

Hvad nu hvis din bærbare computer blev stjålet?

✖ Hvis du mister din bærbare computer – fx ved tyveri – hvad er konsekvenserne så?

Problemerne kan være nogenlunde de samme, hvis det havde været en smartphone eller en tablet, men her er fokus i hovedsagen på computeren.

Forsikring

Indboforsikringen dækker ved indbrud, men der er ofte selvrisko på mindst 2.000,-. Dertil kommer, at elektronisk grej nedskrives hurtigt.

Backup

Hvis du har backup, så er den del af det jo ikke noget problem – men her har de fleste vist dårlig samvittighed.

Bagklog: Backup

✖ En nem måde at lave backup på er at bruge [Dropbox](#) eller [Onedrive](#) eller lignende.

Hvis du sørger for at lægge dine data i en speciel mappe (og evt. undermapper), vil indholdet automatisk blive synkroniseret op på nettet.

Data, der fylder meget (musik, video og fotos): Det kan være nødvendigt at lave backup af disse mediefiler på anden vis – fx på en lokal harddisk.

Ikke rigtig backup

Bemærk, at de nævnte tjenester *synkroniserer* – de laver ikke backup. Synkroniseringen indebærer, at hvis en fil eller en mappe slettes et sted, så slettes den også alle andre steder. Heldigvis gemmer både Dropbox og SkyDrive i et vist omfang slettede filer, så man kan logge ind på nettet og genskabe dem.

Følsomme data

Der ligger ofte følsomme data på computeren, og der er jo en risiko for, at de bliver misbrugt, hvis computeren falder i forkerte hænder.

Det kan fx dreje sig om:

Hvad nu hvis din bærbare computer blev stjålet?

- Adgangskoder
- Personlige dokumenter
- Personlige oplysninger
- Kortoplysninger

Adgangskoder



Undlad "Forbliv logget ind" på den bærbare.

Dine adgangskoder er udsatte på flere måder.

Dels kan det være, du har dem liggende i et dokument, og dels kan det være, at du lader browseren huske dem. I begge tilfælde kan uvedkommende få adgang til din webmail, din Facebook osv.

Din netbank kræver jo NemID, og den har du jo på et plastic-kort, så her burde der ikke være problemer.

Hvis du bruger en FTP-klient, er der formentlig også problemer her – for det er de færreste, der beskytter FTP-koderne.

Personlige dokumenter

Alle de dokumenter, der ligger på din computer, er der normalt uhindret adgang til, for de ligger jo blot i nogle mapper.

Hvis du bruger en mailklient som fx Outlook eller Thunderbird, er der også fri adgang til dine mails.

Bruger du webmail, er der problemer, hvis browseren husker din adgangskode.



Personlige oplysninger

Der kan også nemt ligge personlige oplysninger på computeren. Der ligger måske PDF'er fra banken eller fra skat, og her står dit personnummer fx på.

Hvad nu hvis din bærbare computer blev stjålet?

Kortoplysninger

Handler du på nettet, har du måske skrevet dine kortoplysninger ned i en fil, fordi du ikke gider finde kortet frem, hver gang du handler.

Med dine kortoplysninger kan man købe varer på nettet.

Bagklog: Følsomme data

Man skal være ekstra forsigtig med bærbare enheder, fordi de er nemme at stjæle og nemme at glemme rundt omkring. En stationær pc er mindre udsat.

Beskyt enheden med adgangskode!

For det første skal du sætte adgangskode på din computer, tablet eller smartphone. Den slags beskyttelse er ikke nødvendigvis særlig effektiv, men det er bedre end ingenting. Og det kan jo betyde, at tyven blot vælger at resette hele maskinen og derfor *ikke* begynder at snage i dine data.

Bagklog: Adgangskoder:

Lad ikke browseren huske dine koder. Det nemmeste er at bruge fx [LastPass](#) eller [Dashlane](#). [Læs om at passe op adgangskoderne her](#).

Bagklog: Personlige dokumenter og personlige oplysninger

Selvom du bruger backup, betyder det jo ikke at dine data er beskyttet mod andres snagen. Apparatets generelle adgangskode giver en vis beskyttelse, men sikre er dine data ikke.

Data i skyen

Her er der flere muligheder: Enten kan du lægge dine data i *skyen* – fx på *Google Drev*. Og så skal du undlade at have dine data lokalt.

Kryptering

En anden mulighed er, at du *krypterer* dine data. Det kan gøres på flere måder:

- En krypteret container
Her kan du oprette en stor krypteret fil, som kan åbnes med et kodeord. Når den er åben, bliver den til et virtuelt drev, som kan indeholde filer og mapper. Gratisprogrammet *TrueCrypt* er en glimrende løsning.
TrueCrypt-metoden passer ikke så godt til brug sammen med fx Dropbox. For

Hvad nu hvis din bærbare computer blev stjålet?

det første fordi det er en meget stor fil, der skal synkroniseres, og for det andet fordi TrueCrypt-filen faktisk ikke ændres, selvom indholdet ændres – og derfor bliver den ikke synkroniseret af fx DropBox.

- Kryptering af enkeltfiler

Med fx AxCrypt kan du kryptere følsomme filer enkeltvis, og det er måske den smarteste løsning, fordi den passer godt med fx Dropbox og SkyDrive. AxCrypt er også gratis.

Bagklog: Kortoplysninger

Undlad at gemme dem på computeren. Og hvis du alligevel vil gemme dem der, så læg dem i en krypteret fil eller i en adgangskodehusker som fx LastPass.

Specielle apps til smartphones og tablets

Der findes faktisk apps til både iOS (iPad/iPhone) og Android, som kan lade dig kontrollere din bortkomne enhed. Der er en masse muligheder – fx kan enheden findes via Google Maps og den kan få slettet indholdet. I AppStore kan du søge på *Find my iPad / Find my iPhone*. I Google Play kan du fx se efter *Android Lost* eller *Wheres My Droid*.

Skulle uheldet ske

Skulle du miste den bærbare, og du ikke har sikret dig, kan du måske bruge nogle af disse tips, for at begrænse skaden.

- Adgangskoder
Skift alle de adgangskoder, du kan komme i tanker om. Husk også evt. FTP-koder.
- Data i Dropbox (eller lignende)
Har du data i Dropbox, så download dem hurtigst muligt, og slet derefter indholdet i Dropbox. Hvis du undlader at skifte adgangskode på Dropbox, vil din stjålne computer synkronisere sletningen første gang den kommer på nettet – og Dropbox-indholdet vil derfor blive slettet. Det er jo smart. Logger du ind på Dropbox.com, kan du se om din stjålne computer kommer på nettet.
- Vær bedre forberedt, hvis det sker igen
– følg nogle af de bagkloge råd ovenfor. 

Hvad nu hvis din bærbare computer blev stjålet?

- [Share on Facebook \(Opens in new window\) Facebook](#)
- [Share on Pinterest \(Opens in new window\) Pinterest](#)