Dansk Stalking Center

Sikkerhed på Android

OBS! Der kan være forskellige fremgangsmåder for de forskellige Androidmodeller.

Opdatering af telefonen
Det er vigtigt at holde telefonen opdateret med den nyeste software, da eventuelle sikkerhedsproblemer kan være blevet dækket i de seneste opdateringer.

1. Gå ind i indstillinger - ofte et symbol som dette 
2. Vælg menuen ”Om telefonen” eller ”Om enheden”
3. Under ”Android- version” vil du kunne se hvilken software version, der er installeret på din telefon.
4. Tryk på ”Systemopdateringer” for at søge efter eventuelle nye opdateringer til din telefon.

Skærmlås
Øg sikkerheden ved at tilføje en PIN kode, password eller mønsterkode til telefonen. Det kan være med til at forhindre, at stalkeren får adgang til at plante overvågningssoftware eller aflæse adgangskoder. Der findes en række måder at skærmlåse din enhed på Android. Først kan du vælge at angive en PIN-kode, altså en fire cifret kode, du selv har valgt.

Er du ikke tryg ved en fire cifret kode, kan du vælge adgangskode. Med adgangskode kan du selv angive en kode baseret på tal, bogstaver såvel som tegn. Koden skal dog minimum være på fire tegn. Generelt er reglen, at jo længere kode er, jo mere sikker.

På Android findes også muligheden for at skærmlåse med et mønster. Dette baserer sig på ni punkter, du personligt kan sammensætte i ét strøg. Igen er længden af mønstret afgørende for, hvor svær den er at genangive.

1. Gå ind indstillinger 
2. Vælg menuen ”Sikkerhed”
3. Under ”Skærmsikkerhed” vælger du ”Skærmlås” og vælger den type af skærmlås, du vil have. I nogle tilfælde ligger skærmlås separat under indstillinger → låseskærm.

Når du har aktiveret skærmlås, er det muligt at sætte funktion ”Lås automatisk” her kan man indstille tiden for, at skærmen automatisk skal låse f.eks. 5 sekunder efter dvale.

Kryptering
Hvis dine beskeder bliver læst, kan kryptering af teksten forhindre stalkeren i at få meningsfuldt indhold. Et eksempel på en app, der kan kryptere dine beskeder kunne være: https://play.google.com/ store/apps/details?id=org.thoughtcrime.securesms&utm_source= next.36kr.com.

Android telefoner har muligheden for at kryptere indholdet på mobilen. Dette betyder, at man er nødt til at låse skærmen op for at kunne forstå indholdet. Har du en ny android mobil vil du blive

tilbudt at få krypteret alt dit indhold i opstartsfasen. Har du ikke en ny telefon eller sidder du med ældre enheder, skal du:

1. Gå ind i indstillinger 
2. Vælg menuen ”Sikkerhed”.
3. Her finder du punktet ”krypter telefon” eller ”krypter enhed”. Har du en tablet, står der selvfølgelig ”krypter tablet”.

Telefonen bliver automatisk dekrypteret (gjort læselig), når du indtaster din kode. Den eneste anden måde at dekryptere telefonen, er ved at udføre en gendannelse af fabriksdata, hvilke sletter alle dine data, såsom kontakter, beskeder og billeder.

HUSK! at sætte mobilen til strøm, inden du begynder krypteringen, da processen kan tage lang tid og bruger meget strøm. Hvis mobilen løber tør for strøm, kan du risikere at miste nogle eller alle dine data.

OBS! Hvis du oplader din telefon via USB stik fremmede steder så vær opmærksom på fænomenet kaldet “Juice-Jacking” hvor der overføres malware gennem opladningsstikket.

Slå GPS’en fra
Slukker du for GPS’en, lukker du for adgangen til alle apps og der kan derfor være nogle funktioner, der ikke virker. Her er det muligt at tænde GPS’en, mens du har brug for den, og derefter slå den fra igen.

Undersøg om telefonen har haft et større strømforbrug end normalt, da dette kunne tyde på at en lokationstjeneste kører. Tjek alle apps og services, der er installeret og/eller kører på telefonen.

For at slukke for GPS’en skal du:

1. Åbne indstillinger 
2. Vælg menuen ”Placering” eller ”Placeringstjenester”
3. Vælg placering fra. Nogle gange kan den hedde Brug GPS-satellitter.

