CENTER FOR CYBERSIKKERHED

Cybersikkerhed på rejsen

Gode råd til medarbejderen

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.

Derfor skal du følge de regler og retningslinjer, der gælder. Og du skal sætte dig ind i, hvor du rejser til, og hvad det kan medføre af risici.

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

Hver rejse er unik og kan være forbundet med særlige risici. Derfor indeholder denne vejledning ikke en udtømmende liste over gode råd til rejsesikkerhed. Men efter at have læst den vil du være klædt bedre på til din næste rejse. Vejledningen er udarbejdet af Center for Cybersikkerhed i samarbejde med Politiets Efterretningstjeneste.

Anbefalinger til dig som rejser

Før rejsen

- Sæt dig ind i organisationens rejsepolitik og øvrige regler.
- Sæt dig ind i det land, du rejser til.
- Afklar hvilke informationer du skal have adgang til på din rejse.
- Bliv klædt på af it-afdelingen.
- Afprøv dit it-udstyr.
- Tag en sikkerhedskopi.

Under rejsen

- Brug internetdeling på din telefon og ikke åbne wifi-netværk.
- Brug kun dit eget it-udstyr
- Hav altid dit it-udstyr under opsyn.
- Lån aldrig dit it-udstyr ud.
- Tilslut aldrig fremmede USB-enheder eller strømopladere
- Slå Bluetooth fra.
- Rapporter sikkerhedshændelser.

Efter rejsen

- Aflever lånt it-udstyr.
- Orienter it-afdelingen om eventuelle hændelser og problemer.
- Udskift passwords til de tjenester, som du har tilgået på rejsen.

Før rejsen

Der er en række ting, du sammen med din organisation kan gøre på forhånd for at skabe de bedste betingelser for at sikre dig, dit udstyr og organisationens data.

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.

Vær opmærksom på, hvor du som rejsende er særlig sårbar

Som rejsende skal du være bevidst om, at der er situationer, hvor du er særlig sårbar. Hvis du er bevidst om, at disse situationer kan opstå, kan du og din organisation tage højde for dem. Hvis det er muligt, kan det være en god ide at rejse flere sammen. På den måde kan I hjælpe hinanden med at passe på dokumenter og udstyr, og I kan i fællesskab vurdere de enkelte situationer.

Eksempler på situationer hvor man som rejsende er særligt sårbar:

- Under transport i bil, taxa, tog og fly risikerer man at miste sine dokumenter eller sit udstyr.
- Under sikkerhedstjekket i en lufthavn risikerer man at miste sine dokumenter eller sit udstyr.
- Når man anvender it-udstyret uden for organisationens fysiske rammer (kontoret), risikerer man, at kommunikationen ikke er sikker. Derved kan følsomme informationer blive kompromitteret.
- Uden for organisationens fysiske rammer risikerer man, at udstyret bliver kompromitteret, fordi det er lettere for uvedkommende at få fysisk adgang til det.
- Når man er til konference er man særlig sårbar, fordi der er mange personer samlet og lange dage med faglige og sociale aktiviteter kan gøre det svært at holde sit udstyr under konstant opsyn.

Sæt dig ind i organisationens rejsepolitik og øvrige regler

En sikker rejse kræver, at du som medarbejder er bevidst om det risikobillede, som er gældende, når du rejser, og hvorledes din organisation har besluttet, at du skal agere på den baggrund. Du bør derfor sætte dig grundigt ind i din organisations rejsepolitik og øvrige regler, som gælder for dig, når du rejser.

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 ny 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 din organisation vurderer til at være højrisikolande. Du kan også finde rejsevejledninger om de generelle forhold i en række lande via Udenrigsministeriets app "Rejseklar".

Kend risikoen for din rejse
Lige netop din rejse kan være mere risikabel for dig end din kollega. Derfor bør du sammen med din organisation vurdere, om der er særlige risikofaktorer, der gælder for rejsen. Risikoen kan for eksempel afhænge af, hvilken viden du tager med dig, hvem du skal møde, og hvad du skal foretage dig.

Afklar, hvilke informationer du skal have adgang til på din rejse
Inden du rejser, bør du afklare med dig selv og eventuelt kollegaer og ledelse, hvilke informationer du har brug for til at løse dine opgaver på rejsen. Visse informationer er mere kritiske end andre og stiller større krav til sikkerheden. Dette bør være udmøntet i din organisations sikkerhedspolitik.

Det anbefales under alle omstændigheder, at du kun medbringer de informationer, der er absolut nødvendige for dine opgaver på rejsen. Tilsvarende bør du kun anmode om ekstern adgang til interne systemer, som er absolut nødvendige for dine opgaver.

Du bør også på forhånd afklare, hvilke informationer du kan dele med hvem og hvordan. Det er lettere at afvise interesserede personer, hvis du på forhånd har besluttet dig for, hvad du ikke vil dele.

Bliv "klædt på" til rejsen af it-afdelingen
Uanset om du arbejder fra kontoret eller fra et hotel i et andet land, er det it-afdelingen, der hjælper dig. Du kan blive "klædt på" af it-afdelingen med relevant it-udstyr og viden. It-afdelingen kan have behov for at få beskrevet de opgaver, du skal varetage på din rejse, således at de kan give dig det rigtige it-udstyr, applikationer, tilbehør og råd.

