IT SÄKERHET FÖR ÄLDRE

Sammanfattning

Detta dokument är framtaget inom ramen för projektet ”Bättre tänka efter före”, som är ett samarbete mellan PRO, SKPF och SPRF med stöd av MSB myndigheten.

Dokumentet beskriver på ett lättfattligt sätt de viktigaste sakerna att tänka på när det gäller säkert på Internet. Dvs. saker att tänka på när man e-postar, gör bankärenden, handlar eller surfar på nätet.

Målgruppen är äldre med viss datorvana. Alltså det förutsätts vissa förkunskaper och alla termer förklaras inte.

PRO

SKPF

SPRF

MSB Myndigheten för samhällsskydd och beredskap

Innehållsförteckning

1 Allmänt

Dokumentet innehåller den viktigaste och mest grundläggande informationen när det gäller säker användning av dator och internet. Dock dokument är en spegling av (delar av) verkligheten i augusti 2016 och på intet sätt fullständigt.

Internet utvecklas hela tiden så de programvaror/appar eller verktyg som rekommenderas kan ha ersatts med annat som fungerar bättre. Därför finns i slutet hänvisning till webbplatser där man kan få mer information. Förhoppningsvis finns dessa webbplatser kvar.

Bedragare hittar hela tiden på nya sätt att lura pengar av folk. Därför är det generellt sett bra att vara misstänksam mot saker som kan dyka upp i e-posten, när man surfar, besöker sociala medier eller i samtal på telefon.

En sund skepsis är alltså bra, däremot behöver man inte vara så rädd att man avstår från att lära sig om Internet och datorer.

Målgruppen ska få grundläggande kunskap om
- Risker på internet och hantering av dem
- Hur man skyddar sin viktiga information och sina personuppgifter (integritet)
- Säker lösenordshantering
- Säkerhetskopiering
- Hur man skyddar sin dator, surfplatta och mobil
- Hur man skyddar sig mot identitetsstöld

2 Allmänt om säkerhet

Det är viktigt att tänka på säkerheten när man använder sin dator, surfplatta eller smarta mobiltelefon. Det handlar om att
- man när man använder e-post eller internet uppträder på ett sätt så att man inte utsätter sig för onödig risk att förlora pengar.
- försäkra sig om att informationen finns på mer än ett ställe om datorn/surfplattan/mobilen skulle komma bort eller bli skadad.
- skydda datorn/surfplattan/mobilen från angrepp utifrån, dvs. att, så långt det går, förhindra att skadliga program kommer in i enheten.

2.1 Så skyddar du dig

Här är ett antal generella tips (grunden hämtad från webbplatsen polisen.se) på hur man skyddar sig. Vissa av tipsen finns också i de relevanta avsnitten.
- Öppna inte e-post eller länkar som är okända för dig. Risken finns att du får in virus i din dator som till exempel kopierar dina inloggningsuppgifter.
- Använd inte ett för enkelt eller samma lösenord till olika tjänster.
- Ha ett uppdaterat virusskydd på din dator och mobil.

- Skicka inte person- eller kontouppgifter via e-post. Om aktuellt företag, myndighet eller organisation har begärt in uppgiften försök få alternativt sätt att förmedla uppgifterna.
- Använd tjänster som ger dig information direkt i mobilen eller via e-post om någon tagit en kreditupplysning på dig. Då har du chansen att agera snabbt genom att kontakta polisen och aktuellt kreditbolag för att stoppa krediten/lånet från att beviljas.
- Se till att inga obehöriga kommer åt din post (gäller både e-post och snigelpost).
- Exponera inte dina personuppgifter i onödan. Lämna inte ut ditt personnummer på nätet utan att du försäkrat dig om att mottagaren är seriös. Ta också reda på hur dina personuppgifter kommer att hanteras och användas.
- Släng inte post med personlig information i soporna eller pappersinsamlingen
- Om du tappat bort en identitetshandling, anmäl det till Polisen, banken och till kreditupplysningsföretag.
- Ladda inte ned nya appar utan att ha kontrollerat om de funnits ett längre tag och fått positiva recensioner och betyg.
- Kontrollera antal recensioner och betyg innan du laddar ner appar.

2.2 E-legitimation – varför och hur

E-legitimation är ett sätt att säkert identifiera sig på nätet. Det är en elektronisk ID-handling som är personlig och som man bör skydda så mycket man kan, samma princip som med vanligt körkort, pass eller identitetskort.

E-legitimation behövs för att enkelt och säkert ha kontakt med bank, myndigheter, sjukvård, försäkringskassa m.m. Förutom att deklarera och se sina pensioner på Pensionsmyndigheten finns webbplatsen ”Mina Vårdkontakter”. På den kan man se alla sina recept – hur om det finns fler uttag – man kan också se sina bokade läkartider förutsatt att den vårdgivaren har kontakt med ”Mina vårdkontakter”.

E-legitimation är en fil med dina personuppgifter som läggs på din dator, eller på ett kort; alternativt kan e-legitimation läggas som en App i mobiltelefon/Surfplatta.

E-legitimation skaffar man sig bäst genom sin internetbank eller via Telia. Se mer på bankid.com/.

