Säker på nätet

Idag sker mycket i våra liv via olika tjänster på Internet. Vi kommunicerar och umgås. Vi handlar och betalar. Vi konsumerar kultur. Vi hittar platser och annan information. Ja, vi blir mer och mer beroende av att våra uppkopplade apparater fungerar.

Men när IT växer på alla områden, så blir det naturligtvis också ett mål för kriminella, som kan tjäna på det. Vi hör ofta om bedrägerier och intrång på olika sätt.

Vi måste lära oss var hoten finns och hur vi skyddar oss mot dem. Idag skall vi försöka reda ut hur vi enklast skall klara av det.

Många av oss använder flera *enheter* i vårt uppkopplade liv. **Telefonen,**som är med oss överallt. **Surfplattan** när vi skall läsa och googla hemma. **Datorn** när vi skall skriva, redigera foton eller göra annat, som kräver mera kraftiga program och större skärm. Men i princip spelar det ingen roll vad du använder. Hoten och hjälpen mot dem är desamma.

Inre hot, d.v.s**.** det som kan hända utan att man är uppkopplad. Oftast handlar det om att man blir av med sina sparade dokument och bilder. Det finns flera olika hot.

- **Hårdvarufel.** En IT-enhet är en maskin, som har många delar som kan gå sönder. Förr eller senare händer det. Är lagringsenheten oskadd, kan man ganska enkelt koppla den till en annan enhet och få fram alla sina filer. Är det hårddisken, som är trasig, vilket är det vanligaste på en dator, är det svårare, och kostar pengar, men ofta kan man rädda en del.
- **Mjukvarufel**, alltså program eller appar som bär sig tokigt åt. Gäller det operativsystemet, som styr själva apparaten, är det svårt att göra något själv. Men ofta är det en app som hängt sig och då påverkas bara det man håller på med. Det kan vara väldigt irriterande. Den första åtgärden är att stänga programmet, öppna det igen och då kan man återställa det man höll på med. Hjälper inte det, kan man starta om datorn, och då brukar det lösa sig. Man kan behöva hjälp ibland. Det man höll på med kanske har försvunnit. Att spara då och då när man jobbar med ett dokument är bra.
- **Enheten försvinner**. Den blir borttappad eller stulen, 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. Det är lätt att trycka på fel knapp, eller tänka bakvänt. Man får göra vad man kan för att rätta till. Raderar man en vanlig fil år det inte så farligt, men har man gått in och gjort något längre in i systemet, kan det vara svårt. Man måste tänka sig för innan man rotar bland saker man inte riktigt vet vad det är.

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

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. Ofta är det en *skadlig kod,* som tagit sig in i datorn på något sätt.

- **Virus** är ett gammalt, men tyvärr fortfarande aktuellt elände. Det är program, som nästlar sig in i enheten och gör skada på olika sätt. Att ha ett bra och uppdaterat **Antivirusprogram** är ett nödvändigt och ganska säkert skydd. Man bör bara ha ett program installerat, men det går att söka igenom enheten med program från webben, om man misstänker intrång. I Windows finns numera ett inbyggt skydd.
- **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, och ofta finns det en i routern till hemmanätverket..

- **Nätfiske** är när man via ett mej, som kan se ut att komma från banken eller någon man 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. Öppna aldrig bifogade filer från någon du inte känner.
- **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 år stor att det inte går eller att du blir kidnappad igen av samma program. **Ha säker backup** så du kan radera alla kapade filer. Det finns program som kan hjälpa.
- **Säkerhetshål eller buggar** i program och appar är vägar in 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. Man skall alltid **Uppdatera** program man använder. De man *inte* använder bör man 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.

Så här skyddar du dig och dina enheter

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

^*^*^*^*^*^*

Vad är phishing och nätfiske?

Phishing eller nätfiske som det heter på svenska är ett sätt att ”fiska” efter personlig och känslig information som lösenord eller kortnummer. Phishing skickas som massutskick till flera användare på en och samma gång och ser ofta äkta ut med avsändarens företagslogotyp och adress. Därför är det många gånger svårt att bedöma om e-posten är en bluff eller inte.

Det finns flera olika typer av nätfiske. Det kan vara en e-post som ser ut att komma från en välkänd källa som ett företag, en bank eller organisation där du ska lämna ifrån dig personliga uppgifter. Andra e-post lockar med olika typer av erbjudande där du ska klicka på en länk i e-posten för att komma till erbjudandet. Syftet oavsett tillvägagångssätt är att komma över personlig information som till exempel användarnamn och lösenord, personnummer, kreditkortsnummer eller bankkontonummer som sedan kan användas för bedrägerier som att ta ut pengar från dina bankkonton, utnyttja dina krediter på kortet eller att ansöka om nya krediter i ditt namn.

Se upp med misstänkta e-post som:

- Ber dig att lämna ifrån dig kort- eller kontonummer.
- Ber dig lämna ifrån dig lösenord.
- Ber dig att klicka på okända länkar.
- Ber dig verifiera din kontoinformation.
- Hotar med att stänga ner ditt konto på kort tid.
- Lockar med osannolika erbjudanden.
- Innehåller dålig grammatik, stavning eller ordföljd.
- Innehåller konstiga rubriker eller icke-personligt tilltal i mailet.

Om du misstänker att en epost eller ett webb-medelande är falskt:
Kolla adressen! Är adressen från ett känt företag eller person? Om brevet kommer från Telia, t.ex., då ska namnet ”telia” figurera någonstans i adressen.
Kolla länkarna i brevet/meddelandet! Peka på länken utan att klicka, då kan man se längst ner till vänster var länken leder till. Även här ska företagets namn figurera. Om alla länkar i ett brev/meddelande leder till samma adress då är det definitivt ”spam”.

Du kan kolla en epost- eller länkadress på Google. Skriv upp adressen eller en fras från meddelandet. Öppna Google och skriv in adressen eller fras och Sök. Då kan du se vad andra har att säga, om den är bra eller dålig.

Kolla adressen! Kolla länkarna! Klicka inte!