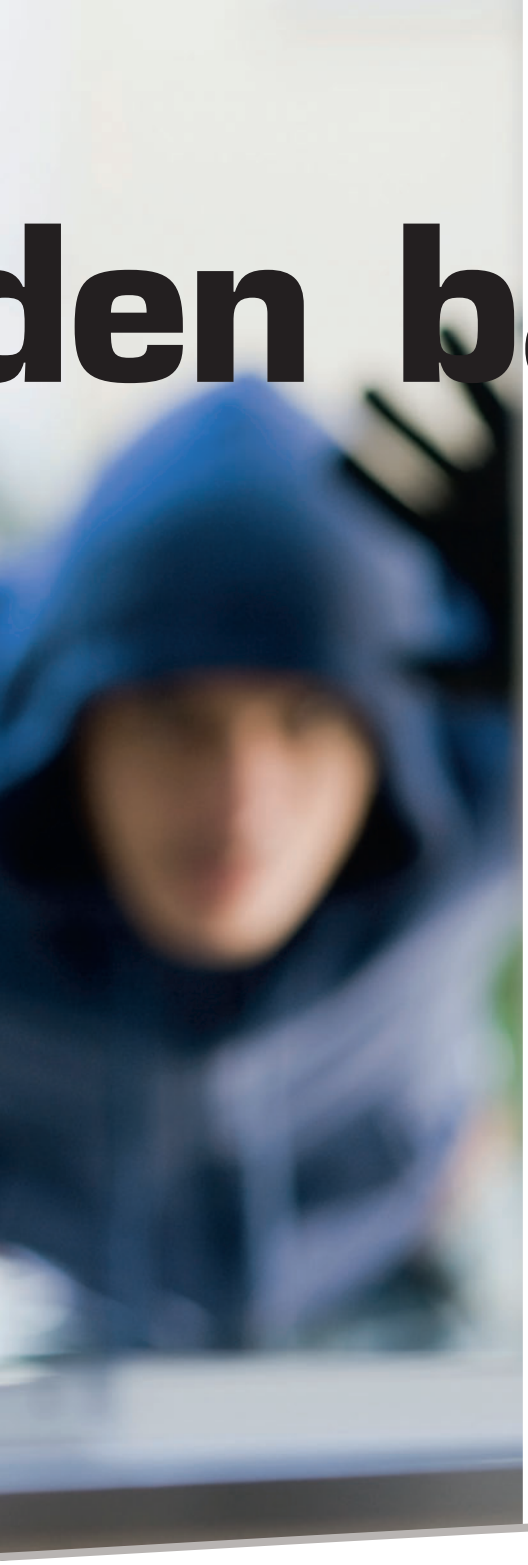
HELT SIKKER BÆRBAR

Pas godt på c

Den bærbare er smart og kan bruges overalt i huset, men henkastet på et tilfældigt bord er den også et oplagt mål for en langfingret tyv, der ikke lige har tid til at skrue fladskærmen ned fra væggen.



den bærbare

Der sælges fire gange så mange bærbare pc'er som stationære i Danmark. Den bærbare pc giver dig frihed og kan tages med, men gør samtidig din pc mere sårbar over for kaffe i tastaturet, ture på gulvet og tyveri.

I 2007 var hele 74,8 procent af computere solgt til private i Danmark en bærbar model. Der findes der ikke tyveristatistik specielt for computere her i landet, men amerikanske tal viser, at 1 ud af 10 bærbare bliver stjålet, og i Danmark er salget endnu større, så der er ingen grund til at tro, at der bliver stjålet væsentlig færre. Det er rart at kunne tage sin pc med sig, men du udsætter dig også for en større risiko, når computeren ikke står solidt plantet på skrivebordet. Lige fra du putter pc'en i tasken med fare for at tabe den, til du sidder i toget og sidemanden spilder en café latte ned i tastaturet. For slet ikke at tale om risikoen for, at computeren bliver stjålet fra din bil eller sommerhuset eller måske bare bliver væk eller forsinket i lufthavnen.

Mere end hardware

Hvis du har vigtige data liggende på computeren, er tabet af maskinen faktisk det mindste problem. Du mister nemlig også alle de dokumenter, koder, billeder og andet, som du kun har på den bærbare.

Det næste problem er, at tyven har fået adgang til alt, hvad du har liggende på computeren. Hvis tyven kan finde kodeord og nøglefiler til din mail og netbank, kan du risikere langt være kriminelle angreb end selve tyveriet af computeren. Det gælder altså med andre ord om at sikre, at tyven ikke kan få adgang til følsomme oplysninger.

Sådan sikrer du dig

I denne artikel giver vi en række helt konkrete råd til, hvordan du kan sikre dig mod uheld og tyveri af bærbare computere. Vi har opdelt rådene i, hvordan du sikrer dig derhjemme, på rejsen, og når du er fremme, samt hvordan du helt fysisk beskytter og vedligeholder maskinen, så den ikke bryder sammen. Mange af de programmer, vi omtaler, ligger på cd'en, så du selv kan sikre din bærbare computer.