Tag en sikkerhedskopi af de kritiske informationer, du medbringer på rejsen.
Hvis du medbringer kritiske informationer på dit it-udstyr, bør du altid sikre dig, at der hjemme i organisationen er en kopi af informationerne. Det gælder også data på eksterne lagringsmedier.

Afprøv dit it-udstyr, inden rejsen påbegyndes
Inden afrejse bør du afprøve det it-udstyr, du skal medbringe. Ellers risikerer du at stå uden en fungerende it-løsning langt fra din organisations it-supportfunktion. Du bør også kontrollere, at du har adgang til de applikationer og tjenester, du har brug for på din rejse, også uden at være på organisationens interne netværk.

For yderligere inspiration til at få en sikker rejse, kan du læse følgende to vejledninger om grundlæggende cybersikkerhed, som især er relevante, når du rejser:

Center for Cybersikkerhed og Digitaliseringsstyrelsen: *God kultur ved distancearbejde*

Center for Cybersikkerhed og Politiets Efterretningstjeneste: *Råd om sikkerhed på mobile enheder*

Under rejsen

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

Åbne offentlige netværk anses som udgangspunkt for usikre. Brug i stedet internetdeling via din mobiltelefon, hvis det er muligt. Husk at beskytte adgangen med en kode.

Brug VPN
Ved altid at anvende VPN vil du reducere en del af risikoen ved eksempelvis brug af åbne offentlige netværk. Spørg eventuelt din it-afdeling om VPN på dit udstyr.

Brug kun dit eget it-udstyr til at udveksle og tilgå følsomme informationer
Du bør 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
Vær opmærksom på, at 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.

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 bør derfor ikke tage fremmede USB-enheder i brug. Dette gælder også strømopladere til eksempelvis din tablet eller mobiltelefon. Medbring i stedet en powerbank eller brug din arbejds-pc som oplader til din arbejdstablet eller arbejdstelefon.

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 bør 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 it-udstyr udlånt af organisationen til og tilslut aldrig privat udstyr til dit arbejdsrelaterede udstyr. På den måde beskytter du både organisationen og dine egne data. Brug dit eget udstyr til din private e-mail og lignende, eller lån eventuelt separat udstyr til privat brug på rejsen af din it-afdeling.

Skærm for nysgerrige blikke og lange ører
Vær opmærksom på omgivelserne, når du arbejder. Er der for eksempel nogen som kan lytte med i samtalen, eller er der nogen, der kan se computerskærmen? Vær samtidig opmærksom, når du indtaster

dit login og password. Som udgangspunkt bør du i offentlige miljøer kun arbejde med ikke-følsomme informationer.

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 bør hverken pc, tablet eller smartphone efterlades ude af syne i det offentlige rum. I den forbindelse skal du være opmærksom på, at hverken hotelværelset eller værdiboksen kan betragtes som sikre, da personalet har adgang til dem.

Brug omstillingen
Ring i videst muligt omfang til omstillingen i stedet for at ringe direkte til kollegaer, når du ringer hjem til organisationen. På den måde skærmer du dine kollegers kontaktoplysninger.

Pas på dig selv og dine kolleger
Din viden og din adgang til din organisation kan være værdifuld for andre med onde hensigter. Derfor er det en god idé, at du passer på dig selv og dine kolleger, ligesom I passer på jeres it-udstyr. Vær opmærksom, hvis du støder ind i personer, som udviser ekstra interesse for dit arbejde eller for dig som privatperson. Det kan være en måde at forsøge at indhente informationer på. Generelt bør der tænde en lille alarmlampe, hvis du pludselig står i en unormal situation. Undgå især at sætte dig i en situation, hvor du senere kan blive afpresset.

Rapporter alle sikkerhedshændelser
Vær opmærksom på tegn på brud på sikkerheden og meld mistænkelige hændelser til din organisation. Der er aktører, som forsøger at udnytte, at en organisations medarbejdere er på tjenesterejse. Det er derfor 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 din organisations sikkerhedsfunktion får besked, så der kan gøres noget ved det.

Efter rejsen

Aflever alt lånt it-udstyr
Du bør tilbagelevere eventuelt udstyr, du har lånt til din rejse, snarest mulig efter din hjemkomst. Hvis du har arbejdet med dokumenter, regneark eller andet under rejsen, som udelukkende findes lokalt på det lånte udstyr, bør du kopiere dem. Spørg eventuelt it-afdelingen om, hvordan du bedst overfører til de interne systemer.

Udskift altid passwords til de tjenester, som du har tilgået på rejsen
Som udgangspunkt bør du udskifte password på de konti til din organisations tjenester, som du har tilgået på din tjenesterejse.

Orienter om eventuelle hændelser og problemer
Du bør efter hjemkomsten være indstillet på at give yderligere informationer om hændelser og problemer til din it-afdeling eller sikkerhedsfunktion.

Vær opmærksom på uventede henvendelser
Du bør være opmærksom på eventuel uventet kontakt eller mails, som du modtager efter din hjemkomst.

CENTER FOR CYBERSIKKERHED

Forsvarets Efterretningstjeneste
Center for Cybersikkerhed
Postadresse: Kastellet 30
Besøgsadresse: Holsteinsgade 63
2100 København Ø
Tlf. 33 22 55 80
E-mail: cfcs@cfcs.dk
www.cfcs.dk

1. udgave, januar 2022