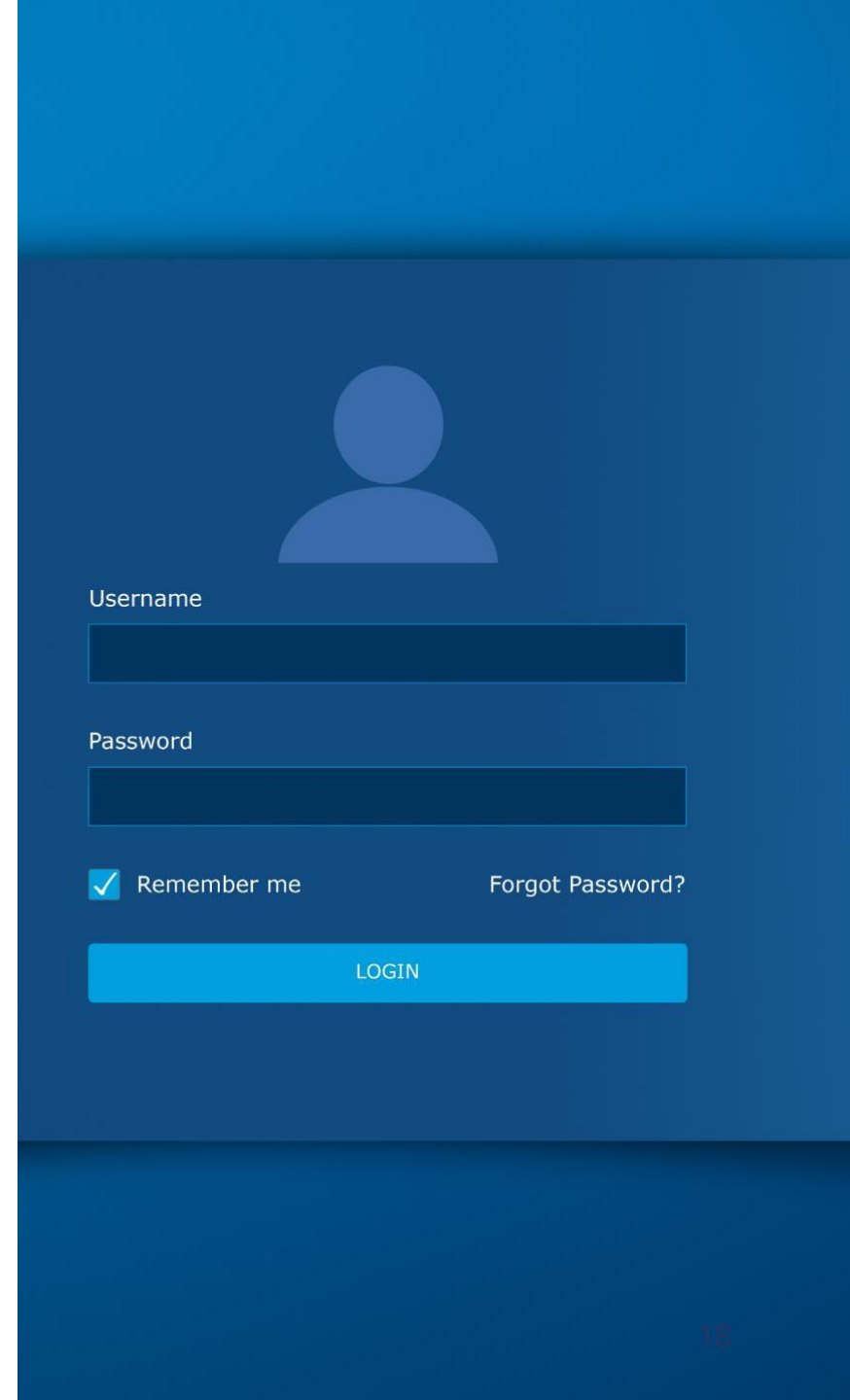
Passordbehandlere lagrer og krypterer passordene dine, noe som gir bedre beskyttelse mot hacking og datainnbrudd.

Bekvemmelighet

Med en passordbehandler trenger du bare å huske ett hovedpassord, noe som forenkler håndteringen av mange kontoer.

Styrke unike passord

Passordbehandlere gjør det enkelt å generere sterke og unike passord for hver konto, noe som reduserer risikoen for databrudd.