Salg af computere i Danmark

		2006	2007
Erhverv	Stationær	**324,668** (46 %)	**322,350** (41 %)
	Bærbar	**383,601** (54 %)	**460,386** (59 %)
	Total	708,269	782,736
Privat	Stationær	**168,500** (34 %)	**140,900** (25 %)
	Bærbar	**324,100** (66 %)	**417,800** (75 %)
	Total	492,600	558,700

Kilde: IDC

Flere facts

I USA stjæles der en bærbar pc hvert 53. sekund
Kilde: Safeware Insurance

Der er en 1 ud af 10 risiko for, at din bærbare bliver stjålet i år
Kilde: Gartner Group

5 % af alle bærbare stjæles inden for de første 12 måneder
Kilde: Safeware Insurance

Tyveri er den anden-største grund til mistede pc'er/data
Kilde: Safeware Insurance

97 % af stjålne computere kommer aldrig tilbage
Kilde: FBI

50 % af alle virksomheder oplevede pc-tyveri i løbet af 2007
Kilde: FBI

Af Jesper Kjems. Foto: Imageclub.

Derhjemme

Når du bruger din bærbare hjemme, gælder de samme sikkerhedsforanstaltninger som for en stationær pc. Men du skal huske på, at det er nemmere for en tyv at stryge af sted med en komplet pc under armen, hvis du har en bærbar, og den er også mere udsat for små, men potentielt alvorlige uheld.

Beskyt med kodeord

Det er altid en god idé at have kodeord på den bærbare, så andre ikke ubesværet kan logge sig ind på dit Skrivebord. Gør det besværligt for tyven, så din mistede bærbare bare er et stykke hardware, der skal videresælges, og ikke en kilde til et mere omfattende tyveri. I tilfælde af tyveri vil en kodeordsbeskyttet computer typisk blive formateret, så den næste ejer kan lægge sit eget styresystem på computeren. Du mister stadig din pc, men lukker ikke op for yderligere angreb på bankkonto eller andet.
Du skal dog være opmærksom på, at tyven med det rigtige udstyr og edb-kunnen godt kan få adgang til filerne på harddisken, så vi anbefaler, at du gemmer vigtige dokumenter på for eksempel en USB-nøgle. Man kan også sætte et kodeord i computerens Bios eller på computerens harddisk, men ligesom et Windows-kodeord kan disse kodeord for det meste brydes forholdsvis let med de rette værktøjer. Du kan sætte et kodeord på computerens brugere under Brugere i Kontrolpanel.

Hold Windows opdateret

Uanset om du bruger *Vista* eller *XP*, er det vigtigt, at du sørger for at holde Windows opdateret. De fleste opdateringer kommer nemlig, når Microsoft finder et sikkerhedshul i styresystemet og derfor laver en programændring, der lukker hullet. Ligesom antivirussoftwaren holder sig selv opdateret, kan du under Sikkerhedscenter i Kontrolpanel sætte Windows til selv at hente og installere opdateringer.

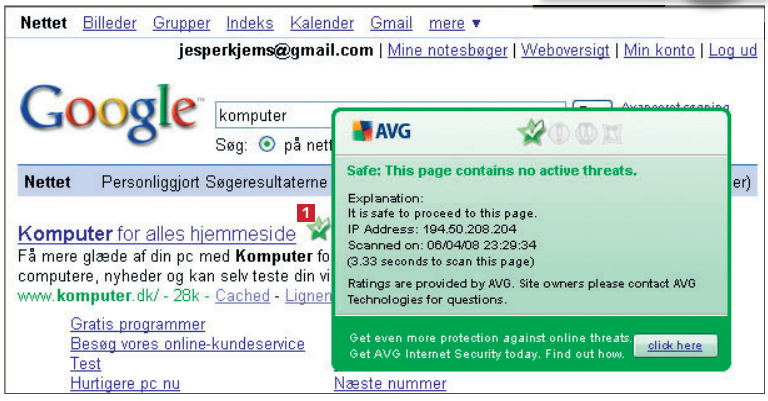
Giv ikke fortrolige informationer

Du kan også risikere at blive udsat for såkaldt phishing. Her fisker bagmanden efter oplysninger om dig – typisk passwords til netbank, PayPal eller eBay. Phishing foregår typisk via mail, hvor modtageren bliver narret til at videregive kreditkortnumre eller koder, fordi mailen ser ud til at komme fra et officielt sted. Hvis der er spamfilter på din mailboks, vil de fleste phishing-mails blive fanget her, men du kan aldrig være helt sikker. Det er derfor vigtigt, at du aldrig opgiver personlige koder i e-mails. Personlige koder er netop, som navnet antyder, personlige, og ikke engang firmaet, der har givet dig koden, bør du oplyse den til. Skulle der være problemer, kan firmaet blot sende en ny kode, som du selv kan ændre – så oplys derfor aldrig et password i en mail.

