Behöver du säker förvaring av bilder och dokument?

Ja, det vet du bara själv. Gör det något om du skulle förlora alla dina bilder eller dokument?

Kom ihåg, det finns t ex bara två typer av hårddiskar: trasiga och de som ännu inte är trasiga.

Datorn kan gå sönder pga ålderskrämpor, du kan tappa den i golvet eller spilla kaffe på den.

Du kan bli bestulen eller glömma datorn, surfplattan eller mobilen på bussen.

Du kan göra fel, t ex radera en bild av misstag eller få in ett virus som förstör dina dokument.

***En backup**, dvs en lagring av kopior av bilder och dokument på en säker plats löser detta!*

Har du flera datorer, surfplattor eller mobiler, så är det arbetsbesparande med funktioner som ser till att det alltid finns samma version av dina bilder och dokument på alla enheter.

***Med fortlöpande synkronisering** av bilder och dokument fungerar detta helt automatiskt!*

Begrunda skillnaden och håll isär dessa två begrepp:

***Backup** för att säkra att du inte förlorar dina bilder och dokument!*

***Synkronisera** för att underlätta din vardagliga hantering av dem!*

Alternativ för backup och synkronisering

Abonnerade molnlagringstjänster

Egna externa hårddiskar och usb-minnen

Mina enheter

Tryckta fotoböcker

Alla dessa bovar…

Bovarna söker upp dig

Traditionellt via fysisk kontakt som inbrott i bostaden, rån på stan etc.
Men även via brev att du t ex fått ett arv. Eller bluffakturor via post.
Numera finns raffinerade sätt att kontakta dig via telefon, mejl eller sms.
Bovarna stressar med en kritisk händelse, du måste t ex stoppa intrång på ditt bankkonto genom att logga in ditt Bank-ID, lämna uppgift om ditt bankkort för att få ut ett paket, etc.

Du söker upp bovarna

När du surfar på **webben** kan du själv ”råka” välja att besöka en (skum) hemsida. Den kanske verkar seriös eller så kan den se ut exakt som din banks. Bovarna kan t ex jobba med snarlika webbadresser, för att få dig att tro att du kommit till din bank. Bovarna kan sen lura dig att trycka på någon ”länk”, så att du laddar ner farliga program, uppger dina kortuppgifter etc.

Bovarna spionerar på dig

Det kan t ex vara **hemma** via **din router** om dina inloggningsuppgifter är kända, byt gärna dessa till egna. Eller **borta** när du ansluter till ett **öppet** (okänt) **wifi-nätverk**, logga aldrig in på din bank etc i dessa fall (endast ”slösurf”). Bättre att använda mobilsurf när du är borta.

Bovarna stjäl din identitet

Ditt personnummer och många andra uppgifter om dig är offentliga. Om du inte spärrat på Skatteverket kan en bov t ex ändra din folkbokföringsadress med en enkel pappersblankett!

Några bra webbplatser om säkerhet

internetstiftelsen.se har mycket information på sin webbplats om på IT och internet. Under **internetkunskap.se** finns fakta och videor om webben och säkerhet. Läs t ex om lösenord: internetkunskap.se/it-brott/ar-det-inte-dags-att-bry-dig-lite-mer-om-dina-losenord

nikkasystems.com är ett företag med inriktning på IT-säkerhet, med aktuell information bl a som poddar (radio på nätet) och videor. Varje vecka burkar de producera ett nytt poddavsnitt som du hittar på sidan: nikkasystems.com/bli-saker/bli-saker-podden

