Säkerhet.

Innehåll.

ALLMÄNT.

Internet

Jag vill påtala att när man är ute och surfar på internet ska man ha i åtanke att det förekommer en hel del fula saker där.Till exempel bedrägerier.

Man behöver inte vara särskilt rädd men man ska iaktaga normal försiktighet. Framför allt, var inte naiv och tro på allt som sägs och görs på internet. Det finns en hel del fula fiskar som på olika sätt försöker komma åt dina pengar.
Ett vanligt bedrägeriförsök är att be om kontouppgifter och koder till ditt bankkonto.
Bedrägeriförsöken görs med olika förklaringar om varför man vill ha dina kontouppgifter.
Men ingen bank begär dessa uppgifter, varken via internet, telefon eller per post/e-mail!

Klicka inte **OK** i rutor som uppmanar till olika erbjudanden. Ingen ger dig några pengar gratis!
Gå inte till adresser/sidor som du erbjuds och inte själv valt.

Din dator

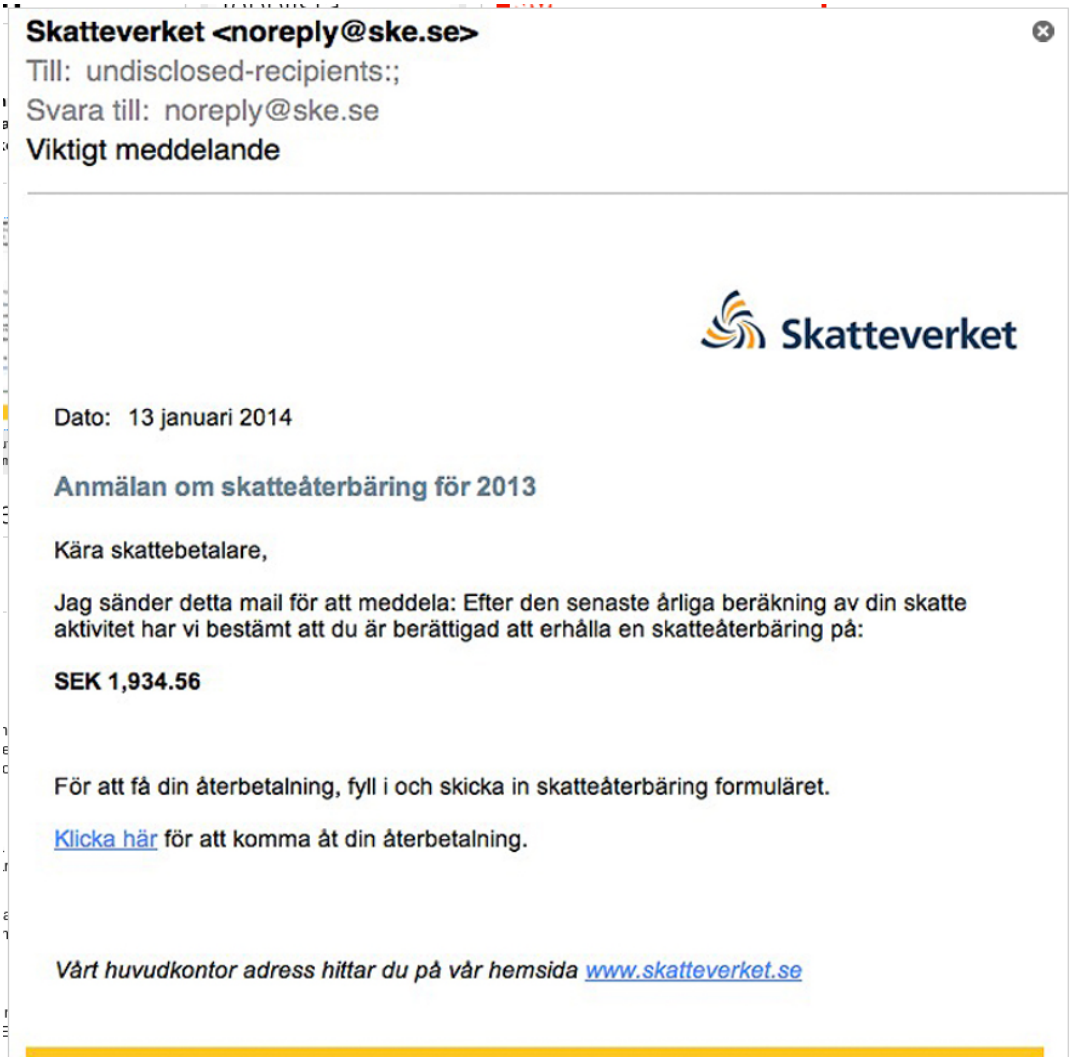
På sidan Backup nedan kan du läsa om hur du skyddar din information.

