



FE



**Brug USB-stikket  
- men med omtanke**

## Brug USB-stikket - men med omtanke

USB-lagringsmedier er blevet en meget populær hardware, og ligesom en stor del af befolkningen, bruger forsvarrets ansatte teknologien, både i hjemmet og på arbejdspladsen.

Brugen af USB-stikket er en nem måde at skabe forbindelse mellem medier. USB-teknologien gør det muligt at overføre informationer på en let og hurtig måde.

Computere får ofte tilsluttet lagringsmedier i forbindelse med en opdatering eller overførsel af forskellige slags informationer (tekst, billeder, lydfiler etc.).

Denne folder har til formål at øge din sikkerhedsbevidsthed, ikke bare når du bruger USB-stikket på din arbejdscomputer, men også på din hjemmecomputer. Folderen retter sig især mod brugen af USB-nøgler (memory sticks).

### Brug af USB-stikket

USB-medier omfatter alle former for ekstern hukommelse, som kan tilsluttes computere ved hjælp af USB-teknologi. Dette kan fx være:

- USB-nøgler
- Eksterne harddiske
- Digitale kameraer
- Mobiltelefoner
- GPS-navigatører
- iPods
- Diverse MP3/4-afspillere.

Fælles for disse er, at de kan anvendes til, frivilligt eller ufrivilligt, at overføre data fra et system til et andet, da de indeholder en eller anden form for hukommelse (harddisk, SD-kort, micro-SD, CompactFlash, Solid State m.fl.). En anden fællesnævner er, at de har brug for at blive tilsluttet en computer for at blive opdateret, fyldt eller tømt.

## Hvorfor skal du være forsigtig?

Her er tre gode grunde:

### 1. For at beskytte din computer og dine USB-medier

Når du benytter USB-medier og tilslutter dem en computer, risikerer du, at enten computeren eller dit USB-medie bliver inficeret af virus. Dermed kan du blive udsat for angreb, bl.a. på din webbank. Din computer kan blive misbrugt som en del af et netværk, hvor andre kan tage kontrol over din computer og bruge den til at sende virus eller andet videre i dit navn (botnetværk).

### 2. For at beskytte forsvarrets netværk

Forsvaret har fastsat regler for brug af USB-medier (nøgler). Overholder du ikke disse regler, er der risiko for, at forsvarrets netværk inficeres, hvilket kan påvirke evnen til at anvende disse. Dette kan i sidste ende få indflydelse på de operationer, som forsvarrets personel er indsat i. (Se reglerne i Forsvarskommandobestemmelse 358-1 Kap. 6 om informationssikkerhed).

### 3. For at beskytte data

Ved en omhyggelig omgang med USB-medier og overholdelse af de gældende regler, kan du og forsvaret undgå at få inficeret netværk og computere og dermed også en mulig kompromittering af data (herunder personlige/klassificerede data).

## Kan du forbedre sikkerheden?

Ja, men det kræver, at du bruger USB-medierne med omtanke.

Grundlæggende er det vigtigt at huske på, at dine private medier ikke må tilsluttes forsvarrets systemer og omvendt. Hvis alle overholder det, nedsættes risikoen for, at forsvarrets systemer bliver ramt af virus.

Det er vigtigt at du, når du står med et USB-medie i hånden og vil tilslutte den en computer, tænker over, om en evt. klassifikation stemmer overens mellem de to systemer.

Gør de ikke det, og har du brug for at få overført data fra et lavere klassificeret system til et højere klassificeret system, så kontakt din administrator.

Når du downloader data til dit medie, så udsætter du også systemet for en risiko. Du bør undersøge, om du kan have tillid til den hjemmeside, du vil skabe forbindelse til, og de data, du vil downloade. Ofte kan skadelige data gemme sig bag billeder eller andre filer, som kan virke uskyldige.

Begræns mængden af data, du har på USB-mediet, og ryd jævnligt op.

Som nævnt har USB-medier brug for at blive tilsluttet en computer for at blive opdateret, fyldt eller tømt. Dermed får det også betydning, hvordan sikkerhedsindstillingerne på din computer er sat. Husk at opdatere de programmer, du har på din computer. Sørg for at holde din antivirussoftware opdateret, og brug evt. også en firewall.

## Gode råd

- Anvend aldrig USB-enheder, som du ikke kender tilhørsforholdet til.
- Udlån aldrig USB-enheder, som du ejer eller har ansvaret for.
- Afmærk altid USB-enhederne med den rette klassifikation.
- Husk, at reglerne for registrering af klassificerede oplysninger, der medbringes uden for tjenestestedet, gælder, uanset om de medbringes i hard copy eller elektronisk.
- Anvend kryptering, så vidt det er muligt. Til privat brug kan fx anvendes et gratis produkt (kan findes på internettet).
- Scan jævnligt såvel tjenstlige som private nøgler for virus.
- Hold din PC ajour med et opdateret antivirusprogram. (Antivirusprogrammer kan f.eks gratis downloades fra internettet).
- Slå "AutoRun"-funktionen fra på din PC (hindrer utilsigtede programmer i at starte op automatisk).
- Vær omhyggelig i forbindelse med flytning af data mellem systemer af forskellig klassifikation (læs FKOBST 358-1 eller spørg din it-sikkerhedsofficer til råds).
- Anvend aldrig private nøgler eller hukommelseskort i tjenstligt udstyr og omvendt.
- Husk at melde tab af tjenstlige USB-nøgler eller nøgler med tjenstlig information til din sikkerhedsofficer/chef.
- Læs også folderne "Hold kontakten – men med omtanke", "Brug internettet – men med omtanke" og "Undgå spionage – for din sikkerheds skyld", som du kan få på dit tjenestested, eller som kan rekvireres ved Forsvarets Efterretningstjeneste. Folderne kan du også finde på FE's hjemmeside på internettet.

Hvad skal du gøre, hvis du mister et tjenstligt USB-medie eller et medie med data fra/om forsvaret?

Du skal kontakte din it-sikkerhedsofficer eller din nærmeste foresatte.



**FE**

Forsvarets Efterretningstjeneste  
- Den Militære Sikkerhedsafdeling  
Kastellet 30  
2100 København Ø  
Tlf. +45 33 32 55 66  
[www.fe-ddis.dk](http://www.fe-ddis.dk)  
email: [fe@fe-mail.dk](mailto:fe@fe-mail.dk)

August 2010