Hot och säkerhet på datorn

Inre hot kan man kalla det som kan hända utan påverkan från Internet. Oftast handlar det om att man blir av med sina sparade dokument och bilder. Det kan finnas flera olika orsaker.

- **Hårdvarufel.** En dator är en maskin, som har många delar som kan gå sönder. Förr eller senare händer det. Är hårddisken oskadd, är det ganska enkelt att koppla den till en annan dator och få fram alla sina filer. Är det hårddisken som är trasig, vilket är det vanligaste, är det svårare, och kostar pengar, men ofta kan man rädda en del.
- **Mjukvarufel**, alltså program som bär sig tokigt åt. Det påverkar oftast bara det man håller på med, men det kan vara väldigt irriterande. Den första åtgärden är att starta om datorn, och då brukar det lösa sig. Ibland måste man ominstallera, och det kan bli krångligt. Man kan behöva hjälp.
- **Datorn försvinner**. Den blir stulen eller man tappar bort den eller huset brinner upp. Det kan man inte göra något åt efteråt, men då är man glad att ha en back-up.
- **Egen klantighet**. Det händer tyvärr inte så sällan. Man får göra vad man kan för att rätta till. Raderar man en vanlig fil är det inte så farligt, men har man gått in och gjort något i operativsystemet, kan det vara svårt. Man måste tänka sig för innan.

Det bästa skyddet är att **säkerhetskopiera** allt man inte vill bli av med. Det finns många sätt. Mer om det senare.

Yttre hot är det man kan råka ut för via Internet. Här handlar det inte bara om att förlora filer, man kan bli lurad och bestulen och utnyttjad på olika sätt.

- **Virus** är ett gammalt, men tyvärr fortfarande aktuellt elände. Det är program, som nästlar sig in i datorn och gör skada på olika sätt. Det kan förstöra datorn eller använda din uppkoppling och kosta dig mycket. Att ha ett bra och uppdaterat **Antivirusprogram** är ett ganska säkert skydd. Man bör bara ha ett AV-program installerat, men det går att söka igenom datorn med program från webben, om man misstänker intrång. Det är också viktigt är att bete sig förnuftigt så man inte släpper in viruset själv.
- **Hackare** försöker ta sig in i datorn och leta reda på känsliga uppgifter eller ta över den för egna ändamål. En bra **brandvägg** skyddar datorn. Man får själv ställa in skyddsnivån, så den inte frågar om för vanliga saker hela tiden. Man kan ha flera brandväggar i bruk.
- **Nätfiske** är när du via ett mejl, som kan se ut att komma från din bank eller någon du känner, luras att ange ditt kontonummer eller inloggningsuppgifter. Det kan också vara ett meddelande om ett arv, eller en lotterivinst. Tro aldrig på sådant. Och är det något som du faktiskt tror är möjligt, kontrollera varifrån mejlet kommer genom att peka på avsändaren. Det finns också program, som varnar i webbläsaren.
- **Kidnappning** av dina filer med låsning och krav på lösensumma. Detta kommer huvudsakligen in via länkar man luras klicka på i mejl eller på webbsidor. **Var förnuftig. Polisanmäl** om du i alla fall drabbas. **Betala inte.** Kanske kan du låsa upp dina filer med en nyckel, men risken är stor att det inte går eller att du blir kidnappad igen av samma program. **Ha säker back-up** så du kan radera alla kapade filer. Det finns program som kan hjälpa.
- **Säkerhetshål eller buggar** i program är vägar in i datorn för olika slag av skadlig kod. Alla programutvecklare arbetar med att komma ikapp eller ligga före nätbovarna. Det är oftast därför det kommer nya uppdateringar. därför skall du alltid **Uppdatera** program du använder. De du *inte* använder bör du avinstallera.

- **Kapning av konton,** mejl eller sociala medier, kan användas för att lura andra på olika sätt. **Bra lösenord** är viktigt och **säkerhetsinställningar** minskar risken.

Personliga hot kan vara trakasserier på sociala medier med spridning av uppgifter, sanna eller osanna, som leder till hat och hotelser. Det kan också vara utpressning. Någon utomstående kan vittja din fysiska brevlåda för att komma åt uppgifter. Sätt lås på den! Var uppmärksam och dra dig inte för att polisanmäla!

