CENTER FOR CYBERSIKKERHED

PET

Råd om sikkerhed på mobile enheder

Center for Cybersikkerhed
Kastellet 30
2100 København Ø

Telefon: 3332 5580
E-mail: cfcs@cfcs.dk
www.cfcs.dk

1. udgave
05.11.2018

Råd om sikkerhed på mobile enheder: God, Bedre, Bedst

Sikkerhedsbehovet ved anvendelse af mobile enheder som f.eks. smartphones, smartwatches, tablets og pc'er afhænger af, hvem man er, og hvilke trusler man står over for. Ikke alle har den samme risiko for at blive udsat for sikkerhedshændelser. Jo mere interessante eller følsomme oplysninger man har adgang til, desto større risiko er man udsat for. Mobilsikkerhed skal derfor prioriteres, og der skal vælges det relevante sikkerhedsniveau ved anvendelse af enheder, der indeholder eller har adgang til statens uklassificerede informationer.

Vejledningen dækker ikke klassificerede informationer og forhold, der er dækket af Justitsministeriets cirkulære om sikkerhedsbeskyttelse af informationer (Sikkerhedscirkulæret). Vejledningen ændrer ikke grundlæggende på det forhold, at der ikke må kommunikeres klassificerede oplysninger på almindelige mobile enheder. Vejledningen forholder sig heller ikke til håndtering af oplysninger på de mobile enheder, der kan være omfattet af anden lovgivning, herunder fx persondatalovgivning.

Vejledningen, der især henvender sig til centraladministrationens embedsfolk, beskriver en række organisatoriske, tekniske og adfærdsmæssige tiltag, der kan styrke mobilsikkerheden omkring den enkelte brugers anvendelse af mobile enheder. Hvis rådene følges kan man således modvirke en række risici for kompromittering af mobile enheder.

Vejledningen er tænkt som basale råd til adfærd og brug af sikkerhedstekniske foranstaltninger, mere end et kontrolredskab.

Der benyttes tre niveauer for mobilsikkerhed: "God", "Bedre" og "Bedst". Alt afhængig af situationen kan valg mellem de tre niveauer eller en kombination bruges. Der kan også være situationer, hvor et anbefalet råd ikke kan anvendes, f.eks. for en mobil enhed der ikke har den relevante teknologi.

Forsvarets Efterretningstjeneste og Politiets Efterretningstjeneste anbefaler, at alle følger rådene. Sikkerhedsniveauet "God" kan opnås ved en sund sikkerhedsmæssig adfærd og anvendelse af enkle tekniske løsninger og indstillinger, som enhver kan håndtere ved anvendelse af mobile enheder.

Listen over råd er ikke udtømmende eller en facitliste, men kan være med til at øge den basale mobilsikkerhed. Det giver mulighed for, at arbejdspladsen selv kan overveje hvilke yderligere tiltag, der er relevante og mulige. Listen er heller ikke statisk, idet Forsvarets Efterretningstjeneste og Politiets Efterretningstjeneste vil opdatere listen efter det aktuelle samlede risikobillede og ikke mindst efter feedback fra brugerne af vejledningen. Forslag til nye sikkerhedsvinkler, der ønskes belyst ved anvendelse af mobile løsninger, er derfor meget velkomne.

15 råd til sikring af mobile enheder

Du kan opnå god mobilsikkerhed med nogle få tiltag, du selv kan klare ved at sætte din telefon eller pc op på en bedre beskyttet måde, men skal din mobilsikkerhed være bedst mulig, så skal du have hjælp fra it-organisationen på din arbejdsplads. Hvilke tiltag, der er nødvendige for at beskytte dine enheder, afhænger af den situation du står i. Skal du rejse til udlandet, kan det være nødvendigt at øge mobilsikkerhedsniveauet. Det afhænger af en vurdering af risikoen forbundet med situationen og destinationerne for din rejse.
Denne vejledning skal hjælpe med at klarlægge de tiltag, du og din it-organisation kan anvende for at opnå den nødvendige mobilsikkerhed i en given situation. Det er en forudsætning, at du ud over denne vejledning har den fundamentale mobilsikkerhed på plads. Eksempelvis bør din telefon eller pc ikke anvende et styresystem, som ikke længere opdateres af producenten. Tilsvarende bør du anvende unikke, stærke passwords til de it-tjenester, du tilgår fra enheden.
Mobile enheder, og andet elektronisk udstyr, der kan optage lyd eller billeder, skal ikke være tilstede i lokalet, når der formidles klassificeret information. Dette kan tillige være tilfældet ved formidling af anden sensitiv information.

