digitaliserings og ligestillingsministeriet

Enhed
Administration og Økonomi

Sagsbehandler
Tobias Christoffer Thykjær

Koordineret med

Sagsnr.
2023-1432

Doknr.
40316

Dato
23-10-2023

IT-sikkerhed på rejser

Når du rejser som en del af dit arbejde, tager du også dit arbejde med uden for de vante rammer. På hotellet, i lufthavnen, på konferencen og på en kundes eller samarbejdspartners kontor står du uden for mange af de sikkerhedsforanstaltninger, som derhjemme beskytter dig, dit udstyr og din organisations data. Derfor hviler en større del af sikkerheden på dine skuldre.

Som medarbejder har du ligesom alle dine kollegaer et ansvar for at rejse cybersikkert. Du har et ansvar for at passe på dig selv og din organisation, når du rejser. Det betyder, at du som medarbejder skal udøve en sikker adfærd og anvende det medbragte it-udstyr på en forsvarlig måde. Det gælder alle medarbejdere, der rejser, herunder ledelsen. Ofte er det medarbejderne, som er hackerens vej ind i organisationen.

Når du rejser, skal du også fortsat huske den samme sikre adfærd, som du er opmærksom på og følger til daglig. De helt grundlæggende regler om sikkerhed på Stormgade og derhjemme gælder også på rejser og kan langt hen ad vejen støtte dig, hvis du kommer i tvivl.

Herunder finder du departementets politik for IT-sikkerhed på rejser. Politikken indeholder en række råd og retningslinjer, baseret på anbefalinger fra Center for Cybersikkerhed og PET, der kan hjælpe dig med at rejse sikkert og sikre departements informationer både før, under og efter din rejse.

Før rejsen

Sørg for at have tid nok

Du kan mindske risici på din rejse ved at planlægge den med god tid indlagt til alle gøremål. Denne lavpraktiske foranstaltning – at være i god tid – styrker sikkerheden. Det er ofte i tidspressede situationer, som for eksempel at man er ved at komme for sent til en flyafgang, at der sker fejl, der kompromitterer sikkerheden.

Kontakt Administration og Økonomi ved rejser uden for EU

Der kan være yderligere risici forbundet med rejser uden for EU, og dit sædvanlige udstyr må ikke benyttes ved rejser til højrisiko-lande. Sikkerhedsfunktionen i Administration og Økonomi skal kontaktes forud for rejsen for at gøre opmærksom på særlige forholdsregler og evt. udlevering af rejseudstyr i forbindelse rejsen til det pågældende land. Dette gælder også rejser i privat regi, hvor departementets it-udstyr medbringes.

Sæt dig ind i det land, du rejser til

Allerede på det tidspunkt hvor du bliver bekendt med, at du skal på en tjenesterejse til et nyt sted, vil det være en god ide at sætte dig ind i de lokale forhold, der hvor du skal bo, deltage i

møder eller er på konference. Det er specielt vigtigt, hvis du skal rejse til lande, som vurderes til at være højrisikolande. Hvis du er i tvivl, om dit rejsemål falder inden for denne kategori, så spørg Administration og Økonomi. Du kan også finde rejsevejledninger om de generelle forhold i en række lande via Udenrigsministeriets app "Rejseklar".

Gem en kopi af dine dokumenter

Hvis du har dokumenter lokalt på din computer, skal du sørge for at gemme en kopi i F2 eller på fællesdrevet (H-drevet). Dermed undgår du, at dit arbejde går tabt, hvis du mister dit udstyr.

Under rejsen

Brug internetdeling via din mobiltelefon og ikke åbne offentlige wifi-netværk

Åbne offentlige netværk anses som udgangspunkt for usikre og må ikke benyttes. Brug i stedet internetdeling via din mobiltelefon. Husk at beskytte adgangen med en kode. Spørg Administration og Økonomi, hvis du er i tvivl om, hvordan du opsætter internetdeling.