BankID ( ) tillhandahålls av de flesta banker. På Skatteverkets ID-kort kan man få Telias ( ) E-legitimation. Då behövs också en kortläsare. Det lösenord man behöver BankID/e-legitimationen bör vara ditt säkraste och gärna ett som du inte använder i andra sammanhang. Läs mer i 2.4 Lösenord.

Lösenordet på ditt BankID, liksom koden till ditt Mobila BankId bör förvaras på ett betryggande sätt. Det är bara du som har den och om du förlorar den behöver nytt (Mobilt) BankId laddas ner.

Man ladda ner BankId och Mobilt BankID på flera enheter.

Underskrifter som skapas med BankID/Moblt BankID/E-legitimation är i de flesta sammanhang likvärdiga med en underskrift på papper.

2.3 Identitetsstöld

Olovligt användande av någon annans identitetshandlingar brukar kallas identitetsstöld. Det kan leda till att någon använder ditt namn för att köpa varor eller ta krediter. Det kan också vara att dina personuppgifter används för att få ut bank- eller kreditkort, lån, speltjänster eller för att köpa varor på kredit i butiker.

Var alltid försiktig med dina personliga uppgifter och om dokument som innehåller personlig information, speciellt dokument som pass, körkort och andra identitetshandlingar.

Om du upptäcker eller misstänker att du utsatts för en identitetsstöld, gör en polisanmälan genom att ringa 114 14 eller besöka en polisstation. Identitetsstöld ska också alltid anmälas till banken.

Några tips:

- Skicka inte person- eller kontouppgifter via e-post utan att först ha kontrollerat att aktuellt företag, myndighet eller organisation har begärt uppgiften.
- Det är viktigt att förstöra elektroniska media, som CD-skivor, USB-minnen, hårddiskar med personlig information innan du kastar/säljer dem.
- Var uppmärksam om det gjorts en kreditupplysning på dig. Ta reda på vem som har gjort den och varför.
- Använd tjänster som ger dig information direkt i mobilen eller via e-post om någon tagit en kreditupplysning på dig. Då kan du agera snabbt och kontakta aktuellt kreditbolag.
- Om någon tar kontakt med dig via mail eller telefon och vill ha information från dig – ska du alltid be att få återkomma via företagets växel. Det kan röra sig om phishing (=någon försöker lura dig på pengar).
- Kontrollera regelbundet dina kontoutdrag. Följ upp om du inte känner igen en utgift eller betalning.

Mer information finns på webbplatserna polisen.se/utsatt-for-brott och dinsakerhet.se/sakrare-hemma/teknik-och-it/identitetsstold/

Ett sätt att begränsa skadan vid en eventuell identitetsstöld är att ansluta sig till företag som meddelar dig vid varje kreditupplysning. Det finns dels Upplysningscentralen (UC, webbplats: minuc.se), som tar betalt och dels Bisnode Kredit (webbplats: minupplysning.se) som är gratis skickar ut information om kreditupplysningar.

Man kan också skaffa sig ett konto (en ”brevlåda”) hos Kivra ((kivra.com). En tjänst som innebär att din post från anslutna myndigheter och företag hamnar i en digital brevlåda hos Kivra, som sedan sänder ett e-postmeddelande till dig om att du fått ett brev. På så sätt slipper du riskera att någon vittjar din fysiska brevlåda och kommer över viktiga handlingar.

2.4 Lösenord

Lösenord är ditt sätt att skydda din identitet, din dator, din e-post och andra konton du kan tänkas ha på olika webbplatser. Därför är det viktigt att ha ett säkert lösenord, ett som inte kan knäckas med hjälp av uppgifter om din person och familj. Ett säkert lösenord består av stora och små bokstäver, siffror och specialtecken. Se också. Checklista för lösenord under *Säkrare hemma* och *sedan Teknik och it* på dinsakerhet.se. Där finns en hel del matnyttig information.

Det rekommenderas att man inte har samma lösenord på flera ställen. I dagens läge kan detta vara svårt att uppnå eftersom så många webbplatser vill att man ska registrera sig och ha ett lösenord. Viktigt dock att man urskiljer vilka lösenord som är viktigast, exempelvis e-legitimationen, e-posten, banken, Facebook, m.m. Dessa viktiga platser bör ha egna och säkrare lösenord än webbplatser som t.ex. DN eller Aftonbladet.

Varför är ett bra lösenord till e-posten viktigt? – Därför om du har ett lösenord som är lätt att gissa sig till kan någon få tillgång till din e-post och då också se de nya lösenord du får när du någonstans har klickat ”Jag ha glömt mitt lösenord”.

Det finns idag hjälpmedel för att lagra sina lösenord. Har man ett sådant hjälpmedel bör lösenordet dit naturligtvis vara det allra säkraste, gärna en hel mening som relaterar till något man säkert kommer ihåg. Det är svårt att rekommendera något speciellt verktyg eftersom det ofta kommer nya som är bättre eller lättare att använda.

Tips 1: Använd olika lösenord för olika tjänster. För att memorera dem kan du komma på ett eget system där du använder ett tilläggsord som är relaterat till respektive tjänst på ditt vanliga lösenord.