Nigeriabrev

På wikimedia kan du läsa om Nigeriabrev som är en form av bedrägeri.
Även andra likartade bedrägerier där man försöker locka av datoranvändare uppgifter av olika slag kallas ofta för **Nigeriabrev**.

Bluffmail.

Exempel på bluffmail. I detta fall utger sig avsändaren att var Skatteverket.



Skatteverket <noreply@ske.se>
Till: undisclosed-recipients:;
Svara till: noreply@ske.se
Viktigt meddelande

Skatteverket

Dato: 13 januari 2014

Anmälan om skatteåterbäring för 2013

Kära skattebetalare,

Jag sänder detta mail för att meddela: Efter den senaste årliga beräkning av din skatte aktivitet har vi bestämt att du är berättigad att erhålla en skatteåterbäring på:

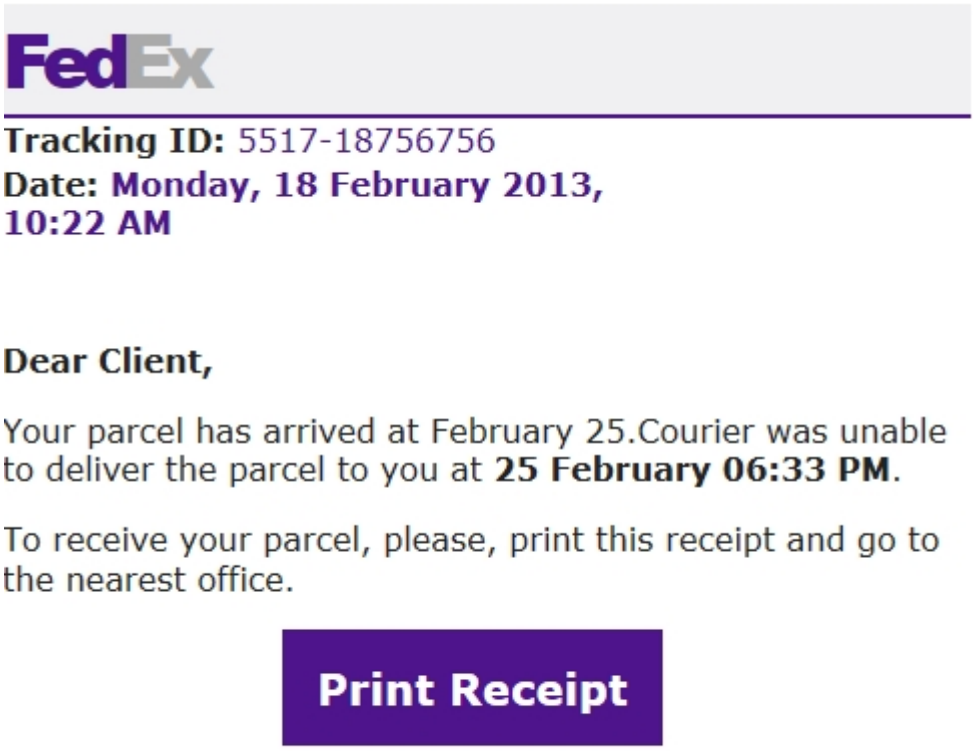
SEK 1,934.56

För att få din återbetalning, fyll i och skicka in skatteåterbäring formuläret.

Klicka här för att komma åt din återbetalning.

Vårt huvudkontor adress hittar du på vår hemsida www.skatteverket.se

Man kan få mail som uppger sig komma från FedEx t ex



Ett paket sägs inte ha kunnat levereras och man ska luras att klicka på en ruta för att skriva ut ett kvitto, men det är det givetvis inte utan i stället kommer ett elakt program att startas.

Elakheter.