Brug kun dit eget it-udstyr til at udveksle og tilgå følsomme informationer

Du må udelukkende anvende dit medbragte udstyr. Hvis du anvender en offentlig pc på hotellet, på konferencen eller lignende, har du ingen umiddelbar mulighed for at sikre dig mod, at pc'en indeholder malware, der vil aflure dine data eller passwords.

Udlån aldrig dit it-udstyr

Du må aldrig udlåne departementets it-udstyr til andre. Der er risiko for, at dit it-udstyr kompromitteres eller at informationer lækkes, hvis det udlånes til andre personer. Også selvom anvendelsen virker uskyldig og kun sker i din nærhed.

Slå Bluetooth fra i alt it-udstyr

Bluetooth kan forbinde din telefon, tablet eller pc til et trådløst headset. Men forbindelsen kan også overføre data og give adgang til dine enheder. Derfor skal du slå Bluetooth fra, når du ikke bruger det. Vær særlig opmærksom på, at Bluetooth-forbindelsen til underholdnings- og navigationssystemet i en bil kan overføre oplysninger om kontaktpersoner og telefonopkald til bilens computer. Derfor bør du ikke forbinde dit udstyr via Bluetooth, hvis du lejer en bil.

Hold arbejde og privatliv adskilt

Anvend kun departementets it-udstyr til arbejdsrelaterede gøremål og undgå at tilgå departementets systemer, herunder mail og F2, fra din private enhed. Brug dit eget udstyr til din private e-mail og lignende. På den måde beskytter du både departementets og dine egne data.

Vær opmærksom på omgivelserne

Du bør være særligt opmærksom på dine omgivelser, når du er på farten. Sørg for at skærme dit arbejde for nysgerrige blikke og lange ører. Er der for eksempel nogen, der kan lytte med i samtalen, eller er der nogen, der kan se din computerskærm? Et skærmfilter, der gør din skærm mindre læsbar for omgivelserne, kan bestilles hos Service.

Tilslut aldrig fremmede USB-enheder eller strømopladere til dit it-udstyr

USB-enheder bruges ofte til at distribuere informationer og som reklame på messer og konferencer. Men disse enheder er også blevet anvendt til at distribuere forskellige former for malware. Du må derfor ikke tage fremmede USB-enheder i brug. Dette gælder også fremmedes strømopladere til eksempelvis din tablet eller mobiltelefon. Medbring i stedet en powerbank eller brug din arbejds-pc som oplader til din arbejdstablet eller arbejdstelefon.

Hav altid dit udstyr og dine dokumenter under opsyn

Hvis dit udstyr bliver stjålet, er der ingen garanti for, at andre ikke kan tilgå informationerne på udstyret, selv om det er sikret med passwords. Derfor må hverken pc, tablet eller smartphone efterlades ude af syne i det offentlige rum.

Rapporter alle sikkerhedshændelser

Vær opmærksom på tegn på brud på sikkerheden og meld mistænkelige hændelser via skemaet på intranettet. Det er vigtigt, at du som medarbejder rapporterer enhver mistanke om en sikkerhedshændelse. Det bør ske hurtigt, så der kan reageres på situationen. Enhver kan blive narret af en phishing-mail, så der er intet pinligt i at indrapportere det. Det er derimod vigtigt, at departementets It-sikkerhedsfunktion får besked, så der kan gøres noget ved det.

Efter rejsen

Aflever alt lånt it-udstyr

Du skal tilbagelevere eventuelt udstyr, du har lånt til din rejse, snarest mulig efter din hjemkomst. Henvend dig til Administration og Økonomi.

Udskift passwords til de tjenester som du har tilgået på rejsen

Det er altid en god idé at udskifte password på konti til de tjenester, som du har tilgået på din rejse. Dette kan være et krav afhængig af, hvilket land du har rejst til.

Vær opmærksom på uventede henvendelser

Vær opmærksom på uventede henvendelser. Du bør være opmærksom på eventuel uventet kontakt eller mails, som du modtager efter din hjemkomst. Meld mistænkelige henvendelser til IT-sikkerhedsfunktionen i Administration og Økonomi.