Tips 2: Ett sätt att skapa ett unikt och lättmemorerat lösenord är att ta begynnelsebokstäver i de första orden i en låttext eller ramsa som du kan utantill.

Tips 3: Använd en kort mening och byt någon del av ord mot en siffra (t.ex. Intressant kan bli In3ssant, råtta kan bli r8).

Tips 4: Om man t.ex. har haft ett husdjur kan man använda djurets namn och året man skaffade djuret, men sedan i namnet byta ut vissa bokstäver mot siffror. T.ex. kan man byta B mot 8, o mot 0, l mot siffran 1. (Ett exempel: Pluto kan bli 91ut0)

I vissa smarta telefoner kan man istället för att ha ett lösenord logga in sig med att rita en figur på skärmen. Det visar sig ge en snabbare och säkrare inloggning.

Använd din fantasi! På webbplatsen dinsakerhet.se under *Starka lösenord* finns tips om vad man ska tänka på när man skapar ett lösenord.

Här finns tester man kan göra på vad som är ett starkt lösenord (testen bör inte göras på egna lösenord):

- http://www.passwordmeter.com/
- https://www.dinsakerhet.se/ under *Starka lösenord*

Här är ett par listor från olika håll som visar vanliga lösenord (som man alltså ska undvika):

FAKTA

Här är de 20 vanligaste lösenorden från hackade Gratisbio.se. Siffran i vänsterspalten anger hur många användare som valt respektive lösen.

1162 123456
612 hejhej
534 hejsan
374 fotboll
354 123456789
311 bajskorv
293 sommar
252 blomma
233 mamma
231 123123
201 dinmamma
173 johanna
166 1234
159 12345
147 smulan
147 amanda
139 qwerty
139 bajs
135 hejhejhej
132 glosor

1. 123456
2. password
3. 12345678
4. qwerty
5. abc123
6. 123456789
7. 111111
8. 1234567
9. iloveyou
10. adobe123
11. 123123
12. admin
13. 1234567890
14. letmein
15. photoshop
16. 1234
17. monkey
18. shadow
19. sunshine
20. 12345
21. password1
22. princess
23. azerty
24. trustno1
25. 000000

2.5 Grundläggande information om säkerhet

En viktig del av säkerhet är att känna till vissa grundläggande principer. Några följer här. Bedragare hittar hela tiden nya sätt att lura till sig pengar så råden här är bara ett axplock av det som är känt i skrivande stund.

Generellt ska man vara skeptisk inställd till att uppge kontoinformation till andra personer. Liksom att vara skeptisk inställd till frågor på sociala medier (t.ex. FaceBook) från vänner som behöver pengar. Kontrollera med ett telefonsamtal att meddelandet verkligen kommer från den person som uppges i meddelandet.

Du ska aldrig uppge pinkoder till någon annat än om du har absolut förtroende för personen i fråga och personen ska ta ut pengar för din räkning.

Din bank frågar aldrig efter pinkoder eller kontoinformation på e-post eller på annat sätt. Kontonummer kan man uppge till personer man har förtroende för. Om du har upprepat behov av att uppge kontonummer till personer som ska sätta in pengar till dig så är det bra att öppna ett speciellt konto för detta ändamål. Sedan flyttar du pengarna till ett konto där du vill ha dom. På så sätt kommer det aldrig att under längre tid finnas stora summor på kontot. Samma konto kan med fördel användas för Swish.

Microsoft (eller någon annan leverantör) skulle aldrig ringa upp dig eller kontakta dig på e-posten för att åtgärda ”säkerhetshot” eller för att ta reda på pinkoder eller inloggningsuppgifter.

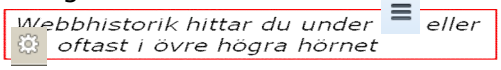
Uppdateringar av operativsystem och annan programvara (appar) dyker automatiskt upp i din dator och kommer aldrig på e-post.

Uppdatering av säkerhetsprogram du har i datorn görs också automatiskt. Det kan tänkas att du får en fråga om du vill uppdatera och om det är det säkerhetsprogram du har är det bara att acceptera uppdateringen.

2.6 Att använda offentliga datorer eller nätverk

Offentliga nätverk är ofta oskyddade till skillnad från ditt privata nätverk som (oftast) har en s.k. brandvägg som utgör ett hinder för att få in på virus, trojaner, maskar eller andra oälkomna besök i din dator.

Det finns situationer när man behöver man låna dator och/eller nätverk på bibliotek eller hotell. Beroende på till vad man behöver datorn bör man tänka på att:

- Försäkra dig om att nätverket är riktigt och inte ett tillfälligt nätverk som någon satt upp för att kunna komma åt person- eller bankuppgifter.
    - Se till att vid inloggning, rutan där det står ”kom ihåg mig” **inte** är markerad. Detta eftersom markering innebär att lösenordet sparas på datorn.
    - logga ut när du är klar
    - rensa ordentligt: radera webbhistoriken och stäng ner webbfönster som använts. 

Om man har en smart telefon eller en surfplatta bör man stänga av den funktion som automatiskt söker efter öppna nätverk. Bättre att man har kontroll på när och i vilket nät man kopplar upp sig.