Sikkerhetspraksis for PC og mobiltelefon

Sterke passord og tofaktor autentisering



Betydningen av sterke passord

Sterke passord er avgjørende for å beskytte kontoer mot hacking og uautorisert tilgang. De bør være lange og komplekse.

Tofaktorautentisering

Tofaktor autentisering gir ekstra sikkerhet ved å kreve én ekstra bekreftelse, som f.eks en kode sendt til mobiltelefonen.



Gode passordvaner

- Bruk minst 12 tegn med bokstaver, tall og symboler.
- Unngå navn, fødselsdatoer og enkle ord som "123456" eller "passord".
- Ikke bruk samme passord flere steder



Passord på iPhone, med iCloud nøkkelring

- Lagre passord i iCloud nøkkelring på Apple-enheter
- Dette er en enkel måte å lagre passord på, og hente innloggingsdetaljene når du trenger dem på en nettside eller i en app.
- Brukernavn og passord lagres trygt i Apples nettsky, med kryptering under lagring og overføring.

iOS 18 og Passord

- Alle som har oppdatert til iOS 18 har fått en ny app på sin smarttelefon. Dette er en passordapp.
- I den kan du lagre alle dine passord, wifi passord og kodenøkler til nettsteder.
- [App Passord på iPhone](#)





Oppdatering og vedlikehold av enheter



Viktigheten av oppdateringer

Regelmessige oppdateringer er avgjørende for å beskytte mot sårbarheter og angrep på enhetene dine.

Automatiske oppdateringer

Det anbefales å aktivere automatiske oppdateringer for å sikre at enhetene alltid er oppdatert med de nyeste sikkerhetsfunksjonene.

Sikkerhetskopiering av passorddata

Betydningen av sikkerhetskopiering

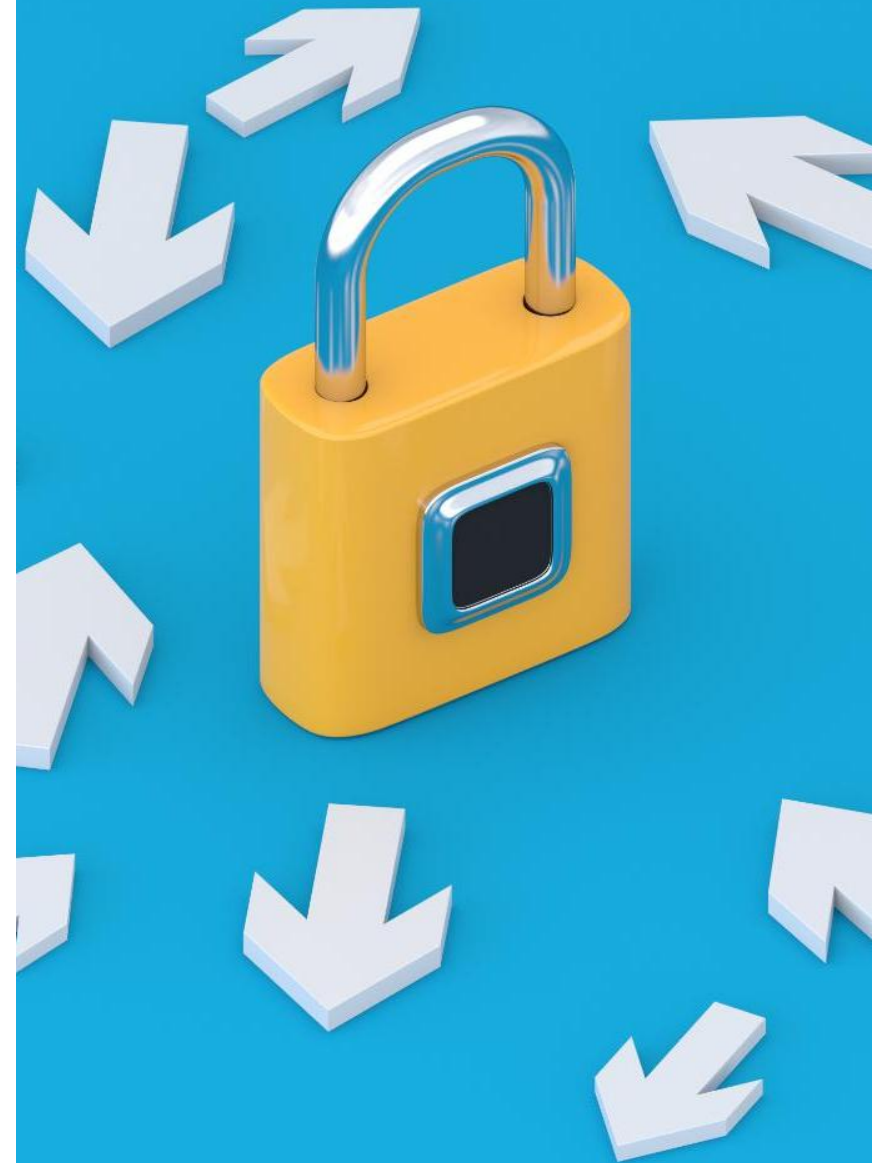
Sikkerhetskopiering av passorddata er avgjørende for å hindre tap av viktig informasjon og beskytte personopplysninger.