De flesta elakheter på nätet attackerar Internet explorer, som finns i versionerna 8, 9, 10, 11. Alla innehåller säkerhetsluckor som man försöker utnyttja. Många sådan säkerhetsluckor har rättats av Microsoft, men det upptäcks ständigt nya som inte hinner åtgärdas innan de börjar utnyttjas. Ett bra skydd är att byta till att använda alternativa webbläsare t ex Chrome, Firefox, Opera m fl. Säkerhetsluckorna i en webbläsare utnyttjas när man surfar till en webbsida som blivit ”hackad”, så att skadlig kod kunnat läggas in på sidan.
Många attacker har som mål att kapa datorer för att använda internetkopplingen utan att användaren vet om det. En s k Trojan (efter trojansk häst) aktiveras på distans för att göra attacker mot myndighetssajter eller liknande. Man kan då få sin internetkoppling blockerad av internetleverantören som ”straff”.

Microsoftsamtal.

Det förekommer inte så sällan att man får ett telefonsamtal från en person, som talar dålig engelska, som utger sig vara från Microsoft. Vederbörande påstår att du fått in farligt program i din dator och han vill hjälpa dig att få bort det. Han vill att du ska ladda ner ett program så att han kan komma in i din dator och rensa bort det farliga programmet.

Ofta är vederbörande ganska påstridig och inte sällan återkommer samtalet ett flertal gånger. Lägg på telefon direkt när vederbörande presenterat sig. Det händer att han frågar om du pratar engelska svara då NO.

Windows XP

Den 18 april 2014 slutar Microsoft att supporta Windows XP. Det innebär bland annat att inga uppdateringar med rättninga av fel kommer att distribueras. Detta i sin tur innebär att kriminella kommer att kasta sig över XP. Användare av XP kommer att bli utan skydd mot skadliga angrepp utifrån.

Okänd avsändare

Ifall du får e-majl från en avsändare du inte känner igen kan du kontrollera från vilket land mejlet kommer.
Alla e-mejl adresser avslutas med hänvisning till en så kallad toppdomän, för Sverige är toppdomänen **.se** (punkt se).
Vad du än gör, ÖPPNA ALDRIG MAILET.

Utpressning

Exempel 1:

Ett mail som utger sig för att komma från polisen berättar att man besökt pornografiska/barnpornografiska sidor. Även om man är oskyldig så vill man inte få ett falskt ryckte om sig att man är ”sån”. Då betalar man de 300$/2100skr som begärs.

Exempel 2:

Genom att man klickat på någon sida och fått in ett virus så har viruset krypterat hårddisken med alla familjebilder mm. Krypteringen gör att man inte kommer åt något av innehållet. Då blir man erbjuden dekryptering mot att man betalar 300$.

Sociala medier

Det förekommer att folk ger sig ut för att ha oförskylt hamnat i en situation med behov av pengar.

Man utger sig för att vara ett barnbarn som blivit rånad i ett främmande land och inte kan ta sig hem. Man ber om pengar till biljett hem.

Man påstår att man själv eller ens barn drabbats av en svår sjukdom som behöver en operation som kostar väldigt mycket, samt att man inte på några villkor har möjlighet att bekosta själv. Så dår ber man om bidrag till operationen.

Detta bör Ni polisanmäla om ni råkar ut för det.

- - - - - - - - - - - - - - - - - - -

HANDLA PÅ INTERNET.

Några tips om vad man bör tänka på.

För det första anser jag att man inte behöver vara rädd för att handla på internet. Men man ska vara försiktig och tänka sig för.

Om du handlar från svenska företag brukar de flesta erbjuda leverans mot postförskott vilket gör att du slipper hantera kreditkort på Internet. Men var observant på vem du handlar av. De stora etablerade postorderkjedjorna kan man nog lita på vad gäller att man beställt och att man kan reklamera mm. En del företag som till exempel Adlibris levererar mot faktura om du handlar för mindre belopp. När det gäller mindre företag och framförallt företag du inte känner så var försiktig.

Blocket, Tradera och liknande ställen manar till extra försiktighet. Dels förekommer det tydligen en hel del stöldgods, dels rena bedrägerier, typ att man skickar en träbit i stället för mobiltelefonen som utlovats.

Det förekommer bedrägerier på internet precis som i verkliga livet. Ni kanske kommer ihåg annonserna att man kunde få en förstoring för 75 x 50 för någon hundralapp. När bilden sedan kom visade det sig att bilden var 75 x 50 **mm** och inte 75 x 50 cm som man trodde. I annonsen stod det inte vilket mått som gällde, mm eller cm.