Brug altid antivirus

AVG Antivirus
LIGGER PÅ CD'EN

Det bør i dag være standard, at du har et ordentligt antivirusprogram liggende på enhver computer, der kan gå på internettet. Hvis du har din bærbare med rundt til forskellige netværk, er antivirusprogrammet endnu mere vigtigt, da virus her også kan komme fra lokalnetværket. Ofte er det ikke nok at bruge det antivirusprogram, der fulgte med, da du købte computeren. Nogle gange gælder det kun i 30 dage eller seks måneder, og desuden skal du ofte selv sørge for at få dit antivirusprogram opdateret. Opdateringen er meget vigtig, da programmet ellers ikke sikrer dig mod de nyeste virustrusler på nettet. På CD'en ligger en fuld version af det gratis og prisbelønnede *AVG Anti-Virus*, som kan sættes til at opdatere helt automatisk, uden at du skal foretage dig noget.



1 I nyeste version af *AVG Anti-Virus Free* bliver søgeresultaterne fra Google også tjekket igennem for trusler. Holder du musen hen over fluebenet 1, kan du se flere detaljer om sidens sikkerhed.

Gør det svært for tyven

Du skal ikke lade din bærbare computer stå fremme på et bord ved et vindue, når du er ude. Klap den sammen, og smid den i en låst skuffe, eller læg den et sted, hvor en tyv ikke gider kigge (et medlem af redaktionen bruger sin ovn, men det vil vi ikke anbefale, medmindre ovnen er meget ren og din hukommelse er helt i top – 200 grader varmluft er ikke sundt for en computer). Har du den på et bord eller i en dockingstation, så lås den fast med en kæde.

Kode på det trådløse netværk

Bruger du din bærbare hjemme, så er et trådløst netværk langt mere praktisk end et med ledninger, der begrænser den frihed, der ellers er en af den bærbare pc's store plusser. Men du bør sætte en kode på, så andre ikke får fri adgang til din netforbindelse. Det er specielt, hvis du har delte mapper på din computer, at du bør sikre dig. Men selv uden deling kan andre bruge din båndbredde – eventuelt til at hente ulovlige ting, der kan spores til dig.

Så vil du være helt sikker, skal du sætte en kode på netværket. Du skal bruge en såkaldt WPA-kryptering, når du vælger en kode i den trådløse router, da den mindre sikre WEB-kryptering i dag er forholdsvis let at bryde.

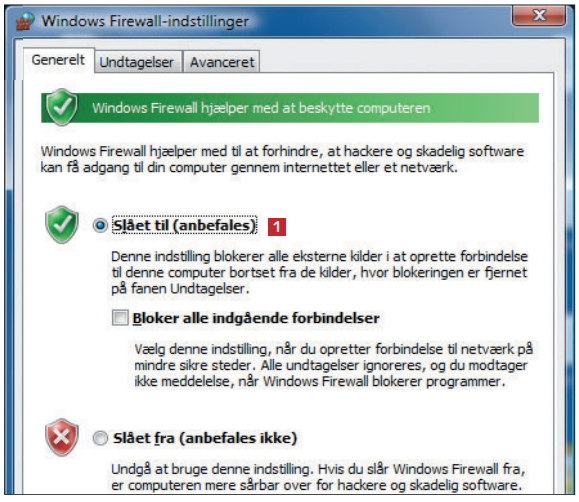
Nyere routere som denne Linksys har et system, hvor man med tryk på kun to knapper automatisk kan opsætte den supersikre WPA-kryptering, der holder andre ude fra dit trådløse netværk.

ZoneAlarm
LIGGER PÅ CD'EN

Beskyt den bærbare mod angreb udefra

En firewall holder øje med al trafik, der kommer ind og ud af computeren. Den sørger altså for, at kun trafik, du giver tilladelse, får lov at passere. På den måde sikrer du dig, at der på computeren ikke kan installeres små programmer, der i baggrunden sender oplysninger ud på nettet, eksempelvis om hvilke websider du besøger.

Når din firewall er slået til, vil et lille vindue dukke op på skærmen, når et program forsøger at få adgang til nettet første gang. Disse advarsler skal du kun svare ja til, hvis du vil give programmet adgang – har du for eksempel lige installeret *Skype*, skal du svare ja, inden *Skype* kan logge på. Men hvis advarslen kommer, uden at du lige har installeret et program, og hvis du ikke kender navnet på den fil, der vil have netadgang, skal du svare nej. I Sikkerhedscenter i Kontrolpanel kan du slå den indbyggede firewall til. Du kan også vælge den noget mere avancerede *ZoneAlarm*, som er på CD'en.



1 Under **Kontrolpanel** finder du **Windows Firewall**, som skal være slået til 1. Du kan også benytte *ZoneAlarm* fra vores Sikkerhedscenter på CD'en.