Man kan hurtigt tænde og slukke for GPS’en via Quick menuen, der kommer frem ved at stryge fingeren ned fra toppen af skærmen. Her kan du tænde og slukke GPS’en ved at trykke på  eller  . Du kan se om GPS’en er aktiv, hvis der er lys i symbolet.

Det er i nogle tilfælde også muligt at slette den tidligere placeringshistorik ved at:

1. Åbne indstillinger 
2. Vælg menuen ”Placering” eller ”Placeringstjenester”
3. Vælg ”Placeringshistorik”
4. Tryk på ”Slet placeringshistorik”

Hvis GPS'en er slået fra, og du bruger en app, der skal have adgang til din GPS, vil du få en besked om af slå GPS'en til. Det er vigtigt at huske, at når du går ud af app'en slår den ikke automatisk GPS'en fra igen. Det skal du gøre ved at følge ovenstående instruktioner.

Fjerne geotagging fra billeder

Nogle telefoner kan være sat op til at indsamle GPS data til billeder, så der er muligt at se, hvor de blev taget. Dette kan slås fra, nogle gange i placeringsmenuen, eller ved at gå ind på kamera app'en og gå ind i indstillinger og vælge GPS fra. Det kan se forskelligt ud fra telefon til telefon. Det kan være et symbol som dette  , eller det kan hedde geotagging, GPS-tag eller gem placering eller lign.

Find din telefon

På nyere Android telefoner kan telefonen være sat op med mulighed for at finde din telefon, hvis du har mistet den, eller den er blevet stjålet. Herfra er det muligt at finde mobilen via GPS'en, låse mobilen og gendanne fabriksindstillinger. Det er overordnet en god funktion, men det er muligt at udnytte disse funktioner til at spore en telefons placering, hvis andre får adgang til det. Det kan slås fra.

1. Gå ind i Google indstillinger (ikke det samme som indstillinger)  eller 
2. Vælg "Sikkerhed"
3. Under Android Enhedsadministrator fravælg "find denne enhed fra ekstern placering" (kan være slået fra hvis GPS'en er slået fra). Og fravælg "Tillad ekstern låsning og rydning"

Vær varsom, når du henter apps

Det er vigtigt at tænke sig om, når man henter apps fra Google Play eller lign. Som udgangspunkt bør der kun installeres apps fra Google Play Store. Der er mindre sandsynlighed for ondsindede apps bliver downloadet, men der er stadig en risiko. Når du henter en app, vil der komme en liste frem, der spørger om tilladelse til at benytte forskellige funktioner på mobilen eller tabletten. Her er det en god idé at overveje, om de tilladelser app'en ønsker giver mening. F.eks. giver det ikke mening for en lommelygte app at have adgang til din placering eller din mikrofon. Når en app er installeret, er det ikke muligt at ændre på tilladelserne. Det er også vigtigt at tænke over, om denne app er nødvendig for dig.

Det er muligt at se dine installerede apps og hvilke tilladelser de har.

1. Gå ind i indstillinger 
2. Vælg menuen "Apps" eller "Programmanager". Her får du en liste over de apps, der er installeret på din mobil eller tablet. Ved at trykke på en app f.eks. et spil, vil du i bunden kunne se, hvilke tilladelser den har. Øverst vil du have mulighed for at deaktivere eller afinstallere app'en

Sluk for Wi-Fi og Bluetooth

Ved at slukke for Wi-Fi og bluetooth kan du mindske sandsynligheden for, at andre får adgang til data fra din telefon.

Sluk for Wi-fi:

1. Gå ind i indstillinger 
2. Tryk på ”Wi-Fi”
3. Vælg ’fra’

Eller åben Quick menuen ved at stryge fingeren ned fra toppen af skærmen og trykke på 
eller 

Sluk for Bluetooth:

1. Gå ind i indstillinger 
2. Tryk på ”Bluetooth”
3. Vælg ’fra’

Eller åben Quick menuen ved at stryge fingeren ned fra toppen af skærmen og trykke på 

Opsætning af ny Android-telefon

Hvis du vælger at få en ny telefon, må du ikke overføre data direkte imellem telefonerne, da dette kan overføre stalking software. I stedet bør gamle ikke-inficerede backups anvendes, eller alternativt, hvis backuppen kan lægges på en Cloud som kan fjerne malware, så kan dele af backuppen downloades manuelt.