2.7 Kakor eller Cookies

En cookie eller kaka är en liten textfil som kan användas för att identifiera din telefon eller dator nästa gång du besöker en sajt. Om du till exempel besökt trafiken.nu och valt Stockholm, kommer den ihåg ditt val och nästa gång kommer du direkt till trafikinformationen för Stockholm.

Du kan ändra i hur stor grad du vill undvika kakor. Det finns i de flesta webbläsare i övre högra hörnet en symbol under vilken man kan leta efter Sekretess, säkerhet eller inställningar och förändra sina val. (Detta ser olika ut för olika webbläsare.)

En cookie kan också lagra lösenord så att du slipper ange det nästa gång du besöker webbplatsen. Det valet finns oftast som en ruta att bocka i vid inloggning. Rekommenderas bara att göra på din egen dator, surfplatta eller telefon.

Numera krävs ofta att man godkänner att webbplatsen använder cookies. Webbplatsen kan således spara din surfing, men har inte tillgång till dina kontakter.

Cookies kan man radera i webbläsaren genom att radera webbhistoriken.

2.8 Företagens informationsskyldighet

Du har alltid rätt att avsäga dig nyhetsbrev och annan marknadsföring.

Enligt personuppgiftslagen har du också rätt att få veta vilken information som finns sparad om dig. Du kan även be att dom raderar information som inte är korrekt.

Ett företag är skyldigt att informera dig om dessa rättigheter i samband med att uppgifter från dig samlas in.

3 E-post, nätfiske och tävlingar

3.1 E-post

En sak att tänka på med e-post är att det inte är ett riktigt säkert sätt att skicka meddelanden. D.v.s. säkert i betydelsen att ingen kan läsa det du skickar. Man brukar säga att e-post är jämförbart med att skicka ett vykort. Om du tänker skicka känsliga uppgifter i e-post. Tänk efter – skulle du skriva dem i ett vykort?

Undersökningar visar att en stor andel av all e-post som skickas ut har som syfte att på något sätt lura dig. Det mesta är ofarliga meddelanden, ofta dåligt formulerade som vill sälja Viagra eller från en ”vacker flicka” som vill ha kontakt. Den typen av meddelanden är det bara att radera.

Med e-post kommer det ibland oönskade effekter. Det kanske minst allvarliga är e-post med roliga bilder, historier eller annat. Dessa är som regel bara störande och ställer inte till problem i datorn.

Viktigt är att inte klicka på länkar och inte öppna bilagor. Viktigt är också att ha inställningen ”låter det för bra för att vara sant är det förmodligen så”. Det finns också orsak att kontrollera adressen i länkar noggrant. Till exempel en länk som leder till Nordea börjar nordea.se eller nordea.com. Detta kan kontrolleras om du med muspekaren pekar på länken dyker det upp en ruta där du ser den webbadress länken leder till – läs den!

Ofta har det verktyg (app) man använder för att läsa sin e-post ett s.k. spam-filter. Alltså ett filter som ska sortera bort e-post som kommer från misstänkta avsändare. Filtret är långt ifrån heltäckande, men e-post som ”fastnar” i filtret läggs i en egen mapp ”Skräppost”. Ibland hamnar e-post som inte är skräp i den mappen.

3.2 Nätfiske

I e-posten kommer ibland meddelanden som brukar kallas ”Nätfiske” (eller phishing). Den typen av meddelanden är att du har vunnit, ärvt eller annan möjlighet att få pengar bara du uppger ett bankkonto. Men sedan visar det sig att för att få pengarna måste du betala för något och i slutänden har du förlorat eftersom de utlovade pengarna inte kommer.

En annan typ av nätfiske är att det kommer ett meddelande från vad som verkar vara en vän. Där ”vännen” säger sig vara i behov av pengar av någon orsak. Den typen av meddelanden ska man kontrollera med sin vän. Oftast visar det sig att vännen inte alls har skickat något meddelande utan kanske fått sin e-post ”kapad” (dvs. någon har ”tagit över” e-postadressen i akt och mening att lura till sig pengar).

En annan typ av nätfiske är att det kommer e-post som verkar vara från din bank och att banken vill att du uppger kontonummer, kreditkortsnummer, koder eller annan känslig information. Ingen bank eller kreditkortsföretag begär någonsin den typen av uppgifter av dig, speciellt inte i e-post.

Ytterligare en variant är ett om paket du ska få. Har du inte köpt en lott eller beställt något så är det någon som vill lura pengar av dig.

Tre saker att kontrollera för att se om man är utsatt för nätfiske:

1. Stavfel eller konstig meningsbyggnad
2. Kontrollera avsändaren, speciellt det som står efter ”@”. Även om avsändaradressen är riktig går det att fejka en avsändare i e-posten.
3. Vart leder länken? Alltså inte vad som står i mejlet/på webbplatsen utan den adress som dyker upp när man ”pekar” på länken med musen. Verkar den vara riktig, är namnet rätt stavat?