Här skulle jag råda den som vill handla att när köpet görs så bör man träffas öga mot öga så man ser vad som levereras.

När du handlar från utländska företag får man vara lite mer försiktig. Dessa kräver ofta förskottsbetalning eller betalning med kreditkort. Själv skaffade jag mig ett ”riktigt” kreditkort med begränsad kredit. Detta gör att en bedragare bara kan själa ”små” belopp. Jag har dock inte råkat ut för någon bedragare. **Än!** Och jag har handlat på internet i över 15 år. Vissa banker, bland annat Nordea, erbjuder möjligheten att skapa ett engångskreditkort. Detta hindrar någon att ”fånga” upp kreditkortsnumret och sedan använda det flera gånger eller på annat håll. Företaget Pricerunner har infört en trygghetsmärkning.

Var försiktig och tänk efter före!

LÖSENORD.

Lite grand av vad man bör tänka på när det gäller användandet av lösenord/password.

1. Välj ett ord som är svårt att gissa. Ordet bör vara minst 6-8 tecken långt. En del hävdar att man ska ha minst 16 tecken i lösenordet. Lösenordet bör innehålla en blandning av bokstäver, stora och små, och siffror och specialtecken såsom utropstecken (!), parantes(}) eller procenttecken (%).

2. Undvik ord som är lätta att koppla till dig som person. Till exempel barnens namn, kattens/hundens namn, släktingars namn, bilnummer, personnummer och framför allt inte typ 1234567.

3. Använd inte samma lösenord på flera ställen. Bedöm hur viktig just det stället är för dig. Fundera över hur det skulle drabba dig om lösenordet kom på avvägar.

4. Byt lösenord varje månad. Men gör det inte enkelt för dig genom att lägga till eller ändra en siffra i nummerordning.

5. Skriv inte ner lösenordet på en lapp och lägg under tangentbordet.

6. Lämna inte ut lösenordet till någon annan. Och framför allt **ALDRIG** via internet/webben, inte ens i ett nödläge. Ifall du i ett nödläge måste göra det så byt lösenordet med det snaraste efteråt.

Fundera lite över detta:
Du kan aldrig veta på vilket sätt en webbplats lagrar ditt lösenord. En del kanske lagrar det i klartext i en fil. Andra kanske lagrar lösenordet på samma dator som webbsida finns. Dessa saker underlättar för hackare att komma åt ditt lösenord.
Ska jag lägga upp personliga uppgifter på internet?

”Bedragaren är alltid smartare än du”

HEMMANÄTVERK.

När du skaffar dig ett trådlöst nätverk hemma får du inte glömma att ställa in lösenord på den trådlösa routern för att ansluta till nätverket. IDGs Techword meddelar att många svenskar med router från Asus är öppna för åtkomst från internet.

Det är sannolikt ganska vanligt att den som är ovan vid lokala nätverk glömmer att ställa om lösenordet som är inställt från fabrik.

Inställningar av en router beskrivs på http://www.pihlgren.se/Forelasningar/HemmaLan2.pdf

Det är mycket viktigt att man byter ut lösenordet som levereras med från fabrik.

Vidare ska man se till att skydda sitt nätverk mot obehörig åtkomst så man ska sätta ett svårt lösenord (se ovanstående länk) för att kunna använda nätverket .

VIRUS OCH BRANDVÄGG.

Begrepp.

- Skadlig kod/malware
- Virus(datorvirus/datavirus)
- Trojan
- Mask/Worm
- Spionprogram/Spyware
- Annonsprogram/Adware
- Keylogger
- Rootkit
- Brandvägg:
  Inom datateknik är en brandvägg en dedikerad dator (s.k. hårdvarubrandvägg) eller en programvara som kan installeras i en generell dator (s.k. mjukvarubrandvägg) i syfte att avvärja dataintrång på nätverksanslutna datorer.
  Källa: Wikipedia.

Datorvirus eller datavirus är små datorprogram som sprider sig genom att lägga en kopia av sig själva inuti andra program, värdprogram, på sådant sätt att koden körs då värdprogrammet körs. Då ett infekterat värdprogram körs kan dess virus spridas ytterligare och även utföra annat som viruset har konstruerats för att göra. I dagligt tal kallar man ofta alla typer av skadlig programkod för virus.

