Bluffmejl

Om du får ett mail som du är tveksam till, ska du vara försiktig med att öppna det. Du riskerar nämligen att drabbas av skadlig kod om du öppnar okända bilagor i e-post, surfar på internet eller importerar filer till din dator via olika media. Skadlig kod är ett samlingsbegrepp för det som kallas virus, trojaner och maskar. Ring och kontrollera med personen/organisationen som du tror har skickat mailet, om avsändaren stämmer.

Ofta kan dessa bluffmejl vara utformade som orderbekräftelser eller viktiga meddelanden som exempelvis uppger att du har beställt varor på nätet eller att du måste komplettera din deklaration eller hamnat i nöd och snabbt behöver pengar. Målet är att lura dig och få dig att öppna ev medföljande bilaga, vilket krävs för att datorn ska smittas. Att endast läsa mejlet utan att öppna bilagan smittar inte din dator.

Om du ändå öppnar bilagan finns det risk att datorn blir infekterad. Datorn kan sedan utnyttjas av bedragare till att stjäla information på datorn eller pengar från ditt bankkonto när du gör betalningar på din internetbank.

Varför mail kommer från din mailadress fast du inte själv har skickat dem

När man misstänker att ens mailadress har blivit kapad finns det 3 olika alternativ:

1. Din mailadress har blivit ”spoofad”
2. Din mailbox har blivit kapad
3. Du har fått virus i din dator

I de allra flesta fall så handlar det om alternativ ett (1), detta är det absolut vanligaste, 99% uppskattas det till. I alternativ två (2) har någon kommit över inloggningsinformationen till ditt mailkonto och använder det olagligt. Tag i så fall kontakt med din internetleverantör (eller systemansvarig). Alternativ 3 kan också förekomma och i så fall mailar din dator ut mail automatiskt. Tag kontakt med din datorleverantör för kontroll om datorn har virus.

1. Din mailadress har blivit ”spoofad”

Om din mailadress har blivit ”spoofad” som oftast är den troligaste orsaken, betyder det helt enkelt att någon skickar mail och anger en falsk mailadress som avsändare och med falsk menas det här att någon annan än dig. Spoof betyder i mailsammanhang förfalskning och ute på internet finns ingen direkt kontroll av mailtrafik och mailservrar så det står var och en fritt att i princip skriva in vilka mailadresser som helst. Bästa jämförelsen är om man tänker sig ett vanligt kuvert med en avsändare på baksidan, vem som helst kan ju skicka ett kuvert till vem som helst med posten och skriva vilken som helst avsändare på baksidan.

Men hur går det hela till egentligen?

Det är faktiskt ganska enkelt för en spammare att förfalska din e-postadress. De behöver inte ens få tillgång till ditt konto. Allt de behöver veta är din e-postadress! E-post är faktiskt ett väldigt sårbart kommunikationsverktyg. Det finns inget som hindrar någon från att skicka ut e-post där de låtsas vara någon annan. Så det enda spammaren behöver göra är att lägga in ett par kommandon i e-postmeddelandets huvud för att få det att se ut som att det har skickats från dig. På så vis kan de enkelt från vilken plats som helst, skicka ut vad som helst, utan att bli upptäckta.

Vad kan jag göra för att slippa detta?

Den olyckliga svaret på denna fråga är… inte så mycket. Falska e-postmeddelanden är otroligt svårt att spåra och även om du lyckas få reda på IP-adressen som ansvarar för att skicka ut skräppost och kontaktar den berörda leverantören för att få det blockerat, kan spammaren helt enkelt bara använda en annan IP-adress nästa gång och fortsätta använda din e-postadress.
Naturligtvis kan du radera ditt e-postkonto och börja om på nytt, men det är kanske inte något som du bara kan göra så där heller. Tragiskt nog brukar den bästa lösningen vara att bara låta det va och vänta ut tills spammaren valt att gå vidare och börjat utnyttja sitt nästa offer istället.

2. Din mailbox har blivit kapad

Det kan även ske att man får sin mailbox kapad, dvs att någon har kommit över inloggningsinformationen till ditt mailkonto och använder det olagligt. Om detta sker så är det bästa alternativet att direkt logga in i kontrollpanelen och bytta ut ert lösenord till ett nytt.

Kapad adressbok

Är mailboxen kapad blir också din adressbok kapad vilket innebär att kaparen kan skicka ut konstiga mejl från dig till alla du har i adressboken. Mejladresserna kan kaparen sälja på internet vilket kan medföra att du kan få konstiga mail långt efter det att lösenordet är bytt eller du skaffat dig en ny mailkonto.

3. Du har fått virus i din dator

Om du har fått virus i din dator så kan det förekomma att detta gör att mail skickas ut från din dator automatiskt. Rekommenderat är att göra en virus scanning och om detta ej hjälper ta kontakt med din datorleverantör eller systemansvarige för för hjälp.

Varför vill någon skicka mail från min adress?

Också detta har ett ganska enkelt svar. Om man vill skicka mail till någon och skickar från en mailadress som är äkta så är chansen mycket större att det kommer fram till mottagaren. Den typen av mail som skickas på detta sättet kallas ju ofta för SPAM eller skräppost. Det finns en stor marknad där man kan tjäna pengar på SPAM. Antingen genom att sälja produkter som finns, sälja produkter som inte finns, bedrägeri, eller genom att sälja äkta mailadresser till andra som i sin tur säljer produkter. Om man skickar erbjudanden till svenska personer från en äkta svensk mailadress kommer detta att gå bättre än om man hittar på någon på måfå. Ibland kan man till och med få mail från ”sig själv”.

Om du har blivit drabbad

Om din dator har blivit infekterad av skadlig kod bör du göra en ominstallation för att vara helt säker på att den är fri från skadlig kod. Eventuellt kan det antivirusprogram som du använder klara av att rensa bort infektionen.

Har din adressbok använts för att skicka mejl så tyder det på ett hackat konto eller att du fått virus i datorn. Kanske har personer du känner hört av sig och undrat vad det är som händer.

Om ditt mailkonto blivit kapat byt till nytt mailkonto.