



NAMN:

Martin Lorentsen

ÅLDER:

29 år

BEFATTNING:

Journalist på
PC-tidningen

VeraCrypt i korthet

Det är ingen trevlig tanke att obehöriga kan komma åt dina privata filer – och det skyddar du dig bäst mot med verktyget VeraCrypt. Genom att spara filer i virtuella enheter som tack vare avancerad kryptering endast kan öppnas med ditt lösenord kommer filerna att vara i säkerhet. På så sätt behöver du inte oroa dig för att den som får tag på datorn också får tillgång till dina privata uppgifter.



Spara hemliga filer bakom lås och bom

Det är frustrerande och förargligt att förlora sin dator. Själva förlusten av datorn är däremot ingenting jämfört med tanken på att dina filer samtidigt kan hamna i orätta händer. Jag sparar till exempel filer med känsliga personuppgifter som bankdokument, där mina kontouppgifter finns, journaler med mitt personnummer och annan viktig digital post i mappar på datorn. Dokumenten gör mig utsatt på det ett eller det andra viset, och därför är jag självklart den enda som ska ha tillgång till filerna. Om de hamnar hos en kriminell kan det utan tvekan få allvarliga konsekvenser.

Blotta tanken gör att jag känner mig otrygg. Därför har jag ingen dator utan VeraCrypt installerat. Programmet kan nämligen kryptera datorns filer, och det innebär enkelt uttryckt att filerna låses med hjälp av avancerade algoritmer. Bara genom att skriva in ett lösenord som jag själv har valt kan de krypterade filerna eller mapparna öppnas.

Lösenord krävs för åtkomst

För att kryptera filerna med VeraCrypt krävs det att du avsätter lite utrymme på datorns hårddisk för att skapa en så kallad virtuell enhet. Den enheten kan

användas som en vanlig hårddisk på datorn, men du kan bara använda den om du har angett lösenordet till den. Annars kommer enheten enbart att fungera som en låst och oläslig fil på datorn. Om olyckan skulle inträffa och du förlorar din dator är det omöjligt för obehöriga att öppna dina filer, såvida de inte har fått tag på lösenordet till den krypterade enheten.

VeraCrypt

Hämta programmet på

www.pctidningen.se/0223

Om programmet

Kryptera dina viktiga filer, så att de blir inlästa.

Systemkrav

Windows 10
och 11

Språk

Engelska



FÖRDELSONEN

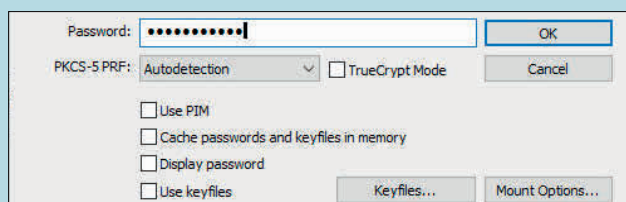


Lås filer med ett lösenord

En krypterad fil är omöjlig att öppna för en eventuell tjuv som får tillgång till datorn. Tjuven ser bara krypteringsfilen som en normal fil utan filändelse, och även om hen har VeraCrypt och öppnar filen i programmet kommer innehållet inte att vara synligt. För det krävs nämligen ditt lösenord, som du väljer när du skapar en krypterad enhet med

VeraCrypt. Därför är det viktigt att du väljer ett kraftfullt lösenord som både är svårt att knäcka för tjuvarna och lätt att komma ihåg för dig. Det kan du få hjälp med på vår hemsida. Besök nedanstående adress för att läsa artikeln, där tre säkerhetsexperten ger goda råd:

www.pctidningen.se/password



När du ska låsa upp filerna anger du bara lösenordet du valde för den krypterade enheten och klickar på knappen OK.



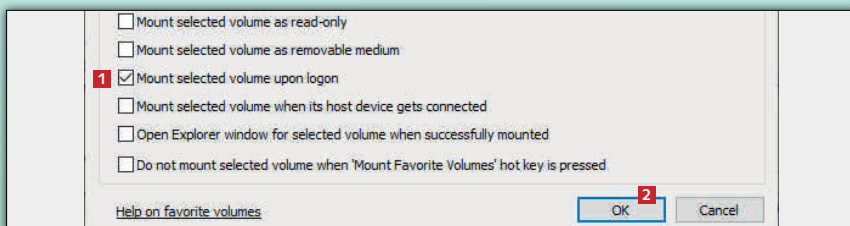
Kom igång med VeraCrypt

I Fördelszonen hittar du en utförlig guide till VeraCrypt som hjälper dig att komma igång med programmet. Leta reda på artikeln med guiden och hämta den som PDF-fil via adressen nedan.

www.pctidningen.se/0223

Gör det enklare att använda din enhet i vardagen

VeraCrypts krypterade enhet är bara synlig i Utforskaren när den har monterats – eller öppnats – med programmet. Du måste ange lösenordet för att låsa upp enheten även om den är synlig i Utforskaren, men om den inte är monterad med VeraCrypt är den inte ens synlig. Därför är det en bra idé att låta VeraCrypt automatiskt montera den krypterade enheten när Windows startar. I guiden här till höger kan du se hur du gör det i VeraCrypts inställningar.



1 I VeraCrypt måste du först montera din krypterade enhet. När du är klar klickar du på **Favorites** och väljer **Add Mounted Volume to Favorites...** på menyn. Markera sedan **Mount selected volume upon login** **1**, som det visas här, och klicka på **OK** **2**. Nu kommer enheten att monteras automatiskt när Windows startar.

Dra filer till säkerhet

I Utforskaren visas den krypterade enheten som om den vore vilken annan enhet som helst på datorn, till exempel ett anslutet USB-minne. Vanligtvis syns den krypterade enheten som en flyttbar enhet i översikten till vänster. Och precis som med ett flyttbart USB-minne eller en extern hårddisk kan du enkelt lägga till filer på den krypterade enheten. Dra bara över dem till enheten från en annan plats på hårddisken, så skapas en kopia av filen på den krypterade enheten. Efter det är det en bra idé att radera filen från den ursprungliga platsen på hårddisken, så att filen *bara* finns i säkerhet på den låsta enheten.



Klicka på den fil eller mapp ska läggas i den krypterade enheten, håll ned musknappen och dra sedan filen eller mappen till den krypterade enheten i Utforskaren. Då läggs filen i säkerhet bakom VeraCrypts kryptering.