En trojansk häst eller trojan är ett datorprogram som utger sig för att vara till nytta eller nöje, men som orsakar skada när det lurat en användare att installera eller köra det. Det kan vara frågan om ett program skrivet för ändamålet eller en modifierad version av ett annat program.

Ett rootkit eller spökprogram är en uppsättning program eller modifikationer på datorprogram som döljer saker för användare och administratörer genom att modifiera systemets funktion. I allmänhet används ett rootkit i samband med dataintrång eller av malware för att dölja annan otillåten aktivitet. Namnet kommer av administratorskontot "root" på Unix-system.

Källa: Wikipedia

Brandvägg.

Man behöver ha en ”brandvägg” som stoppar all utgående trafik man inte själv godkänt – brandväggen kommer ihåg externa kopplingar som man godkänt, men när ett program uppdaterats kräver brandväggen att man auktoriserar det igen.
Om datorn börjar gå trögt och uppföra sig underligt kan det vara värt att göra en virusskanning. Även om man har ett bra anti-virusprogram i datorn är det inte säkert att det upptäcker alla virusattacker.

Om datorn börjar gå trögt och uppföra sig underligt kan det vara värt att göra en virusskanning. Även om man har ett bra anti-virusprogram i datorn är det inte säkert att det upptäcker alla virusattacker. Det finns alternativ som på internet, som man kan ladda ner och använda för en extra sökning

UPPDATERA.

För att hålla sitt datorsystem "up to date", så fritt från fel som möjligt samt ta del av nyheter bör man med jämna mellanrum uppdatera det.
Vi ska skilja på Uppdatera och Uppgradera.
Uppgradera innebär att man får en ny version av programmet. Till exempel: Windows 7 till Windows 8.
Uppdatera innebär att man får rättelser till sin befintliga version av programmet.

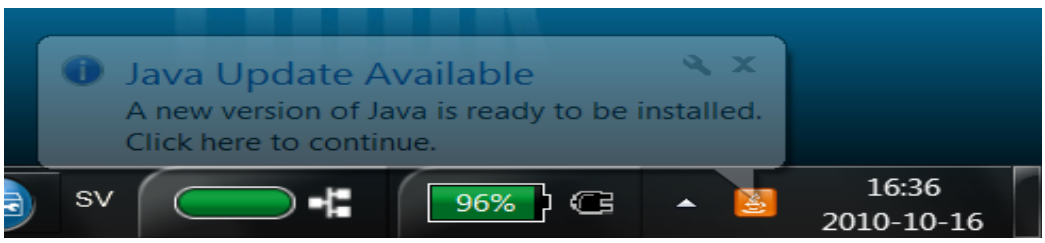
Flera program meddelar när det finns uppdateringar att installera och då bör man så snart det passar installera uppdateringen.
När man godkännt att starta uppdateringen kan man ofta lämna datorn tills uppdateringen är klar.
Ofta ingår det att datorn ska starts om när uppdateringen är klar.

Microsoft skickar normalat ut sina uppdateringar den andra (2:a) tisdagen i månaden.
Övriga tillverkare skickar för det mesta ut sina uppdateringar när det är aktuellt.

Ställ in så att uppdateringar görs automatiskt så att kända säkerhetsluckor ,som inkräktare skulle kunna utnyttja, täpps till snarast.

En sådan här symbol kommer upp när det finns en uppdatering till Windows:

Så här ser det ut när det kommit en uppdatering till Java.



BACKUP

Someday, your operating system will automatically backup your data to a secure remote data-center deep below the Himalayas. But right now, you're simply on your own. ***Backup software*** *is like antivirus software -- we wish it wasn't necessary but it is. Well, the good news is that backup may be a chore but it no longer has to be expensive."*

En dag kommer ditt operativsystem att automatiskt backa upp dina data till en säker plats djupt under Himalayas berg. Men just nu måste du sköta det själv. Backup program liknar antivirusprogram - vi önskar att de inte vore nödvändiga men det är dom. Den glada nyheten är att backup kanske kräver lite arbete men inte längre behöver vara dyr.

"Three quick tips for using freeware backup effectively.