Når du starter din nye telefon, vil du blive bedt om en Google-konto. Hvis du ikke har en i forvejen, vil du blive bedt om at oprette en ny. Hvis du er bange for, at den vil blive hacket, kan du lave en ny brugerbaseret på en ny Gmail. Hvis den bliver hacket, er der således ikke adgang til f.eks. din private mail.

Check din Google-kontos gendannelsesindstillinger for at sikre at det kun er dig, som kan ændre password (hvem sendes det midlertidige login til). Del ikke passwords og andre koder med andre (dette inkluderer også familie og andre nære relationer) og specielt ikke Google-konto login. Det er ikke til at vide om koderne ender i hænderne på en (potentiel) stalker.

Gør Google sikkerhedsspørgsmål sværere at gætte ved at lave underlige svar, fx svaret “lilla” til spørgsmålet om hvor mange søskende du har. Grunden til dette er, at stalkeren meget vel kender personlige oplysninger og derfor ville kunne gætte det korrekte svar.

To-trins verifikation bør aktiveres (før infektion af telefonen), så stalkeren ikke ville kunne få adgang til den anvendte Google-konto uden at have adgang til telefonen også.

Du får mulighed for at forbinde mobilen til dit Wi-Fi. Det er en god idé at vælge fra, da det giver

mulighed for, at din mobil kan blive hacket, hvis stalkeren har eller får adgang til dit trådløse internet.

Lad ikke andre sætte din telefon op, da der er risiko for at denne person allerede stalker dig eller kunne komme til det i fremtiden.

Følg en opsætningsguide i stedet for at lade andre sætte din telefon op (eller slet ikke at sætte den op). Det hjælper med at sikre, at stalkeren ikke kan installere hemmelig software og koder kan holdes private.

Gem aldrig passwords på telefonen (Android tilbyder nogle gange at huske dit password). Hvis stalkeren får adgang til telefonen så er alle koderne allerede gemt og der vil være fri adgang til at ændre data, installere apps med mere.

Når du når frem til Google-tjenester, skal du fravælge følgende, da de alle sender informationer fra telefonen, som f.eks. hvor du befinder dig.

- Brug Googles placeringstjenester
- Hjælp med at forbedre placeringstjenester
- Hjælp med at forbedre din Android-oplevelse

Nulstil telefonen

Hvis du er bange for, at der er blevet installeret spyware eller virus på din telefon, kan du nulstille den. For at nulstille telefonen, skal du gemme alt det, du vil beholde fra mobilen ved enten at lægge det over på en computer, gemme det ned på et SD-kort eller lign eller lave en sikkerhedskopi til din Google-konto. Lav jævnligt sikkerhedskopier mens telefonen er ren således, at der ved en evt. gendannelse ikke mistes meget data.

Ved at fabriksgendanne telefonen slettes alle installerede apps og forhåbentlig også den software som udfører stalking handlinger. Vær dog opmærksom på, at du vil miste data og yderligere, at nogle apps måske kan overleve gendannelsen (Cerberus anti-tyveri påstår, at deres app kan overleve en gendannelse hvis telefonen var rooted[1])

Check om din telefon er blevet rooted (hvis du ikke selv har gjort det), da det kan tyde på, at tvivlsomme apps (som bl.a. kan bruges til stalking) er blevet installeret. Se [3] for hvordan du checker om din telefon er rooted.

Hvis der er mistanke om malware eller spyware, så prøv at installere en anti-virus app og kør en rens. Malwarebytes[5] påstår, at de i hvert fald kan identificere apps som “mSpy”, “PhoneSheriff” og “MobiStealth”, som alle kan bruges til digital overvågning og/eller fjernkontrol.

Lave en sikkerhedskopi

1. Gå ind i indstillinger 
2. Vælg menuen ”Sikkerhedskopiering/nulstilling”
3. Tænd for sikkerhedskopier data

[1] Forklaring af hvad “root” betyder: http://meremobil.dk/2014/08/ root-hvorfor-roote-android-baggrund/

HUSK! at tilslutte din telefon til det trådløse internet

For at nulstille telefonen skal du:

1. Gå ind i indstillinger 
2. Vælg menuen ”Sikkerhedskopiering/nulstilling”
3. Gendannelse af fabriksdata eller nulstil til fabriksstandard

Når du har nulstillet din telefon, vil du blive spurgt, om du vil gendanne din telefon, som den var før. Det skal du sige nej til, da du risikerer at geninstallere de programmer, der var problemet til at starte med. Du kan få adgang til din sikkerhedskopi ved at logge ind på din Google konto.