Foto: © iStockphoto

På rejsen

Når du rejser med din bærbare, er den ekstra udsat, da du let kan tabe den, spilde kaffe i den eller få den stjålet. Du bruger måske trådløse netværk, du ikke kender, eller pc'en bliver en del af forsinket bagage. Kun omtanke kan forebygge helt, men med vores råd bliver et eventuelt tab ikke en katastrofe.

Gem det vigtige af vejen

Det vigtigste råd før rejsen er at få sikret al data, der kan misbruges, eller som du ikke kan undvære. Hvis du kopierer data til en USB-nøgle eller ekstern harddisk, kan du stadig arbejde videre på en anden computer, hvis der sker noget med den bærbare. Problemet er selvfølgelig, at en ekstern harddisk ofte ender i tasken med computeren, så derfor anbefaler vi en fysik undseelig USB-nøgle med høj kapacitet, og som opbevares et andet sted. Det er rigeligt til at gemme hele din dokumentmappe, medmindre du medbringer familiens video- eller billedsamling. Og husk så, at USB-nøglen selvfølgelig også kan blive stjålet eller tabt, så tag ofte backup af nøglens indhold. Det er ikke kun dokumenter, der bør gemmes af vejen. E-mails, nøglefiler til netbanken og andre data, der vil kunne misbruges, bør du også gemme på USB-nøglen.

Mange USB-nøgler bliver leveret med indbygget kryptering på en chip, hvilket er det mest sikre. Men softwarekryptering er rigeligt for folk, der ikke er hemmelige agenter.

Gem det vigtige på nettet

En mulighed er slet ikke at medbringe vigtige filer på den bærbare, men i stedet have alt liggende på nettet. Flere firmaer tilbyder online-plads, som du har adgang til præcis som på en ekstra harddisk. Et online-drev har den fordel, at du kan hente de dokumenter, du skal bruge, og så afbryde internetforbindelsen, mens du arbejder med dokumenterne.

www.xdrive.com

www.mozy.com

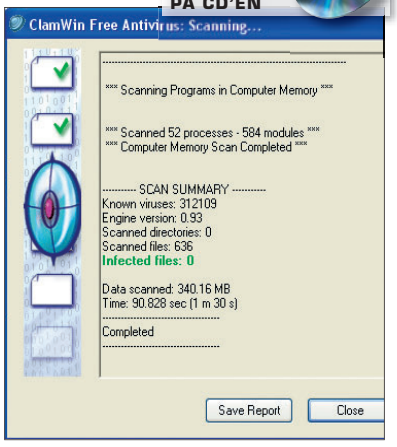
I *Google Docs* kan du lave simpel tekstbehandling, regneark og præsentationer direkte i din browser. Og så snart du logger af, kan andre ikke læse dine dokumenter uden det rette kodeord. Google har netop lanceret muligheden for, at du også kan redigere dine dokumenter uden at være på nettet og så synkronisere ændringerne næste gang, du er online.

http://docs.google.com

Undgå virus – på USB-nøglen

ClamWin Portable
LIGGER PÅ CD'EN

Når du har både programmer og vigtige dokumenter liggende på din USB-nøgle, er det vigtigt, at du ikke får virus på nøglen. Bruger du USB-nøglen på andre computere, kan du også risikere at få en virus med, som så installeres på hjemmecomputeren, næste gang du bruger USB-nøglen her. Du kan derfor installere *ClamWin Portable* fra CD'en direkte på din USB-nøgle. Det er et antivirusprogram, der tjekker filer på USB-nøglen og opdateres via nettet som et normalt antivirusprogram.



Hvem kan læse din chat?

Pidgin Portable
LIGGER PÅ CD'EN

Når du chatter med såkaldte instant messaging-programmer som *Messenger*, gemmes din dialog ofte i en logfil. Og hvis du engang har fået koden til fx din mors webmail for at hjælpe hende med opsætningen, kan du risikere, at denne samtale kan læses af enhver, der får fingrene i din bærbare. Du kan slå alle logfiler fra inde i *Messengers* indstillinger, men du kan også i stedet installere en såkaldt universalmessenger på din USB-nøgle. Med den kan du chatte på tværs af alle de mest benyttede programmer som *Messenger*, *Yahoo!*, *ICQ*, *Google Talk* og også det tekstbaserede IRC. *Pidgin Portable* ligger på CD 'en.

Gem kun kodeord i hovedet

Rigtig mange hjemmesider og programmer kræver i dag login, og mange tilbyder at huske dit kodeord for dig. Det gør livet lettere, men et password på computeren er som en nøgle under dørmåtten. Alle andre kan så også logge sig på uden kodeord, hvis den bærbare skulle blive stjålet. Lad derfor som udgangspunkt være med at logge automatisk ind på forskellige hjemmesider, hvis de på nogen måde kan indeholde fortrolige eller personlige oplysninger. Andre sider som for eksempel et diskussionsforum, en avis eller en side, der samler dine foretrukne webadresser, udgør ingen fare.

