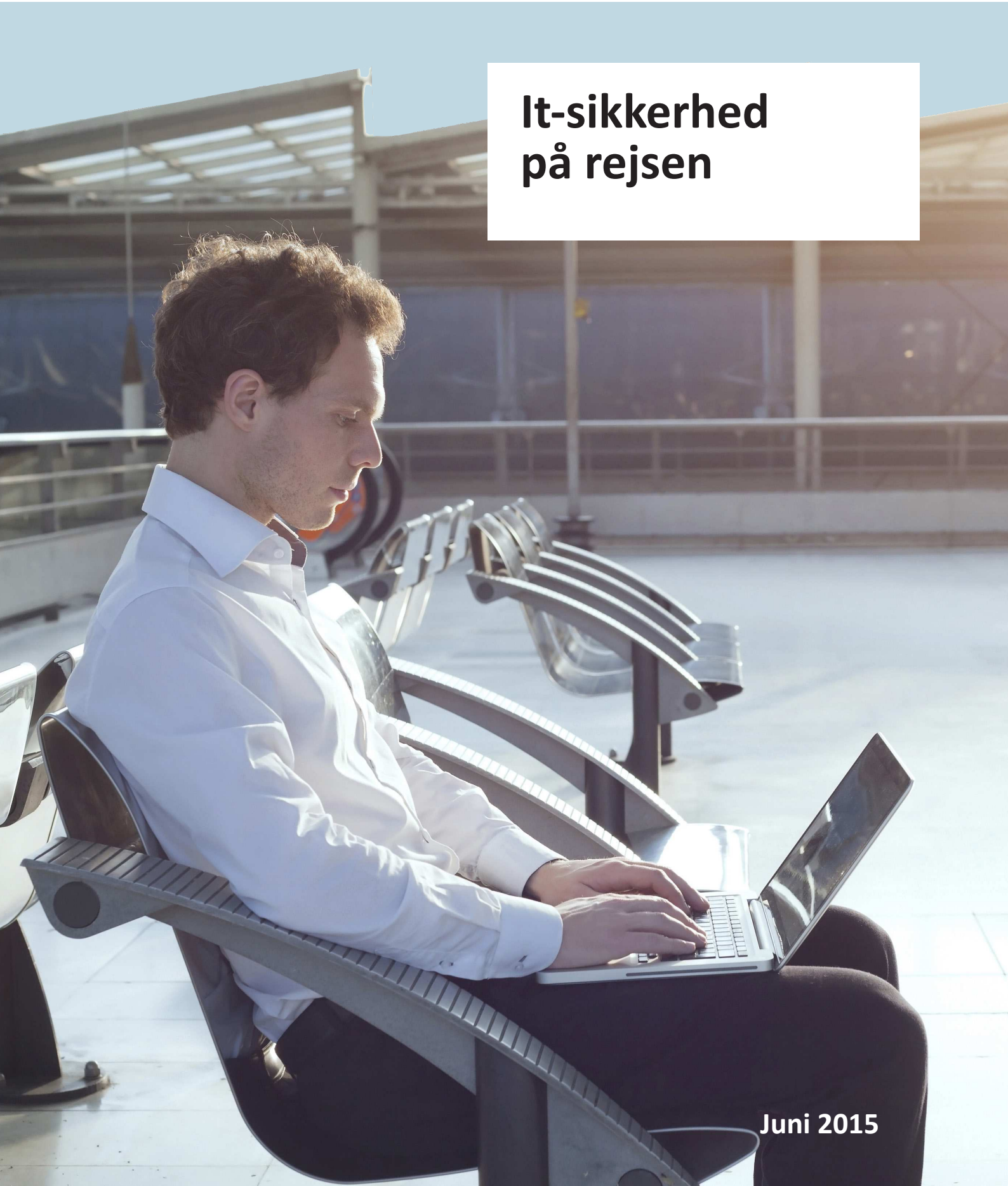
CENTER FOR CYBERSIKKERHED

Sikkerhedsanbefaling

It-sikkerhed på rejsen



Juni 2015

It-sikkerhed på rejsen

En sikkerhedsanbefaling fra
Center for Cybersikkerhed

Om sikkerhedsanbefalingen

Denne sikkerhedsanbefaling fra Center for Cybersikkerhed indeholder råd og vejledning til sikker brug af it-udstyr under rejser i udlandet.

