Aktivistguide til mobiltelefoner

Introduktion

Din mobiltelefon indeholder data om fx hvor du er, hvad du søger på, hvem du kommunikerer med og hvad I skriver om. Det er følsomme data som politiet kan bruge som bevismateriale mod dig og dine venner, hvis du skal i retten for en aktion. Det er altså ikke kun dit eget, men også dine venners privatliv og sikkerhed, der står på spil hvis politiet får fat i din telefon. Politiet har flere gange konfiskeret smartphones, så det er altså et middel de er villige til at tage i brug. Desuden vil vi gerne sikre at politiet ikke ved hvad vi skriver om generelt. Her er en guide til hvordan du kan gøre din telefon mere sikker.

Dette skriv er rettet mod smartphones. Hvis du har en dumbphone, er der ikke meget du kan gøre for at sikre den, så lad vær med at bruge den til fortrolig kommunikation.

Planlægning af aktioner

Kryptér

Et godt sted at starte er at bruge krypterede beskedtjenester og kryptere sin telefon. Bare det, gør en stor forskel.

Når man skriver almindelige SMS'er eller ringer, er det faktisk ret nemt for politiet at få adgang til dem, læse dem, se hvem du skriver med og hvor du er, også når de ikke har din telefon. Ved at skifte til en krypteret beskedtjeneste fx Signal, kan du skrive privat uden at nogen kan se det. Det hjælper dog ikke meget hvis politiet har din mobil og knækker din adgangskode på din låseskærm - derfor skal man ALTID huske at slette Signal-appen før hver aktion.

For at gøre det sværere at knække din adgangskode kan du kryptere din enhed. Det gøres i dine indstillinger og tager et par timer. Hver gang du slukker telefonen helt vil al information blive krypteret og når du genstarter telefonen skal du indtaste en adgangskode der så vil dekryptere den igen. Her er det vigtigt, at man slukker sin mobil helt før hver aktion.

Brug ikke fingeraftryk eller ansigtsgenkendelse

Hvis du bruger fingeraftryk eller ansigtsgenkendelse til at åbne din telefon, er den slet ikke sikker over for politiet. Hvis du ikke vil åbne telefonen frivilligt, har politiet nemlig lov til at anvende magt og tvinge din finger eller dit ansigt til at åbne den. Derfor skal du have en anden andgangskode, og den må gerne være stærk. En tekstkode er den stærkeste adgangskode, men tal kan også gøre det - sørg i øvrigt for at det ikke er en kode, der er nem at gætte.

Drop online kommunikation

Det bedste man kan gøre for sin online sikkerhed i forhold til politiet, er at mindske sine fodspor i første omgang. Skriv om I ikke skal drikke en kop kaffe, lad telefonen blive hjemme og planlæg en aktion i stedet. Prøv at lade være med at skrive noget som helst om aktionen online, især hvis I er

bange for at politiet vil tage sagen meget seriøst. Hvis der ikke er nogle beviser de kan finde frem til, kan I sove trygt om natten.

Læg telefonerne væk

Politiet kan hacke sig ind på din mobiltelefon, få adgang til mikrofonen og på den måde overvåge alt du siger i nærheden. Det er dyrt og teknisk svært for dem men de kan godt, og det firma der har produceret din telefon kan også. For at være på den sikre side anbefales det derfor at planlægge aktioner uden elektroniske devices i nærheden.

Det er også god stil at være opmærksom på om andrer er okay med det og informere dem om det, hvis du kommer hen til dem med en telefon i lommen.

Til aktionen

Lad telefonen blive hjemme!

Så simpelt og så nemt at glemme. Der har været mange aktioner hvor aktivister har haft deres mobiltelefoner med og fået dem med hjem igen. Men ligepludselig eskalerer politiet og så har man mistet sin primære forbindelse til resten af verden og givet politiet muligheden for at fremtrylle masser af bevismaterialer mod dig og dine venner.

Hvis du virkelig har brug for en telefon under aktionen, enten for at komme i kontakt med andre, livestreame eller tage billeder, bør du bruge en *burner-phone* eller en *aktionstelefon*. En burner eller en aktionstelefon er en telefon, som du kun bruger når du er i aktion, og den er altså helt ren for andet data. På den måde gør det ikke så meget, hvis politiet vælger at konfiskere den, for der er alligevel ikke noget sensitiv information på den. Du kan bruge en gammel, fabriksgenstartet mobil som burner.

Hvis du formoder at dit hjem vil blive ransaget

Politiet har sjældne gange valgt at ransage aktivisters hjem i forbindelse med deres anholdelse. Indtil videre er det kun sket et par gange i forbindelse med aktioner med en del højere juridisk risiko end den gennemsnitlige aktion (permanent maling på bygninger osv. eller IT-sager), men som sagt ved vi aldrig hvad politiet vil gøre.

Derfor er det en god ide at sørge for at ens hjem er politivenligt, før man tager til aktion. Brænd dine mødenotater, slet Signal og skaf din kalender, computer, telefon og andre devices af vejen. Et gemmested på et andet værelse kan være fint, men i visse tilfælde vil politiet vælge at gennemsøge hele huset. Politiet må ransage ens hjem uden først at få en dommerkendelse, hvis det er nødvendigt at gøre det med det samme. Men man kan altid kræve at få ransagningen prøvet i retten efterfølgende, og det anbefaler vi altid at man beder om!

Hvis det bliver besluttet at du blev udsat for en ulovlig ransagning, eller at du senere bliver frikendt, er der mange penge at hente i erstatning. Vi anbefaler, at man donerer sin erstatning til det solidariske aktivistnetværk Bødebanken.