Pas på andres netværk

Når du går på nettet i toget, lufthavnen eller på cafeen, skal du være ekstra påpasselig. Her logger du på et fremmed trådløst netværk, hvor du ikke ved, hvem der ellers er logget på.

- Pas på delte mapper. Hvis du har delte mapper på din computer, kan andre brugere på netværket se og også slette eller ændre filer i disse mapper, hvis du har givet adgang til det. Du kan se dine delte mapper under netværkssteder, og du ændrer delingsrettighederne ved at højreklikke på en mappe og vælge Deling.
- Hav et opdateret antivirusprogram på computeren.
- Brug en firewall. Husk at svare nej, hvis din firewall beder om adgang til noget, du ikke kender til, mens du er på et offentligt netværk.
- Sig aldrig ja til at installere software, du ikke har bedt om.

Fingeraftrykslæser

Det giver selvfølgelig lidt mere bøvl at skulle indtaste koden til både *Skype* og mailprogrammet, hver gang du tænder computeren. På mange nyere bærbare computere er der derfor indbygget fingeraftrykslæser, som gør det muligt at logge ind blot ved at køre fingeren hen over en lille plade. Du kan også købe en fingeraftrykslæser til USB-stikket for få hundrede kroner (fx fra APC). På den måde er det altså kun dit helt personlige fingeraftryk, der giver adgang. Med hvisse produkter kan du også låse adgang til computeren og enkelte mapper, så kun dit fingeraftryk giver adgang her.

Engang var det science fiction, men nu er der fingeraftrykslæsere i en del bærbare, og en USB-version kan købes for få hundrede kroner. For de ekstra sikre er der scannere, der kigger dig dybt i øjnene, på vej.

Skriv sikkert

Hvis du bruger et e-mail-program som *Outlook Express* eller *Windows Mail* på din bærbare pc, har du to problemer, hvis den bliver stjålet. For det første har tyven fri adgang til hele dit mailarkiv, hvor han måske kan finde mails, du har fået tilsendt med logins til forskellige hjemmesider og tjenester på nettet. For det andet vil du ikke selv kunne finde dine gamle mails på en ny pc, medmindre du har gemt en kopi af dine mails på serveren eller taget backup af mailfilerne. Det problem kan løses på flere måder, og her er et bud både til den e-mail-konto, du har fået af din internetudbyder, og til et alternativ:

Mozilla Thunderbird
LIGGER PÅ CD'EN

Kør mailprogrammet fra USB

Mozilla Thunderbird er et mailprogram, der findes i en bærbar udgave, som du kan installere direkte på din USB-nøgle. På den måde henter du dine mails på en hvilken som helst computer direkte ned på USB-nøglen, så du ikke efterlader mailoplysninger på computerens harddisk. Du kan altså kun tjekke mails og læse dit mailarkiv, når USB-nøglen er sat i. Husk dog, at det er vigtigt at kryptere din USB-nøgle med alle dine mails. Det er også en god idé, at du ikke vælger automatisk login.

Brug en gratis webmail

En løsning på første problem er at bruge en webmail som eksempelvis Gmail eller Hotmail, hvor du læser og skriver dine mails direkte på nettet og altså ikke gemmer noget som helst på computeren – hvis du allerede har en mailkonto hos din internetudbyder, findes der sandsynligvis også en webadgang til din mail (læs vejledningen fra udbyderen).
http://gmail.google.com

Foto: © iStockphoto

Når du er fremme

Når du har fået den bærbare op at køre i sommerhuset, campingvognen eller på hotellet, er der også et par gode tips til at sikre dine data og maskinen.

Krypter hele harddisken

I nogle udgaver af *Vista* er der et program ved navn *BitLocker*, der kan kryptere alle data på hele harddisken. Det er temmelig teknisk at få sat op og gør det også ekstra problematisk at miste sit kodeord eller de såkaldte nøglefiler, da du i værste fald kan være nødt til at formatere harddisken. Kryptering af hele harddisken er derfor primært til firmaer, hvor de ansatte har personfølsomme oplysninger eller forretningshemmeligheder på pc'en. *BitLocker* findes da heller ikke i *Vista Home*-udgaverne.