1. Beskyt dine mobile enheder med en adgangskode

En kort øjebliks uopmærksomhed kan være nok til at kompromittere f.eks. en smartphone, hvis uvedkommende får adgang til telefonen. En telefon, som bliver stjålet eller tabt, kan også føre til lækket information, hvis telefonen ikke er beskyttet. Det mest grundlæggende, du kan gøre for at sikre telefonen, og den information, der ligger på den, er at bruge en adgangskode. Det er ikke tilstrækkeligt at nøjes med den firecifrede SIM-kortlås. Det skal være en kode, som ligesom dit password skal være svært at gætte, selv for folk, som kender dig godt. Du kan vælge en stærkere type password i telefonens indstillinger, der f.eks. består af både tal og bogstaver. Telefonen giver adgang til din e-mail, og du bruger den måske også som ekstra sikkerhed til to-faktor-autentifikation, dvs. at der skal mere end en adgangskode til for at tilgå et system. Derfor skal du vælge en god, sikker kode. Brug ikke den samme kode på din private enhed og en arbejdsenhed.

A: God	B: Bedre	C: Bedst
Numerisk (cifrene 0 til 9) kode på mindst 6 cifre.	Numerisk kode på mindst 10 cifre.	Alfanumerisk (blanding af tal og bogstaver) på mindst 10 tegn.

2. Kryptér data på dine mobile enheder

Hvis din telefon, pc eller tablet bliver stjålet, eller du på anden måde mister den, kan uvedkommende få adgang til de data, som ligger på den. Ved at kryptere den information, som du har liggende på telefonen eller pc'en, kan du forhindre, at uvedkommende kan læse dokumenter og e-mails, se dine fotos eller stjæle andre data. Derfor bør du slå kryptering til. Hvordan du gør dette, afhænger af, hvilken enhed du benytter. Mobile Device Management er en løsning, som it-afdelingen kan bruge til at administrere mobilsikkerheden på organisationens mobiltelefoner og bærbare pc'er.

A: God	B: Bedre	C: Bedst
Slå enhedskryptering til i indstillingerne for din telefon, pc eller tablet.	Lad it-afdelingen styre enhedskrypteringen (med Mobile Device Management).	Se 'Bedre'.

3. Hold dine mobile enheder opdaterede

Både applikationer og styresystemet på f.eks. din telefon, pc og tablet kan indeholde sikkerhedshuller, som gør det muligt for hackere at bryde ind og få adgang til data. Et sikkerhedshul kan også udnyttes til at installere malware, som kan bruges til aflytning ved hjælp af telefonens eller pc'ens kamera og mikrofoner.

A: God	B: Bedre	C: Bedst
Kontrollér selv regelmæssigt, om der er opdateringer til applikationer eller styresystem, som skal installeres. Slå automatiske opdateringer til og installér opdateringerne, hvis telefonen eller pc'en beder dig om det.	It-afdelingen kontrollerer, at der som minimum installeres kritiske opdateringer til styresystemet inden for en kort tidsfrist.	It-afdelingen håndhæver installation af opdateringer til styresystemet og andre applikationer ved hjælp af en Mobile Device Management-løsning

4. Undgå at uvedkommende kan læse beskeder fra din låste telefon eller tablet

Mange applikationer kan vise hele eller dele af beskeder på din skærm, også selvom den er låst. Denne funktion kaldes ofte notifikationer. Det gælder f.eks. Nyheder, Mail, SMS eller beskeder om mistede telefonopkald. Disse beskeder kan andre læse, også selvom de ikke kan låse din mobile enhed op.

A: God	B: Bedre	C: Bedst
Brug et cover med klap, der kan dække skærmen. Du kan også mindske risikoen ved at benytte et privacy beskyttelsesglas, det begrænser muligheden for at læse skærmen fra skæve vinkler.	Slå notifikationer fra på de applikationer, der kan indeholde følsomme oplysninger, herunder oplysninger om dine kontaktforhold mv. Det kunne f.eks. være mail, SMS, telefonopkald. Hvordan du gør dette, afhænger af, hvilken enhed du benytter.	Se 'Bedre'.

5. Modvirk aflytning af din mobile enhed

Når du anvender f.eks. din telefon, pc og tablet i forbindelse med (telefon)samtaler, er der en risiko for at andre lytter med. Afhængig af den mobile enhed er der en række tiltag som kan reducere denne risiko.