1. ***Backup to a second drive****. NOT a second partition on the same drive!! Data loss is very often caused by disk failure. This alone will dramatically increase your data security.*
2. ***Shut down Outlook at night****. Backup software often cannot access Outlook database files while the program is running. Shut it down at night so that your email can be safely archived while you sleep. (This is not necessary if you have "File Access Manager")*
3. ***Archive backup data to DVD periodically****. Write your entire backup archive to DVD or DVD-RW every week or two and store the disk at a remote location. You'll thank me later!"*

Tre snabba tips att effektivt göra backup.

1. **Gör backup till en annan hårddisk eller USB-minne**.
   Gör inte backupen till en annan partition(del) på samma hårddisk. Dataförlust orsakas ofta av en förstörd hårddisk. Bara detta kommer att dramatiskt öka din datasäkerhet.
2. **Stäng ner Outlook nattetid**.
   Backupprogram kan inte komma åt Outlooks databasfiler när programmet körs. Avsluta programmet nattetid så att dina email säkert kan arkiveras medan du sover. (Detta är inte nödvändigt om du använder "File Access Manager").
3. **Arkivera backupdata till DVD med jämna mellanrum**.
   Kopiera dina backuper till DVD eller DVD-RW varje vecka och spara skivan på annan plats. Senare kommer du att tacka mig.

För den som behärskar engelska finns mer att läsa här: http://free-backup.info/

Ni hanske har hört talas om att vi är åtminstone två sycken i föreningen som drabbats av haveri på våra hårddiskar. Och ingen av oss hade någon backup vilket fick till följd att vi förlorade en del data/information. Bägge förlorade vi våra e-mailadresser. Så vi kan båda två intyga vikten av att ha backup på sina data. Man behöver ju inte ta backup på allt, hela hårddsiken. Detta skulle kräva ganska mycket backuputrymme.

Det räcker om man tar backup på den information man inte vill ska gå förlorad. Dit räknas worddokument, e-mailadresser, e-mail, bilder och liknande.

Bilder kan man med jämna mellanrum spara ner på CD-skivor så att man har dem i säkert förvar. Digitala bilder är ofta av storleksordningen 200-500 KB. Detta innebär att cirka 1200 bilder får plats på en CD och att knappt 10000 bilder ryms på en DVD.

När det gäller worddokument så blir beräkningarna lite svårare eftersom storleken på worddokument varierar kraftigt. Samma sak med e-mail och e-mailadresser.

Hur ofta bör man då ta backup?

Jag föreslår att man planerar för att göra backup **minst** en gång per vecka. Detta beror ju på hur mycket man använder sin dator och hur mycket nytt man producerar.

Hur lägger man upp backuptagning?

Om du inte har ett backupprogram som sköter backupen åt dig behöver du strukturera dina backuper.

Exempel på hur du organiserar backuptagning.

En gång per dygn.

Måndag backup till media A

Tisdag backup till media B

Onsdag backup till media C

Torsdag backupp till media D

Fredag backup till media E

Lördag backup till media F

En gång per vecka.

Söndag backup till media VA (vecka 1), VB (v 2), VC (v 3), VD (v 4)

En gång per månad.

Söndag backup till media MA (månad 1), MB (månad 2), MC (månad 3)

Därefter börjar man om från början.

Vilken typ av backup bör man välja?

Som jag skrev här ovan så när det gäller bilder kan man kopiera ner sina bilder på en CD-skiva.

Worddokument kan man med fördel kopiera till en USB-"pinne". Då ska man kopiera ner sina dokument till nya mappar varje gång. När en pinne börjar bli full så kan man kopiera innehållet till en DVD-skiva.

E-mail och e-mailadresser blir lite mer komplicerat:
Adressboken kan exporteras till en textfil:
Öppna Outlook Express
Klicka sedan på *Arkiv - Exportera - Adressbok och välj Textfil*.

Att exportera **e-mailen** är ganska komplicerat. En lösning kräver att man använder webbläsaren Firefox och dess e-mailklient Thunderbird. Här finns en översättning från engelska - http://www.pihlgren.se/thunderbird/index.php.

Man ska då vara uppmärksam på att den är kanska stor, i mitt fall omkring 700 MB vilket kanske inte ryms på en CD utan man får ta till en DVD.

Väljer du det senare alternativet så får du med dig allt du inte vill sakna utom program, program som du kanske tankat ner från internet. Men personligen tycker jag att program tar man en säkerhetskopia av i samband med installationen så är det problemet löst.