1702 Säker på nätet & Lösenord

5 vägar till datorsäkerhet

- Ha alltid ett **aktiverat antivirusprogram** när du är uppkopplad till Internet. I de nyare versionerna av Windows finns det inbyggda *Defender*. Det kopplas bort, när man har ett annat antivirusprogram installerat. Det finns många program, både betalprogram och gratisprogram att välja på. En del är något bättre. Vilka varierar med tiden. Det Uppstår problem med alla ibland, men det brukar rättas till ganska snabbt. Välj ett du känner dig bekväm med. Personligen har jag bara *Defender*, och det verkar räcka för mig, som inte surfar på så riskabla sidor. Spel och porr bör man då undvika. Ställ in programmet så det uppdaterar sig automatiskt, minst ett par gånger i veckan. Man hittar Defender under *Inställningar, Uppdatering och säkerhet.* Man bör bara ha **ett** antivirusprogram installerat, för de kan arbeta mot varandra.
- Ha en **fungerande brandvägg**. Windows har en inbyggd. Säkerhetsprogrammen har säkert en, som man kan ställa in. Din router har troligen en. Din internetleverantör har kanske en. Men kan ha flera brandvägar, det gör inget, men är de för petiga, kan det ta tid att godkänna allt som vill in i datorn, även helt normala saker. Ställ in på en nivå du tycker är vettig. Även om det finns flera brandväggar på din uppkoppling, skall man alltid ha en i själva datorn. Håll **alla program uppdaterade**. Ställ in Windows på automatisk uppdatering och uppdatera program du använder ofta så fort du får en uppmaning. Uppdateringar handlar oftast om att täppa till nyupptäckta säkerhetshål.
- **Var förnuftig** på webben och klicka inte på knappar och länkar utan att veta vart de leder. I bästa fall kanske du binder dig för att köpa något du inte vill ha, i värsta fall hamnar du på en sida, som installerar ett farligt program på den dator och kapar den. Och öppna aldrig bifogade filer eller länkar från mejl, där du inte känner avsändaren.
- **Säkerhetskopiera** allt du inte vill bli av med. Det finns bra program som gör det automatiskt åt dig, men de kan också kopiera de fel du gör och ofrivilliga raderingar, så se upp lite. I Windows 10 finns en bra funktion, så du kan gå tillbaka i filhistoriken.

5 goda skäl för att ta back-up (säkerhetskopiera).

- En dator är en maskin som nöts. Förr eller senare går något sönder. En hårddisk beräknas hålla i genomsnitt 4 år. Mer om man använder den mindre såklart. Men en alldeles ny disk *kan* också krascha. Det går ofta att rädda filer från en trasig hårddisk, men det kostar pengar, och allt kanske inte går att rädda. Även om det inte är hårddisken det blir fel på, försvinner alla filer vid en ominstallation. Då går det att rädda filerna först, men det kostar.
- Ett program kan också få fnatt och förstöra det man håller på med.
- Datorn kan försvinna. Bli stulen eller brinna upp eller drunkna eller bli glömd någonstans.
- Du bär dig klantigt åt och förstör eller raderar något du vill ha kvar.
- Du vill komma åt ditt dokument, när du inte har din dator till hands.

Säker back-up. En kopia på samma dator är en dålig säkerhet, även om det är på en egen partion av hårddisken eller en annan intern hårddisk. Välj andra alternativ!

- Att bränna på en skiva är ett dyrbart alternativ, som börjar bli omodernt, då det inte är lika vanligt men skivspelare i datorerna. Dessutom är skivorna hållbarhet osäker.
- Usb-minnen och minneskort fungerar, men kan vara svåra att hålla reda på. De blir lätt många och är väldigt små. Man måste ha ett system för att förvara dem
- En annan dator går förstås bra. Bara man har ett enkelt sätt att föra över filerna.
- En nätverkshårddisk är egentligen en dator, som alla datorer i ett nätverk kan komma åt. Har man flera datorer och ett hemmanätverk är det ett bra alternativ. Man kan även nå den via Internet, om man inte är hemma. (och den är på)
- En extern hårddisk är ett utmärkt och ganska billigt sätt. Men förvara den helst inte intill datorn hela tiden, då kan den utsättas för brand eller stöld på samma gång som datorn.
- Molnlagring på ett etablerat ställe är mycket säkert, på så sätt att risken för att de skulle slarva bort dina filer är extremt liten. Dessutom kan du nå dem från vilken dator som helst, om du loggar in med ditt (säkra) lösenord. Däremot kan det finnas risk för att de blir hackade och lästa och kommer i orätta händer. *Mycket* känslig information bör man kanske inte lägga upp, men vanliga privata bilder och dokument är inte intressanta för hackare. Numera kan man få stora lagringsutrymmen gratis, och vill man betala lite finns hur mycket som helst.