3.3 Tävlingar på nätet

När du anslutit dig till en webbplats, eller på sociala medier kan det tänkas dyka upp erbjudande av typen ”Svara på några frågor och vinn en Ipad” eller ”Grattis du är den 100 000 besökaren och har vunnit…” Dessa och liknande oseriösa erbjudanden förekommer ofta på internet.

För att få till gång till vinsten/gåvan behöver du ofta ange kortnummer och godkänna avtalsvillkoren. Dessa avtalsvillkor ska man alltid läsa igenom. Villkoren kan innebära att dina uppgifter skickas vidare till alla deras samarbetspartners (ofta en lång lista) som ges rätten att kontakta dig via brev, e-post eller telefon. Det kan också tänkas att dina uppgifter skickas till annat företag där villkoret innebär att du tecknat ett avtal om något som inte alls är gratis.

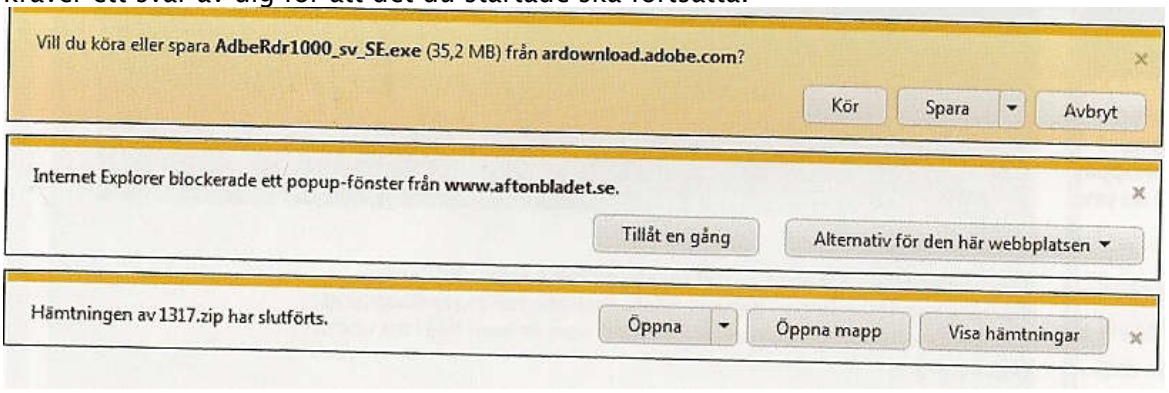
4 Informationsfält och Pop-up fönster

4.1 Informationsfält

Informationsfält dyker upp i olika situationer, speciellt om länken du klickade på vill öppna ett eget fönster eller om du startat en nedladdning. Om det inte händer det du väntade dig titta efter om det dyker upp någon information någonstans. Detta är olika i de olika webbläsarna.

4.2 Pop-up fönster

Pop-up fönster är rutor eller fönster som öppnas av din webbläsare och som kanske kräver ett svar av dig för att det du startade ska fortsätta.



Men pop-up fönster kan också dyka upp som annonser, erbjudanden, enkäter eller annat irriterande. Läs och försök förstå vilken typ av pop-up fönster du fick. Det händer också att du får något i stil med ”Du är den 100 000 besökaren och har vunnit …” Tro inte på det! Klicka inte på den typen av länkar.

Pop-up fönster har oftast ett (rött) x i övre högra hörnet – där kan man stänga fönstret.

Ibland kommer ett s.k. pop-up fönster upp i webbläsaren och påstår att din dator är långsam eller utsatt för säkerhetshot eller att minnet är fullt. Klicka aldrig i ett sådant pop-up fönster. Det minst allvarliga som händer är att du hamnar på en webbplats där du kan köpa program för att åtgärda ”felet” (som långt ifrån alltid är ett verkligt fel eller problem).

Det är bra att ha kontroll på vilket/vilka säkerhetsprogram man har i datorn. Det är bara varningar från de egna programmen som ska tas på allvar.

Även i detta fall förändras beteenden hela tiden, så det som beskrivs här kanske inte används längre utan det är andra saker som händer på din skärm. Så, även här var lite misstänksam!

5 Att handla på nätet

5.1 Avtal på nätet

När man handlar på nätet ingår man ett avtal med företaget/personen man handlar med. Ett sådant avtal är bindande förutsatt att det varit tillräckligt tydligt på webbplatsen där avtalet ingicks att det är det man gör.

Inte bara när man handlar utan också i andra fall där man klickar in ”Jag accepterar villkoren” kan det vara bra att läsa åtminstone de delar av villkoren som reglerar godkännande av personuppgifter och dataanvändning (=användning av filer, foton och annat). Några exempel nedan.

Företag som tillhandahåller e-post eller andra molntjänster (dvs. tjänster på nätet) har tekniska möjligheter att söka igenom dina filer. Därför är det viktigt att läsa igenom den delen av villkoren.

Vissa säger tydligt att ”Vi använder inte det du säger i e-post, chat, videosamtal eller röstmeddelanden för att rikta reklam till dig. Vi använder inte dina dokument, foton eller andra personliga filer för att rikta reklam till dig.”

I andra sammanhang kan det till exempel anges ”Dessa och andra funktioner kan kräva att våra system kommer åt, lagrar och söker igenom dina saker. Du ger oss tillstånd att göra dessa saker, och detta tillstånd sträcker sig till betrodd tredje part som vi arbetar med.”