Så här skyddar du dig och din dator:

- **Antivirusprogram** aktiverat och uppdaterat.
- **Brandvägg** i datorn och gärna också i nätverket, lagom inställd.
- **Säker back-up.** Helst på flera ställen.
- **Uppdatera** alla program du använder.
- **Bra lösenord.**
- **Kontrollera säkerhetsinställningar** i datorn, i webbläsaren, på sociala medier**.**
- **VAR FÖRNUFTIG!**

Säkerhetskopiering

En kopia på samma dator är en dålig säkerhet, även om det är på en egen del av hårddisken eller en annan intern hårddisk. I program som skapar back-up automatiskt, måste men kontrollera var kopian sparas.

Hur och var?

- Att bränna på en skiva är dyrt, krångligt, omodernt och är kanske inte så hållbart.
- Usb-minnen och minneskort fungerar, men kan vara svåra att hålla reda på, då de är så små. Man måste ha ett system för att förvara dem och hitta innehållet.
- En annan dator går förstås bra. Bara man har ett enkelt sätt att föra över filerna.
- En extern hårddisk är ett utmärkt och ganska billigt sätt. Men förvara den helst inte intill datorn, då kan den utsättas för brand eller stöld på samma gång som den.
- Molnlagring på en etablerad tjänst är mycket säkert på så sätt att risken att förlora filerna är extremt liten. Däremot kan det finnas en liten risk för att de blir hackade och kommer i orätta händer.
  Man kan synkronisera sina mappar i molnet med flera datorer. Det är praktiskt, då man har uppdaterade filer på alla sina enheter. Det kan tyvärr även vara en risk, om man får sina filer kidnappade och låsta. Men det finns oftast möjlighet att gå tillbaka till en tidigare version.
  Det finns många olika tjänster, som har en del gratis utrymme, men behöver man mycket får man betala för det. OneDrive, Google Drive, Dropbox är de mest kända och innehåller olika tjänster förutom lagring.

Jag rekommenderar att man har sina filer på minst 2, helst 3 ställen, förutom i datorn. Varje gång du sparar en fil, kopiera den till molnet. Med jämna mellanrum, t.ex. en gång i vecken för också över till en extern fysisk enhet, som du förvarar på en annan plats än hemma.

Den enda säkra back-upen är den som verkligen blir av!!

Checklista för datorsäkerhet.

- Gå igenom alla inställningar på dina program, speciellt FaceBook och Google.
- Tänk efter innan du lägger ut bilder och information på sociala medier.
- Spärra obehöriga adressändringar hos **skatteverket.se** och **adressändring.se**
- Säkerhetskopiera (Back-up) regelbundet! Det finns program som kan hjälpa till. Sökord: ”***back up program***”.
- Brandvägg – kolla i säkerhetsinställningar att den är påslagen.
- Antivirusprogram. Sökord: ”***antivirus”, ”bäst antivirus”, ”gratis antivirus”.***
- Uppdatering av operativsystemet (Windows, Apple IOS, Android).
- Uppdatering av program. Kolla regelbundet efter nya uppdateringar.
- Installera ett antimalware-tillägg i din webbläsare. Sökord: ”***malwarebytes browser guard***”.
- Kolla adress till alla länkar på webbsidor innan du klickar på dem.
- Använd webbsidan ”***virustotal.com***” för att kolla webbadresser och datorfiler.
- Lösenord: om du inte har ett bra system för att ha individuella lösenord för varje konto, då ska du använda ett lösenordshanterare-program. Sökord: ”***lösenordshanterare***”.

Epost säkerhet:

- Kolla avsändaradressen. Använd Google för att kolla avsändaren.
- Var speciellt uppmärksam om någon frågar efter pengar, kontonummer, lösenord eller dylikt.
- Är din epostleverantör pålitlig? Kolla med Google.
- Öppna ej bifogade filer eller länkar om du inte är 100% säker. Kolla med ”***virustotal.com***”.
- Använd helst **Hemlig kopia** (Bcc) istället för **Kopia** (Cc).
- Kolla att **Ämnesraden** stämmer innan du använder **Svara** eller **Svara alla**.
- Var kritisk! Är det sant?
- Använd sunt förnuft