Sikkerhedsanbefalingen er særligt rettet mod rejser i lande, hvor der må formodes at foregå indsamling af kommercielle og beskyttelsesværdige oplysninger fra digitale enheder og netværk.

Målgruppen er primært statslige myndigheder, virksomheder med kommercielt beskyttelsesværdige informationer, samt deres medarbejdere, som rejser i tjenesteligt ærinde.

Andre vil dog også kunne drage nytte af sikkerhedsanbefalingen, da niveauet for de sikkerhedsmæssige foranstaltninger altid bør afpasses den specifikkes rejses formål og eventuelle trusselsbillede i forhold til cyberangreb.

Indledning

Spionage mod statslige institutioner og danske virksomheder via internettet udgør en alvorlig cybertrussel imod Danmark. Samtidig udsender danske myndigheder og virksomheder hver dag medarbejdere og ledere til udlandet for at varetage danske interesser. Men med udlandsrejserne følger der potentielt en forhøjet risiko for, at medarbejderen, virksomheden eller Danmark også ad den vej udsættes for cybertrusler.

Dette skyldes, at mange medarbejdere i dag er afhængige af at have elektronisk adgang til informationer for at kunne udføre deres arbejde. Derfor er de nødt til at medbringe computere, smartphones og tablets på rejsen.

Konsekvensen er, at der opstår en risiko for, at informationssikkerheden bliver kompromitteret – især når udstyret bliver brugt til også at tilgå forretningskritiske informationer via internettet.

Hvis organisationens informationssikkerhed bliver kompromitteret, kan det betyde tab af forretningshemmeligheder, tyveri af intellektuel ejendom og ikke mindst, at hackere får tilegnet sig viden, der kan danne grundlag for de avancerede og vedholdende såkaldte APT-angreb, som kan stå på i det skjulte længe efter, at rejsen er forbi.

Det er derfor vigtigt, at både organisationen og de udsendte medarbejdere kender de risici og trusler, der er forbundet med udlandsrejser, og følger en række it-sikkerhedsmæssige forholdsregler.

De følgende sikkerhedsanbefalinger til at styrke it-sikkerheden på rejsen retter sig primært mod statslige institutioner og danske virksomheder, der kan være mål for avancerede cyberangreb. Anbefalingerne vil også være relevante for underleverandører til disse organisationer.

Anbefalingerne er rettet mod henholdsvis organisationens ledelse, den interne it-afdeling og den enkelte medarbejder.

Center for Cybersikkerhed

Center for Cybersikkerhed er statens kompetencecenter på cybersikkerhedsområdet og fokuserer på beskyttelse af samfundsvigtige funktioner mod avancerede cyberangreb. Det sker bl.a. ved, at Center for Cybersikkerhed varsler om cyberangreb, og ved at centeret efter nærmere vurdering bistår angrebne organisationer med at imødegå og afhjælpe cyberangreb.

På Center for Cybersikkerheds hjemmeside, www.cfcs.dk, er der yderligere information om cybertrusler og cybersikkerhed, herunder trusselsvurderinger, vejledninger samt en årlig efterretningsmæssig risikovurdering.

Anbefalinger til ledelsen

For at mindske de risici, der er forbundet med udlandsrejser, er det ledelsens ansvar at holde sig orienteret om det trusselsbillede, der er relevant for organisationen. Når ledelsen har erkendt eventuelle cybertrusler, bør den sikre, at it-afdelingen involveres aktivt i at støtte medarbejderne i form af råd og vejledning før, under og efter, de har været i udlandet.

Ledelsen bør i den forbindelse sørge for, at it-afdelingen får det nødvendige ledelsesmæssige fokus og de nødvendige ressourcer.