Jag rekommenderaratt man skall ha sina filer på minst 2, helst 3 ställen. Förutom i datorn t.ex. i molnet och på en extern fysisk enhet. Radera aldrig från kamerans minneskort utan att ha bilderna på två oberoende ställen. Glöm inte att bilderna i telefonen också behöver kopieras. Jag vet många som förlorat massor av bilder när telefonen tappas bort eller går sönder.

SeniorNet Uppsala februari 2017 Birgitta Avholm

Lösenord

Vad ska man ha för lösenord?
Det ska vara lätt att komma ihåg.
Det ska vara svårt för någon annan att komma på.

Ett bra lösenord:
- ska vara omöjligt att hitta i en uppslagsbok eller lexikon.
- ska inkludera specialtecken (# * ¤ $ €) och siffror.
- ska ha stora och små bokstäver.
- ska ha minst tolv tecken.

- ska inte vara baserat på aktuella data,
t.ex. personnummer, postkod, telefonnummer, osv.

Lösenordshanterare:
En lösning kan vara att använda en Lösenordshanterare – ett program eller tillbehör i din webbläsare som kommer ihåg alla dina lösenord.
När du startar datorn, loggar du in i lösenordshanteraren med ett ”master” lösenord och sedan när du öppnar ett program som kräver ett lösenord, då hoppar lösenordshanteraren in och fyller i alla uppgifter som behövs.
Naturligtvis, måste det master-lösenord du väljer uppfylla alla krav på ett bra lösenord.
Alla dina lösenord sparas på ett säkert sätt (krypterat), antingen på hårddisken eller på en molntjänst, t.ex. DropBox eller OneDrive.
Om lösenordsdatan sparas på hårddisken är det viktigt att du har en ”back-up” någon annanstans ifall någonting händer hårddisken.
Om datan sparas på en molntjänst, måste du vara uppkopplad till internet för att använda lösenordshanteraren.

Kom ihåg!
Det är helt möjligt att uppfylla alla krav för bra lösenord och fortfarande kunna komma ihåg dem.
Ett två-komponents-lösenord kan vara svaret. Vi har alla en enkel kombination av siffror och bokstäver som vi lätt kan komma ihåg. Det kan vara registreringsnummer på pappas bil eller telefonnummer som du kommer ihåg från barndomen. Den kombinationen kan du använda som en komponent i dina lösenord.
Den andra komponenten ska vara kopplad till namnet på konton eller programmet som lösenordet tillhör. T.ex. vi kan ta första tre eller fyra bokstäverna i namnet, eller första två och sista två bokstäverna.
Sedan kan vi lägga till några specialtecken för att avskilja delarna i lösenordet.

Här kommer några exempel:
Vi kombinerar ett bilnummer och namnet till lösenordet vi använder vid Googlekontot
go#BNM135#og eller BNM135&goog
Till Tele2-kontot kan det bli: tele*BNM135 eller te¤BNM135¤e2 eller BNM135&tee2
Så länge du använder samma metod varje gång, då behöver vi inte skriva ner alla lösenord. Du kan även sätta upp en lapp på datorn med ett mall för den kombination du har valt.
aaöö#BIL betyder första två och sista två bokstäverna i kontonamnet följd av en fyrkant och sedan bilnumret.

Det finns många gratis Lösenordshanterare på nättet:

1Password
Passwordsafe
Passwordmanager
KeePass
LastPass
PasswordBox

SeniorNet Uppsala februari 2017 Harley Thomas