Alternativer for sikkerhetskopiering

Mange passordbehandlere tilbyr innebygde sikkerhetskopieringsmuligheter, noe som gjør det enklere å beskytte passordene dine.

Sikre lagringsplasser

Det er lurt å lagre sikkerhetskopiene på et trygt sted, enten lokalt eller i skyen, for å unngå uautorisert tilgang.





Anbefalinger og beste praksis



Unike passord for forskjellige kontoer

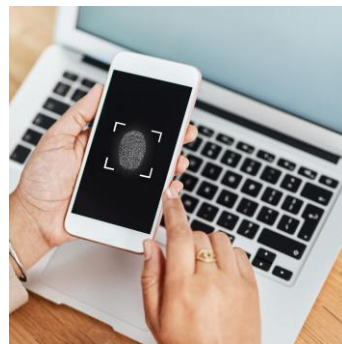
Redusere sikkerhetsrisiko

Unike passord for hver konto reduserer risikoen for omfattende databrudd, og beskytter sensitive opplysninger.

Viktig sikkerhetspraksis

Å bruke unike passord er en enkel, men effektiv metode for å forbedre personlig nettsikkerhet.

Bruk av biometrisk autentisering



Sikkerhetsfordeler

Biometrisk autentisering gir høyere sikkerhet sammenlignet med tradisjonelle passord, da det er vanskeligere å kopiere biometriske data.

Praktisk bruk

Bruken av biometrisk autentisering er praktisk, da brukere enkelt kan få tilgang til enheter med sitt unike biometriske kjennetegn.

Moderne enheter

Mange moderne enheter, inkludert smarttelefoner og bærbare datamaskiner, har innebygd støtte for biometrisk autentisering.





Vanlige fallgruver

- Å dele passord med andre – selv familie.
- Å klikke på lenker i e-poster som ber om passord.
- Å bruke gamle passord over lang tid.

Regelmessige sikkerhetskontroller



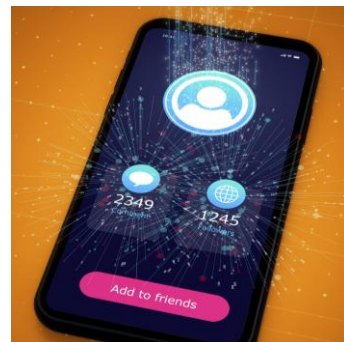
Oppdatere passord

Regelmessig oppdatering av passord er avgjørende for å opprettholde sikkerheten på kontoene dine. Bruk sterke og unike passord for hvert av dine kontoer.



Tofaktorautentisering

Sjekk innstillingene for tofaktorautentisering for å legge til et ekstra lag av sikkerhet på kontoene dine. Dette beskytter deg mot uautorisert tilgang.



Sjekke kontoaktivitet

Overvåk kontoene dine for ukjente aktiviteter eller unormale pålogginger. Dette kan bidra til å oppdage sikkerhetsbrudd tidlig.



Konklusjon

Sikkerhetspraksis

For å hindre uautorisert tilgang til passordene dine, er det viktig å ta i bruk robuste sikkerhetstiltak.

Bruk av passordbehandlere

Passordbehandlere kan hjelpe med å generere og lagre sterke passord, og gjøre sikkerheten mer effektiv.

Vær oppmerksom på trusler

Ved å kjenne igjen vanlige svindelmetoder som falske e-poster og virus, kan du lettere unngå at passordene dine kommer på avveie.