Et tilbud om råd og vejledning kan ikke stå alene. Ledelsen bør sikre, at den enkelte medarbejder forstår vigtigheden af at opretholde informationssikkerheden i organisationen. Dette kan gøres ved at lave oplysningskampagner og generelt fokusere på at informere medarbejderne

I lufthavnen

I det fortravlede og alsidige miljø i lufthavne vil du potentielt kunne komme ud i situationer eller have adgang til teknologier, som kan have betydning for it-sikkerheden. Dette kan eksempelvis være:

- **Tyveri af udstyr**
  Lufthavnen er et miljø med mange mennesker, hvor du kan risikere at blive udsat for forskellige former for forsøg på tyveri af værdifulde ejendele – herunder dit it-udstyr. En af de mere risikofyldte situationer er i sikkerhedstjekket, hvor dit it-udstyr, der typisk skal lægges frit frem til gennemlysning, ikke vil være under dit opsyn, hvis der eksempelvis opstår kø ved visitationen.
- **USB-ladestik**
  Flere lufthavne stiller USB-ladestik til rådighed for de rejsende i venteområderne. Der er dog ingen mulighed for at sikre sig, at disse tilslutninger ikke er kompromitteret af tredjepartsaktører, eksempelvis med malware,. Derfor bør du kun bruge de USB-ladere, som din it-afdeling har udleveret.
- **Trådløst internet**
  Der er ofte trådløst internet til rådighed i lufthavnene. Der er dog en risiko for, at tredjepartsaktører overvåger trafikken på disse offentlige forbindelser. Derfor bør du ikke bruge forbindelsen til at tilgå sensitivt materiale. Hvis dette ikke kan undgås, bør en VPN-tjeneste anvendes.

om informationssikkerhedspolitikkerne og de gældende retningslinjer.

Ledelsen bør sikre, at organisationens informationssikkerhed løbende bliver evalueret og forbedret på baggrund af erfaringer og ændringer i trusselbilledet, der er relevant for organisationen, og for rejser i de aktuelle lande.

Her er de anbefalinger, som ledelsen bør sikre, at organisationen følger for at styrke it-sikkerheden i forbindelse med medarbejdernes og ledelses egne udlandsrejser:

- Identificér organisationens vigtigste og mest sensitive informationer, hvor de fysisk er opbevaret, og hvilke overordnede trusler, de skal beskyttes imod herunder om der skal være adgang til dem ved ophold uden for virksomheden.
- Kend konsekvensen for organisationens forretning, hvis de internetbaserede tjenester bliver kompromitteret, og vigtige og sensitive informationer bliver stjålet eller lækket.
- Det er ledelsens ansvar, at holde sig orienteret om det aktuelle trusselsbillede, som eksempelvis kan findes i FE's trusselsvurderinger. Desuden skal ledelsen løbende vurdere organisationens egen risikoprofil i forhold til udlandsrejser.
- Formuler og nedskriv en informationssikkerhedspolitik og retningslinjer, der dækker håndteringen af vigtige og sensitive informationer. Sørg for at medarbejderen forstår og følger dem.
- Vær opmærksom på, at enhver person, herunder familie og bekendtskaber, som medarbejderen kontakter på rejsen, potentielt kan indgå som ufrivillig kilde i en informationsindsamling, der foretages af en tredjepart. Disse informationer kan blive brugt i forbindelse med et målrettet cyberangreb mod organisationen eller medarbejderen.

- Ledelsen skal gøre sig klart, at den også selv er underlagt disse politikker og retningslinjer, når den er på rejse.

Selv om det sidste punkt kan virke åbenlyst, er det alligevel vigtigt at understrege. Ledelsen skal erkende, at den i særlig grad selv er mål for de it-trusler, som opstår på udlandsrejser. Dette skyldes ikke mindst, at det især er ledelsen, som typisk har behov for at tilgå de mest følsomme data på rejsen.

På hotellet

På dit hotel er der mange faktorer, som du ikke har kontrol over, og som potentielt kan have betydning for din egen og din organisations it-sikkerhed. Eksempler på dette er:

- **Pengeskabet på dit værelse eller i receptionen**
  Uanset om det er sikret med nøgle eller pinkode, har personalet efter al sandsynlighed en ekstranøgle eller masterkode. Dermed er der en risiko for, at indholdet af pengeskabet kan blive kompromitteret. Det er ikke et sikkert sted at opbevare it-udstyr.
- **Internetadgang**
  Det er en risiko, at trafikken på hotellets netværks- og internetforbindelse bliver overvåget af tredjepartsaktører. Derfor bør du ikke tilgå sensitivt materiale via disse forbindelser. Hvis dette ikke kan undgås, bør en VPN-tjeneste eksempelvis anvendes.