A: God	B: Bedre	C: Bedst
Vær opmærksom på hvilket netværk (EDGE, 3G, 4G) din mobile enhed er på. Anvend helst 4G, herved mindsker du risikoen for at nogen "lokker" din mobile enhed over på et netværk uden kryptering. EDGE (2G) er mere sårbart end 3G, der er mere sårbart end 4G.	Benyt en app med end-to-end-kryptering, f.eks. Signal, WhatsApp m.fl. Herved sørger app'en for at samtalen er krypteret. Sådanne apps fås til din telefon, tablet og pc.	Benyt en mobil app med end-to-end kryptering som er underlagt it-afdelingens centralt administrerede Mobile Device Management–løsning.

6. Backup og lagring af informationer uden for din mobile enhed

Det kan være nødvendigt at lagre informationer fra din mobile enhed andre steder f.eks. i skyen, for at få de fornødne funktionaliteter. Det er desuden en praktisk måde at sikre fleksibel tilgang til dine data og ofte en god måde at lave backup. Når du lagrer informationer andre steder end på den mobile enhed, øger det imidlertid risikoen for, at uvedkommende kan komme til dem.

A: God	B: Bedre	C: Bedst
Brug kun lagringstjenester på internettet hvis de er krypteret. F.eks. iCloud. Sæt din mobile enhed til automatisk backup til den valgte tjeneste.	Brug en lagringstjeneste it-afdelingen har indgået aftale med.	Brug en lagringstjeneste som It-afdelingen driver og har kontrol over (private cloud).

7. Slet data fra din mobile enhed, hvis du mister den

Hvis du mister din telefon, pc eller tablet, så er det ikke kun værdien af hardwaren, du mister. Du risikerer også, at dine data, dokumenter, fotos eller beskeder falder i forkerte hænder. Derfor bør du være klar til at slette indholdet af din telefon eller pc, hvis du mister den.

A: God	B: Bedre	C: Bedst
Benyt leverandørens tjeneste til at slette enheden f.eks. 'Find min iPhone'.	Telefonen indstilles til at slette indholdet efter 10 fejlslagne forsøg på at indtaste koden.	It-afdelingen bruger en Mobile Device Management-løsning til at slette data fra enheden.

8. Brug trådløse netværk (Wi-Fi) med omtanke

Trådløse netværk (Wi-Fi) er meget usikre, idet de sender information gennem luften, som alle med en antenne kan få adgang til. Undgå derfor at benytte Wi-Fi, men hvis du gør, så er det vigtigt at kryptere de informationer, du sender og modtager via et trådløst netværk. Du skal også være opmærksom på, at din telefon, pc mv. kan snydes til at koble på et usikkert netværk, som udgiver sig for at være et netværk, du tidligere har været logget på, uden du opdager det.

A: God	B: Bedre	C: Bedst
Slå automatisk etablering af forbindelse (auto-join) til Wi-Fi fra i din enheds indstillinger. Undgå Wi-Fi, hvor du ikke skal bruge et password til at forbinde til netværket.	Benyt kun kendte Wi-Fi-netværk og med password. Det vil f.eks. sige netværk derhjemme og på kontoret. Undgå brug af offentlig Wi-Fi f.eks. på hoteller, caféer, i lufthavne, eller på konferencer. Brug din telefon til internetdeling (mobildata) i stedet.	Benyt kun Wi-Fi-forbindelser, når du samtidig bruger en VPN-løsning fra en anerkendt VPN udbyder.

9. Brug "Virtuel Private Network" (VPN)

Du bør benytte en VPN-løsning til at gå på internettet. Det giver dig en krypteret, forbindelse, der også kan benyttes til at forbinde til dit firma eller organisations lokale netværk over internettet.

VPN virker ved at kryptere trafik fra dig til din VPN-udbyder. Derfor er valget af VPN-udbyder vigtigt og har indflydelse på, hvor sikker VPN er.

A: God	B: Bedre	C: Bedst
Benyt en VPN-løsning fra en anerkendt VPN udbyder.	Benyt en firmaindkøbt VPN-løsning.	Benyt en VPN udbyder, der er administreret af din IT afdeling.

10. Slå Bluetooth fra

Bluetooth kan forbinde din telefon eller pc til et trådløst headset eller computeren i en bil. Men forbindelsen kan overføre data og give adgang til din pc eller telefon, og derfor bør du slå Bluetooth fra, når du ikke bruger det. Vær også opmærksom på, at Bluetooth-forbindelsen til underholdnings- og navigationssystemet i en bil overfører oplysninger om kontaktpersoner og telefonopkald til bilens computer, som kan være vanskelig at slette. Vær opmærksom når du kobler dine enheder til din bils computer, og gør det aldrig, hvis der er tale om en leje- eller lånebil.

