REDAKTIONENS FAVORIT PROGRAMMER

NAVN:
Martin Lorentsen

ALDER:
29 år

STILLING:
Journalist på Komputer for alle

VeraCrypt kort fortalt

Det er ingen rar tanke, at uvedkommende kan få adgang til dine private filer – og det sikrer du dig mod med værktøjet VeraCrypt. For ved at gemme filer i virtuelle drev, som takket være avanceret kryptering kun kan åbnes med dit eget kodeord, kommer dine filer i sikkerhed. Således skal du ikke bekymre dig om, at en person, der får fingrene i din pc, også får adgang til dine private oplysninger.

DERFOR ER JEG VILD MED VERACRYPT:

Gem fortrolige filer bag lås og slå

Det er frustrerende og ærgerligt at miste sin pc. Men selve tabet af computeren er intet i forhold til tanken om, at dine filer samtidig kan havne i de forkerte hænder. Jeg gemmer fx filer med personfølsomme oplysninger som bankdokumenter, hvor mine kontooplysninger fremgår, sundhedsjournaler med mit CPR-nummer og anden vigtig digital post i mapper på computeren. Dokumenterne gør mig på den ene eller anden måde udsat, og derfor er jeg selvfølgelig den *eneste*, der skal have adgang til filerne. Hvis de havner hos en kriminel, kan det uden tvivl få alvorlige konsekvenser.

Bare tanken gør mig utryg, og derfor har jeg ingen pc uden programmet VeraCrypt installeret. Programmet kan nemlig kryptere computerens filer, og det vil i bund og grund sige, at filerne bliver låst ved hjælp af avancerede algoritmer, og kun ved at indtaste et kodeord, som jeg selv har valgt, kan de krypterede filer eller mapper åbnes.

Adgang kræver en kode

For at kunne kryptere filerne med VeraCrypt kræver det, at du afsætter noget plads fra pc'ens harddisk til at oprette et såkaldt virtuelt drev. Drevet kan bruges præcis som en almindelig harddisk på pc'en, men du kan kun bruge det, hvis du har indtastet adgangskoden til det. Ellers vil drevet blot optræde som en enkelt, låst og ulæselig fil på computeren. Hvis uheldet skulle være ude, og du mister din pc, er det altså umuligt for uvedkommende at åbne dine filer, medmindre de har koden til det krypterede drev.

VeraCrypt

Hent programmet på
www.komputer.dk/0223

Om programmet
Krypter dine vigtige filer, så de bliver låst.

Systemkrav
Windows 10 og 11

Sprog
Engelsk

FORDELSZONEN

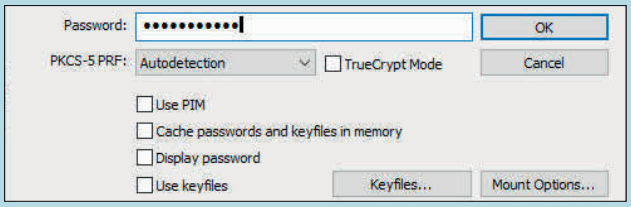
Foto: Shutterstock

Lås filer med dit kodeord

En krypteret fil vil være umulig at åbne for en potentiel tyv, der får adgang til pc'en. Tyven vil blot se krypteringsfilen som en normal fil uden filendelse, og selv om han har VeraCrypt og åbner filen i programmet, vil indholdet ikke være synligt. Det kræver nemlig dit kodeord, som du vælger, når du opretter et krypteret drev med VeraCrypt.

Derfor er det vigtigt, at du vælger et stærkt kodeord, som både er vanskeligt at knække for tyvene og nemt for dig at huske. Det får du hjælp til på vores hjemmeside. Besøg nedenstående adresse for at læse artiklen, hvor tre sikkerhedseksperter giver gode råd:

www.komputer.dk/password



Når du skal låse filerne op, skal du blot indtaste den kode, du har valgt til det krypterede drev, og klikke på knappen OK.

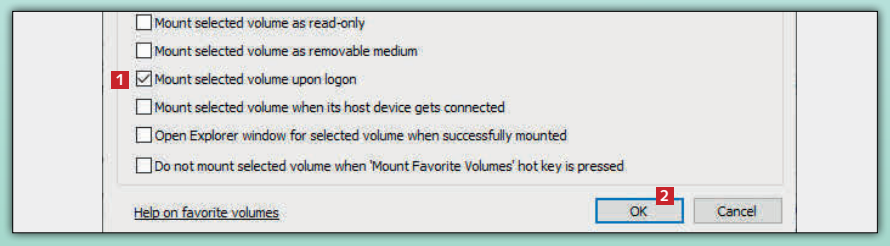
Kom godt i gang med VeraCrypt

I Fordelszonen finder du en udførlig vejledning til VeraCrypt, som hjælper dig med at komme godt i gang med programmet. Find artiklen med vejledningen, og hent den som PDF-fil via nedenstående adresse.

www.komputer.dk/0223

Gør det nemmere at bruge dit drev i hverdagen

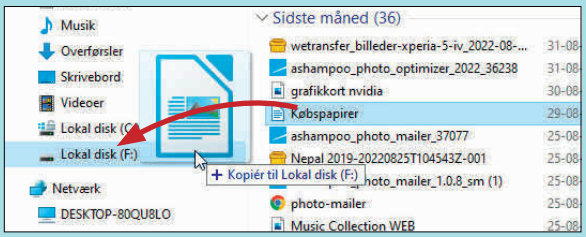
VeraCrypts krypterede drev med dine filer er kun synligt i Stifinder, når det bliver monteret – eller åbnet – med programmet. Du skal stadig indtaste din kode for at låse drevet op, selv om det er synligt i Stifinder, men hvis ikke det er monteret med VeraCrypt, kan drevet slet ikke ses. Derfor er det en rigtig god idé at få VeraCrypt til automatisk at montere det krypterede drev, når Windows startes. Her i vejledningen til højre kan du se, hvordan du gør det i VeraCrypts indstillinger.



1 I VeraCrypt skal du først montere dit krypterede drev. Når det er gjort, klikker du på punktet **Favorites** og vælger **Add Mounted Volume to Favorites...** fra menuen. Sæt så flueben ved **Mount selected volume upon logon** 1, som det er sat her, og klik på knappen **OK** 2. Så vil drevet automatisk blive monteret, når du starter Windows.

Træk nemt filer i sikkerhed

I Stifinder optræder det krypterede drev, som var det et hvilket som helst andet drev på pc'en, fx en tilsluttet USB-nøgle. Typisk ser du det krypterede drev som en flytbar disk i oversigten ude til venstre, og som tilfældet er med netop en flytbar USB-nøgle eller en ekstern harddisk, kan du nemt tilføje filer til det krypterede drev. Du skal blot trække dem over i drevet fra et andet sted på harddisken, og så er en kopi af filen oprettet i det krypterede drev. Herefter er det en god idé at slette filen fra det andet sted på harddisken, så filen nu *kun* findes i sikkerhed på det låste drev.



Du skal blot klikke på den fil eller den mappe, du vil tilføje til det krypterede drev, holde museknappen nede og trække filen eller mappen over i det krypterede drev i Stifinder. Så er filen lagt i sikkerhed bag VeraCrypts kryptering.