Anbefalinger til it-afdelingen

Organisationens it-afdeling skal være med til at sikre, at udlandsrejsende medarbejdere ved, hvordan det medbragte it-udstyr anvendes sikkert på rejsen. Denne støttende funktion er vigtig, da der ellers er risiko for, at medarbejderen, der måske ikke har tilstrækkelig viden om sikker it-anvendelse, udsætter sig selv og organisationen for unødige risici både under og efter udlandsopholdet.

It-afdelingen bør derfor følge disse anbefalinger på baggrund af en relevant risikovurdering:

- Medarbejdere, der skal rejse til områder med særlig høj risiko for kompromittering, skal med kort varsel kunne få stillet låneudstyr til rådighed.
- Hvis virksomhedens medarbejdere rejser til særligt risikofyldte destinationer, kan det overvejes at have en udlånspulje af elektronisk udstyr, som udelukkende bruges i forbindelse med udlandsrejser.
- Tag backup af informationer på det it-udstyr, som medbringes på rejsen.
- Foretag en gennemgang, oprensning eller fuld sletning af indholdet i det it-udstyr, som medarbejderen har medbragt på rejsen, og genetabler indholdet med den backup, som blev lavet før afrejsen.
- It-afdelingen bør sikre, at alt medbragt it-udstyr anvender kryptering af de informationer og data, der lagres lokalt på udstyret.
- Sørg for, at softwaren i it-udstyret er opdateret med de nyeste sikkerhedsrettelser.
- Tag stilling til, om der skal stilles en alternativ mailboks til rådighed for medarbejderen for at undgå, at den normale arbejdsmail bliver kompromitteret på rejsen.
- Afsæt tiden til at rådgive og vejlede medarbejderne før, under og efter rejsen.

Anbefalinger til medarbejderne

Organisationens medarbejdere bør altid forholde sig til de trusler og risici, som de udsætter sig selv og organisationens informationsaktiver for. I den forbindelse skal medarbejderne gå ud fra, at ejerne af de netværk, som de bruger på deres ophold i udlandet, kan registrere alle telefonsamtaler, samt alt hvad der hentes eller sendes af data. Det indebærer, at uvedkommende har mulighed for at få adgang til disse informationer.

Både organisationen og den enkelte medarbejder bør desuden være opmærksomme på, at der altid er en risiko for, at uønskede tredjeparter kan tiltvinge sig elektronisk adgang til it-udstyr, når det er tændt og tilsluttet et fremmed netværk.

Derfor bør alle medarbejdere sørge for at indhente information og støtte fra it-afdelingen i forbindelse med arbejdsrelaterede udlandsrejser.

Det er medarbejderens ansvar at følge organisationens retningslinjer for it-sikkerhed på rejsen, så de informationer, der medbringes eller tilgås elektronisk via fjernadgang, bliver beskyttet bedst muligt.

Medarbejdere, der er på rejse, må gå ud fra, at de kan være mål for trusler, der kan kompromittere organisationens informationssikkerhed. Derfor bør organisationens medarbejdere efterleve følgende anbefalinger:

- Medbring kun de informationer, der er behov for, og husk at tage backup af dem inden rejsen.
- Lad så vidt muligt arbejdscomputer, tablet eller smartphone blive hjemme og medbring i stedet låne-udstyr, som kun giver adgang til de mest nødvendige informationer og programmer.
- Vær opmærksom på, at der er risiko for, at it-udstyret kompromitteres eller at informationer lækkes, hvis det udlånes til andre personer eller ikke er under opsyn.
- Organisationen og medarbejderen udsættes for store risici, hvis der benyttes trådløse netværk på eksempelvis konferencer, caféer og hoteller. Derfor bør medarbejderen undgå at udveksle og tilgå følsomme informationer over denne type netværk. Hvis der skal udveksles følsomme oplysninger, kan en VPN-tjeneste eller et 4G-modem eventuelt bruges som alternativ. GSM/2G-mobilkommunikation må generelt betragtes som usikker.