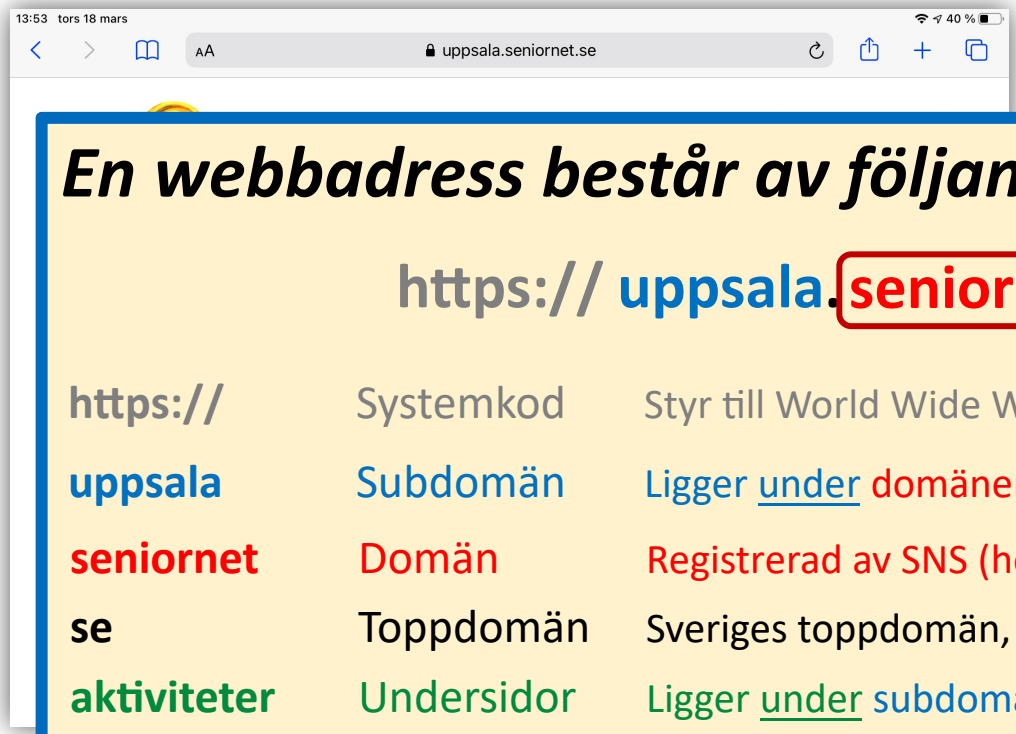
stoldskyddsforeningen.se har många tips och checklistor för att skydda sig mot bedrägerier och brott, både på nätet och i den fysiska världen. På sakerhetskollen.se har de samlat tips om digital säkerhet. Varför inte kolla om du är ”nätklok” på sidan: natklok.sakerhetskollen.se

polisen.se har givetvis en mängd information och hjälp om du blivit utsatt för brott, men även många tips och råd för att förebygga att du råkar illa ut. T ex följande med fokus på äldre: **polisen.se**/utsatt-for-brott/skydda-dig-mot-brott/aldre-och-funktionsnedsatta/forsok-inte-lura-mig

Nyhetsbrev erbjuds av NikkaSystems, Internetstiftelsen och Stöldskyddsföreningen. Du behöver bara ange din e-postadress på deras webbplats, så får du ett mejl med aktuella tips eller varningar om speciella brott som pågår för tillfället och hur du kan skydda dig mot dem.

Webbadressens olika delar

Var försiktig när du surfar, för det finns många elaka bovar ute på nätet!
Klicka inte på vad som helst. Lär dig att ”tolka” webbadressens olika delar.
Begrunda om adressen verkar seriös och stämmer med webbsidan du ska till!



En webbadress består av följande delar (trädstruktur):

https:// uppsala.seniornet.se/aktiviteter

https://	Systemkod	Styr till World Wide Web (behöver normalt ej anges)
uppsala	Subdomän	Ligger under domänen seniornet (förvaltas av SeniorNet Sweden)
seniornet	Domän	Registrerad av SNS (hos en av Internetstiftelsens återförsäljare)
se	Toppdomän	Sveriges toppdomän, som förvaltas av Internetstiftelsen
aktiviteter	Undersidor	Ligger under subdomänen uppsala (Förvaltas av SeniorNet Uppsala)