Terms of Service; didn’t read – webbplats: https://tosdr.org/ – är en organisation där olika webbtjänsters villkor är klassificerade och man lätt kan få en övergripande uppfattning om vad man tillåter när man accepterar villkoren.

Checklista innan du godkänner ett avtal:

- Vilken information om mig lämnar jag ut och hur används den?
- Finns en policy för vem som får se informationen?
- Lämnas information om mig vidare till andra företag? I vilket syfte?
- Kan jag kryssa bort ev. nyhets- och marknadsföringsbrev?
- Vad händer med filer jag laddar upp? – Kan företaget använda det fritt?
- Hur avslutar jag mitt konto? Vad händer med den information jag laddat upp?
- Vad förbinder jag mig till?

En grundregel är också att om det är en gratistjänst ska man inte behöva uppge något kreditkortsnummer.

Även när man träffar på tävlingar på nätet ska man läsa villkoren. Oftast är villkoren ”bara” att man tillåter alla ”samarbetspartner” att kontakta dig på telefon, e-post och brev. I det fallet kan man inte hänvisa till ”NIX” i telefonen. Någon gång kan det dock hända att villkoren är något annat t.ex. att du beställer en prenumeration. Så LÄS villkoren alltid!

5.2 Betala på Internet

Vissa e-handelsplatser ger möjlighet att välja betalningslösning. Där det går är betala mot faktura det som känns säkrast, i annat fall välj ett betalningssätt du känner dig trygg med.

Nordea, Swedbank och Föreningssparbanken erbjuder en möjlighet att skapa tillfälliga betalkort som då används för bara ett köp. Andra banker har system som Verified by Visa eller Secure Card som är säkrare sätt att betala på Internet. Ytterligare andra banker erbjuder möjligheten att stänga kortet för internetbetalningar. Då öppnar man precis när man vill handla och kan stänga igen när man är klar.

Swish är en funktion i mobilen där man med appen Swish och Mobilt BankId kan föra över och ta emot pengar. Man behöver inte uppge ett bankkonto utan det räcker med mobilnumret. När någon betalar till dig får du direkt ett meddelande till telefonen att pengarna betalats.

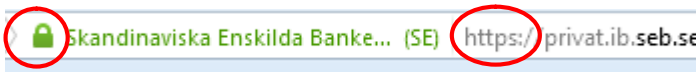
Man beställer på sin bank och knyter ett bankkonto till Swish. Där anger man också hur mycket pengar man kan ”swisha” under en dag. Det kan kanske vara bra att det kontot man knyter till Swish är ett konto där det normalt inte står mycket pengar.

5.3 Handla på e-handelsplatser

Webbplatser som är seriösa e-handelsplatser har ofta en märkning: eller

Det kostar pengar att få en märkning därför kan det tänkas att små aktörer inte har märkningen även om dom är seriösa.

En annan sak att kontrollera är att webbadressen börjar med https och att det finns ett hänglås som markerar att det är en säkrare webbplats. Lämna bara kortnummer på platser där detta finns. Om man klickar på låset kan man verifiera att det är rätt ägare/utgivare.



Det ställs krav för att få en certifiering:

- Tydlig avsändare
- Godkända betallösningar
- Personlig support
- Tydliga riktlinjer för returer och reklamationer
- Tydliga priser

Saker att tänka på när man handlar på nätet:

- Handla endast på kända webbplatser
- Kontrollera att det finns informationen på webbplatsen om hur du kan kontakta företaget för personlig information och service
- Kontrollera alltid att det finns information om leveranstider och -kostnader

- När det finns möjlighet att välja betalningssätt (faktura, kreditkort, postförskott …) välj något du känner dig säker med
- Kontrollera att företaget upplyser om ångerrätt (inom EU gäller 7 dagar, inom Sverige 14 dagar) och att det finns information om hur du gör om du vill återlämna varan.
- Handlar du från webbsida som inte är i Sverige kontrollera att ev. garanti gäller i Sverige.
- Om du handlar från företag utanför Sverige tänk på att du kan behöva betala tull.
- Välj gärna kända företag

Ångerrätt gäller när man handlar av företag på internet, via telefon eller på annat ställe där försäljaren inte är i sin ”affär”. För varor gäller ångerrätten från när du mottagit din vara. För tjänster börjar ångerrätten gälla från du skrivit på avtalet.

På Internet säljs också piratkopior. Eftersom det är olagligt både att köpa och att sälja piratkopior så undviker man det.

På nätet säljs stöldgods. Eftersom begreppet ”god tro” inte lägre finns är det viktigt att kontrollera att kvitto, garanti eller annat bevis för äganderätten finns. Detta är speciellt viktigt när man handlar av privatpersoner.

När man handlar privat är det viktigt att man säkrar att man får varan innan betalningen når säljaren. På handelsplatser som Blocket och Ebay brukar det finnas lösningar för detta. Bäst är att handla lokalt så att man byter vara och pengar direkt.

6 Mötesplatser – sociala medier och annat

Det finns på nätet ett antal olika mötesplatser där FaceBook är det (idag) mest kända exemplet.