A: God	B: Bedre	C: Bedst
Slå kun Bluetooth til, når det skal benyttes. Undgå at tilknytte til enheder, du ikke selv ejer som f.eks. lejebiler. Husk at slå Bluetooth fra igen.	Hold altid Bluetooth slået fra.	It-afdelingen slår Bluetooth fra via en Mobile Device Management-løsning, og brugeren kan ikke slå den til.

11. Deling af data ved direkte trådløs forbindelse mellem mobile enheder

Direkte trådløs forbindelse til deling af data mellem mobile enheder kendes f.eks. under navnene på de platform-specifikke løsninger fra Apple (Airdrop), Microsoft (Near Share), Google (Files Go) m.fl. Deling af data direkte mellem mobile enheder kan ofte være bedre end delingstjenester, der går via internettet, fordi du herved mindsker muligheden for, at andre kan aflytte kommunikationen via nettet. Vær generelt opmærksom på ved brug af delingstjenester, at de skal slås fra umiddelbart efter brug. Dette gælder også f.eks. Bluetooth.

A: God	B: Bedre	C: Bedst
Brug en løsning der er krypteret og vær opmærksom på, at du forbinder dig til den rigtige anden mobile enhed.	Indstil din delingsfunktion til kun at kunne dele med enheder, der er i din telefonbog, så du kun deler med dem du kender.	Se 'Bedre'.

12. Slå lokalitetstjenester fra og skjul din placering

En telefon, tablet eller pc med GPS eller Wi-Fi kan registrere, hvor du befinder dig, også selvom du ikke bruger navigationen. Det kan afsløre, hvor du arbejder, hvor du bor og hvor du ofte færdes.

A: God	B: Bedre	C: Bedst
Begræns applikationers adgang til lokalitetsdata, og giv kun de mest nødvendige apps adgang. Del ikke oplysninger om din placering på sociale medier, herunder fitness-apps mv., især ikke under udlandsophold.	Slå lokalitetstjenester fra og slå dem kun til, når du skal bruge dem. Slå dem fra igen, når du er færdig med at bruge navigation.	It-afdelingen slår lokalitetstjenester fra via en Mobile Device Management-løsning, og brugeren kan ikke slå dem til.

13. Installér kun apps fra officielle tjenester

Malware, spionprogrammer og andre ondsindede applikationer kommer ofte via uofficielle distributionskanaler. Du bør derfor aldrig installere apps på dine mobile enheder, som kommer fra en ukendt tjeneste eller apps, der beder dig om at ændre sikkerhedsindstillingerne, for at du kan installere den.

A: God	B: Bedre	C: Bedst
Installér kun apps fra de officielle app-biblioteker som f.eks. Google Play, Apple App Store eller Microsoft Store	It-afdelingen begrænser installation af apps til forhåndsgodkendte (whitelistede) apps fra officielle app-butikker og eventuelt organisationens egen enterprise app-store.	Det er kun it-afdelingen, som kan installere apps på enheden.

14. Send krypterede SMSer

SMS-beskeder sendes uden ekstra kryptering over mobilnetværket. Det betyder, at beskederne er sårbare over for aflytning. Mobilsikkerheden er op til operatøren af mobilnetværket. Derfor bør man især i udlandet anvende beskedtjenester, som lægger ekstra kryptering på beskederne.

A: God	B: Bedre	C: Bedst
Brug krypterede sms-løsninger som f.eks. iMessage, hvor muligt.	Benyt en besked-app med end-to-end-kryptering, f.eks. Signal, WhatsApp e.lign.	Benyt en besked-tjeneste, hvor it-afdelingen administrerer end-to-end-krypteringen.

15. Adskil arbejde og privatliv

Du skal være opmærksom på, at både dine private, personlige data og information fra dit arbejde kan være følsomme eller værdifulde. Hvis du f.eks. mister din telefon, skal du være parat til også at miste de private fotos eller andre data, som ligger på telefonen. Sammenblanding af private og arbejdsmæssige konti og funktioner øger derfor din mobilsikkerhedsmæssige sårbarhed.

A: God	B: Bedre	C: Bedst
Brug så få personlige konti som muligt, og brug ikke enheden som varigt lager for private data. Tag backup af dine personlige data fra telefonen eller pc'en, så du ikke mister noget, hvis du mister telefonen.	Anvend en telefon eller bærbar pc, som kun bruges på en udlandsrejse og efterfølgende slettes. Sæt kun de mest nødvendige tjenester op på denne telefon.	Brug én telefon til arbejde og en anden telefon til dine private aktiviteter. Brug ikke den samme konto til opsætningen af begge telefoner.