Læg en virus på din egen computer

Virus, der gemmer sig dybt i ens system, vil man normalt undgå. Men samme teknik kan også bruges til noget fornuftigt. Når computeren bliver logget på et fremmed netværk, sender et sporingsprogram diskret en mail til dig med oplysninger om IP-adresse, og hvad programmet ellers kan opsnuse om netværket. Nogle af sporingsprogrammerne kan sågar tage et billede, når der er museaktivitet, hvis den bærbare har indbygget webkamera. Billedet sendes så til din mailadresse og viser måske et fint portræt af tyven, som du kan give til politiet. IP-adressen kan normalt ikke fortælle andet, end hvilken internetudbyder tyven kobler sig på nettet hos. Men hvis du kan få politiet på sagen, og de tager IP-adressen og en dommerkendelse med til internetudbyderen, skal denne oplyse den fysiske adresse.

www.trackion.com

Spor den bærbare med GPS

Det virker umiddelbart oplagt at installere en lille GPS-modtager, som sender oplysninger om, hvor den bærbare befinder sig. Men sådanne dimser er både dyre og ikke særlig udbredte. GPS kræver nemlig en forholdsvis direkte adgang til satellitterne og vil derfor ikke virke inde i huse. Et andet problem er, at det er svært at få plads til en GPS inde i en i forvejen pakket bærbar pc, og putter man den i tasken, så kan tyven blot fjerne senderen, hvis han opdager den.

Et GPS-sporingssæt som dette fra BrickHouse Security er bedst til den dyre bil. Det koster nemlig over 2.500 kroner, og den lille antenne er ikke så god indendørs, hvor den bærbare oftest vil befinde sig.

Gem dine bogmærker ét sted

Det er nok ikke den store katastrofe, hvis en tyv får adgang til dine bogmærker. Men det kan være irriterende, hvis du selv skal finde alle de gode hjemmesider igen. Med programmet *Zinkmo* kan du få synkroniseret dine bogmærker, så du altid har de samme på dine forskellige computere og også i forskellige browsere. Programmet kræver, at du registrerer dig på producentens hjemmeside. Herefter skal du installere et lille stykke software, som sørger for at synkronisere dine bogmærker med en server. På den måde sikrer du altså ikke kun, at dine bogmærker ikke går tabt – du vil også altid se de samme bogmærker på alle dine computere.

www.zinkmo.com

Zinkmo
LIGGER PÅ CD'EN

Zinkmo samler praktisk alle bogmærker et sted, der ikke kun kan ses fra én pc.

Mærk den bærbare

Operation Mærkning er et samarbejde mellem Det Kriminalpræventive Råd og forsikringsselskaberne. Det skal gøre det sværere for indbrudstyve at komme af med fx elektronik. Du kan mærke computeren med navn og adresse med en lille ridsepen. Du kan også bruge en brænder eller en elektrisk minisliber, men det kræver en lidt bedre teknik, hvis du ikke vil have grimme dybe mærker i din bærbare pc. På nedenstående side kan du bestille et gratis ridsesæt med bogstavskabelon. Der medfølger også klistermærker, så tyven ved, at alt er mærket.

www.stopindbrud.dk

Med en lille ridsepen som denne kan man ridse ejerens navn så dybt ind i den bærbare, at det ikke lige lader sig fjerne. Som stelnummeret på en bil er det svært at komme uden om.

Pas på mobilregningen

Hvis du bruger mobilnettet til internet, skal du ofte betale pr. megabyte. Husk derfor at få slået automatiske opdateringer fra. Det gælder både Windows, opdatering af antivirus og automatisk opdatering af andre programmer. Men også programmer, der automatisk kobler sig på nettet, kan give dig en ekstraregning – for eksempel *Skype* og e-mail. Specielt med de nye 3G-netværk kan det blive en dyr fornøjelse. Er du i udlandet, kan en MB koste 100 kroner, og så kan regningen hurtigt løbe op, når det kun tager få minutter at hente en opdatering på 22 MB.