Generellt att tänka på när man lägger ut personlig information på någon som helst plats på Internet är att information och bilder man lägger upp har man inte längre någon kontroll på och det finns kvar även om man försöker ta bort den.

Därför att det bra att tänka ett extra varv och inte lägga ut alltför privat information.

Läs igenom villkoren noga och ställ in säkerheten. T.ex. vill du verkligen att din adressbok skall vara åtkomlig? Tänk till ett varv extra här.

7 Hur man skyddar sin dator, surfplatta och mobil

Detta avsnitt handlar om två saker – dels att skydda sin dator från skadlig kod och dels att skydda det man har på datorn om datorn skulle skadas eller försvinna.

Det är viktigt att man i surfplattan har samma skydd som i datorn. Telefonen bör också ha ett skydd.

7.1 Skadlig kod

Med ”skadlig kod” avses små program som kan ställa till problem i din dator. Den typen av program kallas ofta virus, trojaner eller maskar. Det är alla olika typer av program som är skadliga på olika sätt.

Virus kan t.ex. radera filer på din hårddisk eller utnyttja datorn så att den blir långsam när du använder den. En trojan kan exempelvis användas för att ”avlyssna” din dator och den vägen komma över kontokortsinformation, koder och lösenord.

Dessa typer av skadlig kod sprids via e-post, men kan också spridas på andra sätt t.ex. via USB-minnen, DVD/CD skivor, sociala medier eller ibland från andra webbplatser.

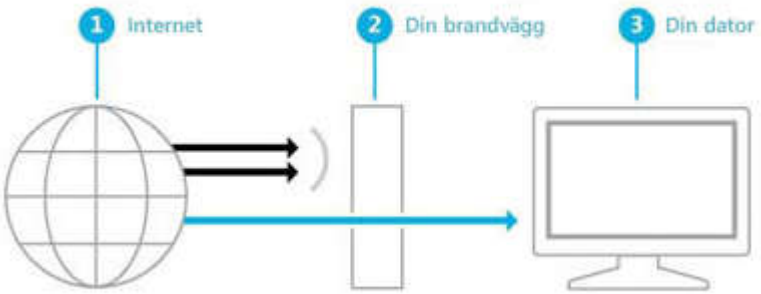
Nyligen började det florera något om kallas ”Ransomware”. Råkar man ut för det blir alla dokument (MS Word, Excel, pdf, powerpoint, …) krypterade och kan inte läsas/tydas. Erbjudande om att lösa krypteringen kommer, men det kostar pengar. Ingen har hittills lyckas lösa den krypteringen. Denna skadliga kod sprids med e-post.

Det kan också hända att bedragare ringer upp dig och säger sig vara från t.ex. Microsoft. Bedragaren uppger sig se att du har problem med din dator och vill att du ska utföra ett antal kommandon. Gör inte det. Bedragaren som ofta pratar engelska låter mycket trovärdig, men, nej Microsoft eller andra arbetar inte på det sättet.

7.2 Säkerhetsprogram

Det finns tre huvudtyper av säkerhetsprogram ett kallas brandvägg (firewall), ett är antivirus program och det tredje är appar mot skadlig kod.

En brandvägg låser ytterdörren och ska fungera som en barriär mot intrång av hackare eller maskar, se bilden nedan kopierad från Windows webbplats.



Med Windows följer en brandvägg och ytterligare skydd behöver man troligen inte som privatperson. Man ska ha bara en brandvägg på datorn har man fler kan det orsaka konflikter och problem. Det finns också oftast en brandvägg i den router som Internetleverantören tillhandahåller, den brandväggen måste också finnas.

Antivirusprogram däremot skyddar mot virus och appar mot skadlig kod skyddar just mot skadlig kod.

Med Windows 10 följer Windows Defender som är ett antivirusprogram som skyddar din dator på två sätt:

- Realtidsskydd. Om spionprogram försöker installera sig eller köras på datorn, eller om ett program försöker ändra viktiga inställningar visas en varning.
- Sökalternativ. Man kan använda Windows Defender för att söka efter spionprogram som kan ha installerats på datorn.

Man kan också söka på nätet efter gratis antivirus. Det finns många t.ex. AVG. När man ska ladda ner ett gratisprogram gäller det att läsa noga i villkor och beskrivningar eftersom vissa utgivare kallar det gratisprogram, men egentligen är det bara en gratis provperiod och sedan vill dom ha betalt.

7.3 Säkerhetskopiering

Säkerhetskopiering av det man har på datorn är viktigt om datorns hårddisk skulle skadas eller gå sönder (eller att du råkar ut för RansomWare). Tänk efter vad du har på datorn som du verkligen skulle sakna – bilder, meddelanden, dokument, …

Säkerhetskopiering kan göras på olika sätt. Man kan ha en lös hårddisk, eller lagring på nätet (eller som man säger ”i molnet”).

Fördel med att ha på nätet är att i händelse av brand så finns filerna kvar. Nackdelen är att om man har mycket så kostar det per månad eller år.

En lös hårddisk kostar i inköp. Men inte mer än så, Nackdelen är att i händelse av brand eller inbrott finns risken att också den lösa hårddisken inte är kvar.

