



NAVN:

Martin Lorentsen

ALDER:

29 år

STILLING:

Journalist i
Komputer for alle

Kort om
VeraCrypt

Det er ingen hyggelig tanke at uvedkommende kan få tilgang til private filer – og det sikrer du deg mot med verktøyet VeraCrypt. For ved å lagre filer i virtuelle stasjoner som takket være avansert kryptering bare kan åpnes med ditt eget passord, er filene dine i sikkerhet. Da trenger du ikke bekymre deg for at en person som får tak i pc-en også får tilgang til dine private opplysninger.



Lagre konfidensielle filer bak lås og slå

Det er frustrerende og irriterende å miste pc-en. Men selve tapet av datamaskinen er ikke noe i forhold til tanken på at filene dine samtidig kan havne i feil hender. Jeg lagrer filer med personopplysninger, for eksempel bankdokumenter der kontoopplysningene mine fremgår, helsejournaler med personnummer og annen viktig digital post, i mapper på datamaskinen. Dokumentene gjør meg på ulike måter utsatt, og derfor er jeg selvfølgelig den eneste som bør ha tilgang til filene. Hvis de havner hos en kriminell, kan det uten tvil få alvorlige konsekvenser.

Bare tanken gjør meg utrygg, og derfor har jeg ingen pc uten programmet VeraCrypt installert. Programmet kan nemlig kryptere datamaskinens filer, og det vil i hovedsak si at filene blir låst ved hjelp av avanserte algoritmer, og bare ved å skrive inn et passord som jeg selv har valgt kan de krypterte filene eller mappe åpnes.

Tilgang krever passord

For å kryptere filene med VeraCrypt kreves det at du setter av litt plass på pc-ens harddisk til å opprette en såkalt virtuell stasjon. Harddisken kan brukes ak-

kurat som en vanlig harddisk på pc-en, men du kan bare bruke den hvis du har angitt passordet. Ellers vil stasjonen bare opptre som en enkelt, låst og uleselig fil på datamaskinen. Hvis uhellet skulle være ute og du mister pc-en, er det altså umulig for uvedkommende å åpne filene dine, med mindre de har passordet til den krypterte stasjonen.

VeraCrypt

Last ned programmet via
www.komputer.no/0223

Om programmet
Krypter viktige filer slik at de låses.

Systemkrav
Windows 10 og 11

Språk
Engelsk

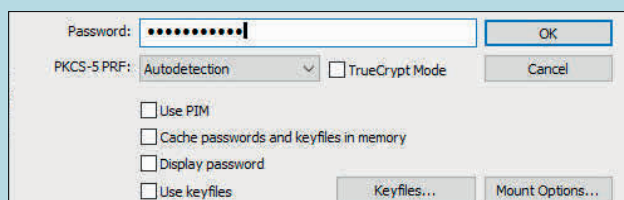


Lås filer med passordet

En kryptert fil vil være umulig å åpne for en potensiell tyv som får tilgang til pc-en. Tyven vil bare se krypteringsfilen som en vanlig fil uten filendelse, og selv om han har VeraCrypt og åpner filen i programmet vil innholdet ikke være synlig. Det krever nemlig passordet ditt, som du velger når du oppretter en kryptert stasjon med VeraCrypt.

Derfor er det viktig at du velger et sterkt passord som både er vanskelig å knekke for tyvene og lett for deg å huske. Dette får du hjelp til på nettsiden vår. Besøk adressen nedenfor for å lese artikkelen der tre sikkerhetseksperter gir gode råd:

www.komputer.no/password



Når du skal låse opp filene, skriver du bare inn passordet du har valgt for den krypterte stasjonen og klikker på OK.



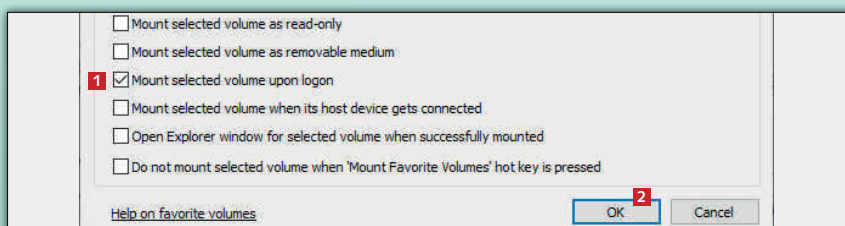
Kom i gang med VeraCrypt

I Fordelssonen finner du en utførlig veiledning til VeraCrypt som hjelper deg med å komme i gang med programmet. Finn artikkelen med veiledningen og last den ned som PDF-fil via adressen nedenfor.

www.komputer.no/0223

Gjør det enklere å bruke stasjonen i hverdagen

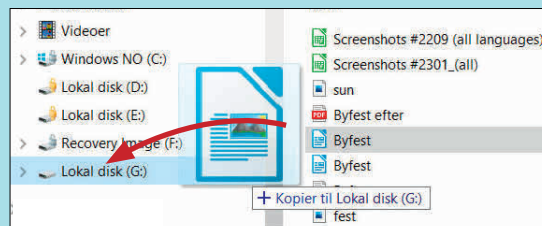
VeraCrypts krypterte stasjon med filene dine er bare synlig i Filutforsker når den blir montert – eller åpnet – med programmet. Du må fortsatt skrive inn passordet for å låse opp stasjonen selv om den er synlig i Filutforsker, men hvis den ikke er montert med VeraCrypt, kan harddisken ikke vises i det hele tatt. Derfor er det en god idé å få VeraCrypt til å montere den krypterte stasjonen automatisk når Windows startes. I veiledningen til høyre ser du hvordan du gjør dette i VeraCrypts innstillinger.



1 I VeraCrypt må du først montere den krypterte stasjonen. Når det er gjort, klikker du på **Favorites** og velger **Add Mounted Volume to Favorites...** fra menyen. Merk deretter av for **Mount selected volume upon login** 1, slik det er gjort her. Klikk på **OK** 2. Da vil stasjonen automatisk bli montert når du starter Windows.

Dra filer enkelt i sikkerhet

I Filutforsker opptrer den krypterte stasjonen som om det var en hvilken som helst annen stasjon på pc-en, f.eks. et tilkoblet USB-minne. Vanligvis ser du den krypterte stasjonen som en flyttbar disk i oversikten til venstre, og som tilfellet er med nettopp et flyttbart USB-minne eller en ekstern harddisk, kan du enkelt legge til filer i den krypterte stasjonen. Bare dra dem over til stasjonen fra et annet sted på harddisken, så opprettes det en kopi av filen på den krypterte stasjonen. Deretter er det en god idé å slette filen fra det andre stedet på harddisken, slik at filen nå kun finnes i sikkerhet på den låste stasjonen.



Klikk på filen eller mappen du vil legge til i den krypterte stasjonen, hold museknappen nede og dra filen eller mappen til den krypterte stasjonen i Filutforsker. Da er filen lagt i sikkerhet bak VeraCrypts kryptering.