__Toppdomäner__ kan vara __nationella__ (se, dk, no, us etc) eller __generiska__ (com, net, org, info etc)

__OBS: Subdomäner__ och __Undersidor__ (inkl filer, bilder etc) kan domänförvaltaren döpa till vad som helst!

__MÄRK:__ Delarnas struktur (ordningsföljd) är ologisk, jmf med telefonnumer: __+46 18 123456 /789__

En mer __logisk ordningsföljd__ för en webbadress skulle vara: __se.seniornet.uppsala/aktiviteter__

”Webbadress-exempel”

Jämför följande webbadresser:

OK!

demo.bankid.com

nordea.se

telia.se

polisen.se

uppsala.seniornet.se

”Fejk”

demo.bankid.com.login-pbkdf2.info

nordea.se.login-to.io *(Toppdomän Brittiska Indinska oceanen)*

telia.com *(Generisk toppdomän för företag, föreningar m fl)*

polisen.to *(Bokstav 3 = versalt ”i”, toppdomän Tonga)*

uppsala.seniomet.me *(Bokstav rn = ”m”, toppd. Montenegro)*
uppsala.senior.net *(Generisk toppd. för nätverksorganisationer)*

Läs mer om och se lista över toppdomäner t ex på Internetstiftelsen.se eller Wikipedia

Bli säker till låg kostnad

Nikkasystems Poddavsnitt #154
Under årens gång har det getts många rekommendationer i ***Bli säker-podden***. Veckans avsnitt blickar tillbaka på några av rekommendationerna och försöker prioritera dem utifrån hur pass viktiga de är för en vanlig privatperson. Det ges många konkreta tips på hur du kan höja din IT-säkerhet utan att det kostar skjortan.

Poddens rekommendationerna delas in i tre nivåer:
1. Obligatoriskt
2. Rekommenderat
3. Valfritt (”nice”)

1. Använda en uppdaterad dator - Obligatoriskt.
Se till att alltid ha ett aktuellt operativsystem, som fortfarande får säkerhetsuppdateringar.

2. Använda en uppdaterad mobil - Rekommenderat
Inte lika viktigt att ha mobilen uppdaterad, eftersom det inte är så vanligt med attacker mot mobiler med äldre operativsystem. Kolla t ex med Bank-ID, om det tillåts för ditt operativsystemet, bör versionen vara ok.

3. Använda en uppdaterad router - Valfritt
Liten risk för attacker mot privatpersoner via en router, vilket gör att det inte är lika kritiskt för privatpersoner.

4. Använda en lösenordshanterare - Obligatoriskt
Inte rimligt att komma ihåg alla lösenord utantill, så en lösenordshanterare rekommenderas mycket starkt. Men det finns gratisalternativ som är helt ok.

5. Använda en VPN-tjänst - Valfritt
Rekommenderas främst av integritetsskäl eller för att kringgå geografiska begränsningar. Ur säkerhetssynpunkt tillför de normalt inte så mycket för privatpersoner.

6. Använda ett antivirusprogram på dator - Obligatoriskt
Microsoft Defender har blivit riktigt bra och ger ett fullgott skydd, betalversioner kan motiveras om du dessutom vill ha olika extra tjänster och funktioner. På Apple Mac finns obligatoriskt inbyggt virusskydd.

7. Använda tvåfaktorsautentisering - Obligatoriskt
Det finns flera metoder och välj alltid någon om det är möjligt. Framför allt på ditt e-postkonto, som du använder för lösenordsåterställning.

Nikka Systems Webbplats: nikkasystems.com
Lyssna på podden ”Bli säker till låg kostnad” (ca 13 min)**: Poddavsnitt #154**

19:00 Inledning
21:45 Uppdaterad dator
23:50 Uppdaterad mobil
25:30 Uppdaterad router
27:00 Lösenordshanterare
27:40 VPN-tjänst
28:35 Antivirus på dator
29:35 Tvåfaktorsautentisering