I båda fallen följer det med programvara för att göra regelbundna säkerhets-kopieringar.

7.4 Installation av appar

En app är ett program som installeras på din dator, i din surfplatta eller i din telefon.

Olika appar begär olika mycket åtkomst till din information. Innan du laddar ner appen, läs användarvillkoren och se till att du vet vilken information du ger appen tillgång till.

När villkoren för en app förändras innebär det att appen behöver uppdateras. Om du vill granska uppdateringen kan du inaktivera funktionen automatisk uppdatering. Du får då möjlighet att granska förändringarna.

Om en app vid en uppdatering behöver åtkomst till något i din telefon som inte tidigare varit åtkomligt för appen måste du alltid godkänna uppdateringen.

8 Sammanfattning

För att skydda din dator och dina personliga uppgifter:

- Installera ett antivirusprogram och håll det uppdaterat
- Installera en brandvägg (följer oftast med från din Internet leverantör)
- Uppdatera datorns operativsystem och webbläsare (en automatisk fråga dyker upp i datorn, aldrig i e-post)
- Kortnummer, koder, lösenord och liknande är att betrakta som värdehandlingar. Lämna därför aldrig ut denna information till någon, inte ens till din egen familj
- Lämna aldrig ut lösenord, kortnummer eller koder via e-post, telefon eller sociala medier till någon. Lämna inte ens ut koder till din egen bank.
- Ladda inte ner bilder, filmer, spel och program från okända webbplatser
- Logga alltid ut när du är färdig med dina bankärenden och stäng webbläsaren
- När du tar ut kontanter eller betalar med kort är det viktigt att du skyddar din kod, till exempel genom att dölja den med handen
- Var extra uppmärksam på pop-up-fönster som ser konstiga ut eller om du ombeds lämna ut personlig information – läs vad som står, det kan vara förknippat med något du vill göra. Om det inte är det stäng fönstret (krysset i hörnet kan man alltid använda)
- Var extra försiktig vid bankomatuttag. Bankomaten kan ha försetts med så kallad skimningsutrustning. Kontrollera att det inte sitter en dold kamera på bankomaten eller att den är manipulerad annat sätt
- Välj aldrig en PIN-kod som är en del av ditt personnummer, telefonnummer eller annat nummer som lätt kan förknippas med dig.
- Undvik att göra dina bankärenden via publika datorer, till exempel på internetcaféer

Tips för att känna igen falska sidor är att kontrollera adressfältet i webbläsaren. Du ska känna igen adressen till sidan du ämnade gå in på. Kontrollera stavningen noga, ofta används webbadresser som starkt påminner om den verkliga. T.ex. kan det stå Svedbank istället för Swedbank.

9 Referenser

Referenser till litteratur som använts till detta dokument men som också kan användas för fördjupning:

Ref.1. Surfa säkert, Max Walter
Docendo, ISBN 978-91-7882-781-7

Ref.2. It-säkerhet för privatpersoner – en introduktion, Daniel Goldberg och Linus Larsson; Beställs eller laddas ner från iis.se/lar-dig-mer/guider

Ref.3. Användarvillkoren som ingen läser, Johanna Lundeberg
Beställs eller laddas ner från iis.se/lar-dig-mer/guider

Referenser i form av länkar till webbplatser som använts eller som kan användas för fördjupning

Ref.4. MSB: Informationssäkerhet https://msb.se/informationssakerhet och dinsakerhet.se/ under *Säkrare hemma* och sedan *Teknik och IT*

Ref.5. MSB: Datorstödd informationssäkerhetsutbildning för användare disa.msb.se/

Ref.6. MSB; Om att skydda sig mot identitetsstöld https://www.dinsakerhet.se/sakrare-hemma/teknik-och-it/identitetsstold/

Ref.7. http://www.dinsakerhet.se/Informationssakerhet/Konkreta-rad-informationssakerhet/Identitetsstold/

Ref.8. Windows: Hur skyddar jag datorn från virus http://windows.microsoft.com/sv-se/windows-8/how-protect-pc-from-viruses

10 Länkar

Några ”kan vara bra att ha” länkar

1. Tips: Hur man skyddar sig mot identitetsstöld http://www.testfakta.se/konsument/article62739.ece
2. Tips: Hur man skyddar sig mot identitetsstöld http://www.forsakra.net/blogg/identitetsstold-sa-skyddar-du-dig
3. Tips: Hur man skyddar sig mot identitetsstöld https://www.paypal.com/se/cgi-bin/webscr?cmd=xpt/Marketing/securitycenter/general/UnderstandIdTheft-outside
4. Guide om nätfiske https://www.paypal.com/se/cgi-bin/webscr?cmd=xpt/Marketing/securitycenter/general/UnderstandPhishing-outside
5. ICA kuriren: Så funkar appar i mobilen http://www.icakuriren.se/Test-Rad/Konsument/SFD-appar/
6. Webbplats om skydd för personlig integritet dataskydd.net
7. Ny Teknik: Din Mobil läcker som ett såll: http://www.nyteknik.se/tekniknyheter/article3889462.ece