På konferencen

Når du står på konferencegulvet, vil typisk være flere forskellige faktorer, der kan have betydning for din og din virksomheds it-sikkerhed. Dette kan eksempelvis være:

- **Gratis USB-nøgler**
  USB-nøgler kan potentielt indeholde malware, der kan kompromittere dit it-udstyr, hvis du tager dem i brug. Derfor anbefales det at undlade at anvende disse, før indholdet har været kontrolleret af din it-afdeling.
- **Internetadgang**
  Der er ofte gratis trådløst netværk på messer og konferencer. Det bør imidlertid forventes, at trafikken på internetforbindelsen er overvåget af tredjepartsaktører.
- **Offentlige lånecomputere**
  Visse arrangører stiller også computere med internetadgang til rådighed for deltagerne Disse maskiner kan imidlertid indeholde værktøjer og malware, der eksempelvis kan indsamle de kodeord, som du indtaster.

- Den fysiske sikring af it-udstyret er en væsentlig faktor, når de medbragte informationer skal beskyttes på rejsen. Selv om udstyret er sikret med passwords, er der ingen garanti for, at andre ikke kan tilgå informationerne på udstyret, hvis det bliver stjålet. Derfor bør hverken pc, tablet eller smartphone efterlades ude af syne i det offentlige rum. I den forbindelse bør det også overvejes, om det er sikkert at efterlade udstyret på hotelværelset, eller om det på anden vis er muligt at sikre udstyret mod uautoriseret adgang.
- Opbevaring i hotelværelsets sikkerhedsboks anses normalt ikke for sikkert på risikofyldte destinationer. Anvendelse af forseglede engangskuverter ved opbevaring uden opsyn vil kunne hjælpe til at afsløre uautoriseret adgang til it-udstyret.
- Hvis der bruges fremmed it-udstyr til at tilgå informationer via fjernadgang til organisationen eller andre onlinetjenester, indebærer det altid en risiko for, at vitale informationer, herunder passwords via keyloggere, falder i hænderne på uvedkommende. Derfor bør det undgås at tilgå og anvende følsomme informationer via fremmed it-udstyr, herunder udstyr placeret på internetcaféer, hoteller og konferencer.
- USB-enheder anvendes i stort omfang til at distribuere informationer og som reklameværktøj på firmamesser og konferencer. Men disse enheder bliver også anvendt til at distribuere forskellige former for malware. Derfor bør ingen fremmede USB-enheder tages i brug.
- Når rejsen er afsluttet, bør der skiftes kodeord på alle de it-tjenester, der har været brugt på rejsen.
- It-afdelingen bør skanne og om nødvendig rense alt det it-udstyr, der har været med på rejsen. Låneudstyr bør geninstalleres efter hvert udlån.

6 sikre råd til rejsen

Når du er ude at rejse, kan du blive udsat for mange situationer, som kan udnyttes af ondsindede aktører til at kompromittere din og din organisations it-sikkerhed.
Her er 6 generelle råd til at styrke it-sikkerheden på rejsen:

- Undgå offentlige internetopkoblinger til at udveksle og tilgå sensitive informationer
- Benyt aldrig fremmed it-udstyr til at udveksle og tilgå sensitive informationer
- Hav altid dit it-udstyr under opsyn
- Tilslut aldrig fremmede USB-enheder eller -strømopladere til dit it-udstyr
- Udlån aldrig dit it-udstyr til fremmede personer
- Udskift altid dine kodeord til de tjenester, som du har tilgået på rejsen, når du vender hjem

It-sikkerhed på rejsen

6 sikre råd til rejsen

Når du er ude at rejse, kan du blive udsat for mange situationer, som kan udnyttes af ondsindede aktører til at kompromittere din og din organisations it-sikkerhed.
Her er 6 generelle råd til at styrke it-sikkerheden på rejsen:

- Undgå offentlige internetopkoblinger til at udveksle og tilgå sensitive informationer
- Benyt aldrig fremmed it-udstyr til at udveksle og tilgå sensitive informationer
- Hav altid dit it-udstyr under opsyn
- Tilslut aldrig fremmede USB-enheder eller strømopladere til dit it-udstyr
- Udlån aldrig dit it-udstyr til fremmede personer
- Udskift altid dine kodeord til de tjenester, som du har tilgået på rejsen, når du vender hjem

CENTER FOR CYBERSIKKERHED

Kastellet 30
2100 København Ø

Tlf.: 3332 5580
cfcs@cfcs.dk
www.cfcs.dk