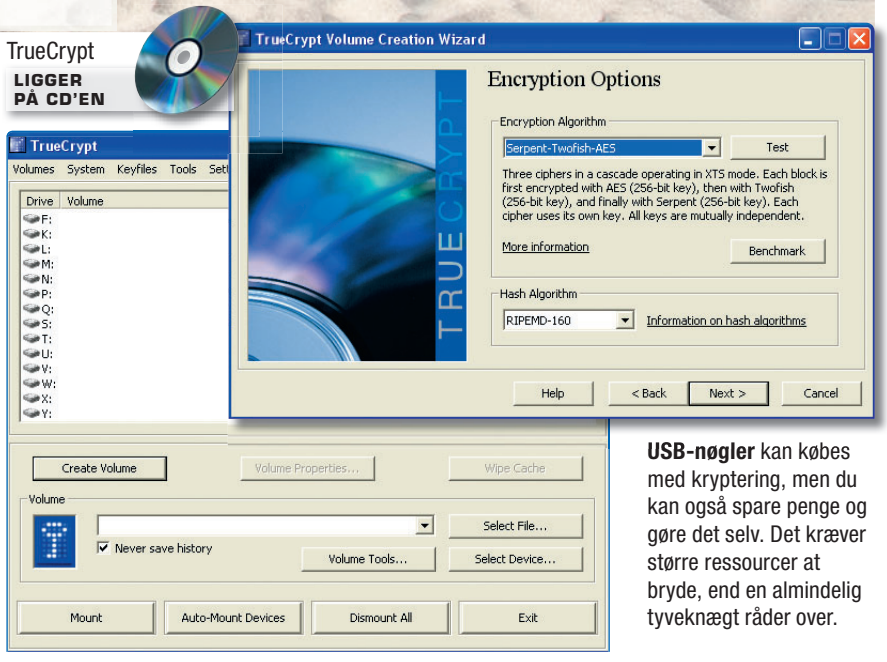
Krypter enkelte mapper

I både *Vista* og *XP* er der indbygget mulighed for at kryptere enkelte mapper, så indholdet kun kan ses, hvis den rigtige bruger er logget på. Man skal være logget på med kodeord, og kryptering virker desværre ikke i *XP Home* eller *Vista Home Basic*, men her kan du i stedet bruge programmet *TrueCrypt*, som ligger på CD'en. Når du krypterer dine filer, er der et par vigtige forholdsregler, der er værd at følge. Det er ekstra vigtigt med en backup af filerne, da du heller ikke selv vil kunne åbne de krypterede filer, hvis du har glemt dit password. Filer i mappen bliver fremover grønne, så du kan se, at de er krypterede.

Krypter USB-nøglen

Skulle du miste din USB-nøgle, er det en god idé at have den krypteret, så man kun kan læse indholdet ved at indtaste det rigtige kodeord. Med programmet *TrueCrypt*, som ligger på CD'en, kan du kryptere hele din USB-nøgle, så man kun kan få adgang til indholdet ved at taste det rigtige kodeord. Når først kodeordet er indtastet, fungerer nøglen præcis som en almindelig nøgle, hvor du kan gemme og læse dokumenter samt afvikle programmer. Ingen kryptering kan give 100 procent sikkerhed, men med *TrueCrypt* vil det tage meget lang tid og store anstrengelser at få knækket krypteringen til dine data.

TrueCrypt
LIGGER PÅ CD'EN



USB-nøgler kan købes med kryptering, men du kan også spare penge og gøre det selv. Det kræver større ressourcer at bryde, end en almindelig tyveknægt råder over.

Foto: © iStockphoto

I det fri

Når du har fået den bærbare op at køre i sommerhuset, campingvognen eller på hotellet, er der også et par gode tips til at sikre dine data og maskinen.

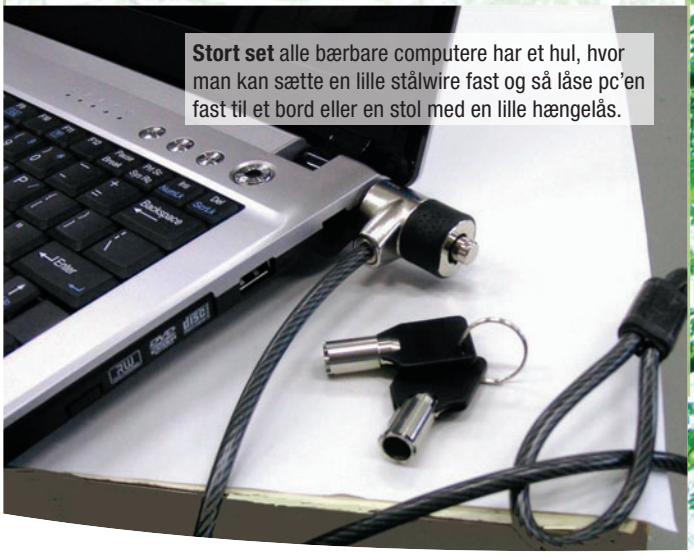
Varme lårbasser

Mange bærbare bliver meget varme under brug. Pas derfor på med at sidde med maskinen på lårene. Dels risikerer du brændemærker på bukserne, dels risikerer du, at den bærbare overopheder, fordi dine lår spærrer for den blæser, der er placeret i bunden af den bærbare computer. Hvis du gerne vil kunne sidde med den bærbare på lårene, kan du investere i en USB-drevet kølerplade, der sørger for kold luft til både lår og computer.

Belkins køleplade koster 159 kroner og beskytter både din bærbar og dine lår.

Lås computeren fast

På langt de fleste bærbare er der et hul med et lille kædesymbol. I disse huller kan du fastgøre en såkaldt Kensington-lås. Kensington var det firma, der opfandt systemet, men mange andre producenter laver i dag låse, der kan bruges. Låsen findes i mange varianter, men kan fx være en stålwire med kombinationslås, der kan fastgøres til bordet eller væggen. Som med de fleste låse er en lås til den bærbare ikke mere sikker, end at tyven kan klippe låsen over, hvis han da ellers lige har værktøj med. Men en lås sikrer mod en person, der måske blot bliver tyv, fordi han øjner en chance. Låsen sender også et signal om, at den bærbare er sikret, så tyven forhåbentlig går videre til et lettere mål.



Stort set alle bærbare computere har et hul, hvor man kan sætte en lille stålwire fast og så låse pc'en fast til et bord eller en stol med en lille hængelås.

Sluk computeren og vent

Du sidder i toget med den bærbare og opdager pludselig, at du skal af ved næste station. Her er det oplagt blot at klappe låget sammen og så ellers få proppet pc'en ned i tasken i en fart. Det er bare ikke særlig smart. Dels kan computeren blive meget varm nede i tasken, dels kan du miste data, hvis computeren får et hårdt stød, mens der skrives på harddisken. I det hele taget skal du være varsom med at flytte rundt på en tændt bærbar computer.

Hold den bærbare ren

Når du tager computeren med rundt, bliver den hurtigere beskidt end derhjemme. Sørg derfor ofte for at aftørre tastaturet med en fugtig klud og skærmen med renseservietter beregnet til fladskærme. Endnu mere vigtigt er det, at du holder øje med computerens blæserhuller, der sørger for at holde temperaturen inde i computeren nede. Disse huller må aldrig blive stoppet til med støv eller på anden måde blive blokeret, da du dermed risikerer, at computeren bliver for varm og i værste fald brænder sammen. Rens blæserhullerne med en støvsuger og klud, og brug evt. en vatpind, hvis støvet sidder fast.

En taske skal først og fremmest beskytte din bærbare. En af de dyre tasker signalerer måske nok, at du er med på moden, men også, at her er sandsynligvis en dyr bærbar, der er værd at rende med.

En god computertaske

En god computertaske er først og fremmest en taske, der kan beskytte din computer mod slag, regn og støv. Men inden du render ud og bruger flere tusinde kroner på en moderigtig Crumbler-taske, skal du også tænke på, hvad tasken fortæller tyven. En ultradyr computertaske signalerer nemlig en ultradyr bærbar og dermed et oplagt emne for tyveknægte. I stedet kan du overveje en taske, der slet ikke ligner en computertaske – eksempelvis har mange studerende en rygsæk til computeren, ligesom der findes dametasker specielt designet til også at kunne passe på din computer.

Fjern udstyr inden du pakker sammen

Det er lynhurtigt lige at proppe den bærbare i tasken og lade stik til strømforsyning, mus, USB-nøgle eller harddisk sidde i. Men det kan hurtigt blive en rigtig dårlig idé, da disse stik let kan knække, når computeren bevæger sig rundt nede i tasken. Fjern derfor alt udstyr fra computeren, inden du pakker den sammen.

Tab ikke computeren

Det er svært på forhånd at beslutte sig for ikke at tabe noget, men der er visse forholdsregler du kan tage. Enkelte bærbare har indbygget en mekanisme, der får harddiskens læser til at slippe skiven, hvis computeren er på vej mod gulvet. Og ellers gælder det om at være yderst forsigtig, hvis du flytter på en tændt computer, og helst lukke computeren helt ned inden.

Når skaden er sket

Selv om du har sikret alle dine vigtige filer, står du stadig uden pc, hvis den bærbare forsvinder eller går i stykker. Her er nogle fakta, som er gode at kende, inden du beslutter dig for, om du skal købe dig fattig i butikkernes tilbud om ekstra forsikring af den bærbare.

- For det første skal du huske, at du ifølge købeloven har to års reklamationsret. Inden for de første seks måneder gælder den såkaldte formodningsregel, hvor man som udgangspunkt formoder, at en fejl har været i produktet fra starten, og kunden derfor har krav på en ombytning af varen.

- Købeloven hjælper kun ved fejl på produktet. Tyveri, brand og andre uheld skal dækkes af en forsikring. Mange af disse ting vil være dækket af en almindelig familieforsikring. Her skal du dog undersøge, både hvad din forsikring dækker, hvor stor selvrisikoen er, og hvordan forsikringsselskabet vurderer værdien af din computer i forhold til alder. Desuden dækker en familieforsikring ikke nødvendigvis tyveri eller andre skader i udlandet og sandsynligvis heller ikke dine egne uheld.

- I udlandet dækker din nuværende rejseforsikring muligvis, og igen skal du tjekke reglerne i policen for bærbare computere samt selvrisikoen.

- Rejser du meget og har en dyr computer, kan forretningens totalforsikring være en mulighed. Disse fås også i forskellige udgaver, men den vigtigste forskel fra købeloven og de almindelige familieforsikringer er, at du her kan betale dig fra også at få dækket de dumme uheld som kaffe i tastaturet, og hvis du taber computeren på gulvet. Nogle af totalforsikringerne har også ingen eller lav selvrisiko, ligesom nogle giver dig det fulde beløb retur ved tyveri. Men disse servicer betaler du selvfølgelig en høj pris for, så vurder altid, om det bedre kan betale sig selv at købe en ny maskine.

www.forbrugerraadet.dk/raad/forbruger/alle/kobelov/

Foto: © iStockphoto