VIGTIG VIDEN OM MOBILTELEFONER // IMPORTANT INFORMATION ON PHONES - VENDEPUNKTET 2022

Indholdsfortegnelse // Table of contents

Intro

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.

Til aktionen

Lad telefonen blive hjemme!

Så simpelt og så nemt at glemme. Der har været mange aktioner hvor rebeller 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, men XR sørger også for at have burner-dumbphones og burner-smartphones på lager.

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, og mon ikke de vælger at eskalere lidt op til Vendepunktet.

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 hvisse 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.

Important to know about mobile phones

Your mobile phone contains data with, among other things, your location, search log, contacts and messaging content. This is sensitive data that the police can use as evidence against you and your friends in court. It's not just your own privacy and security at stake if your phone's taken, but also that of your friends! The police have confiscated smartphones several times and are quite capable of doing it again. We'd like to keep them out of the loop! The information below will help you make your phone more secure.

Smartphone that is: if you've got a dumbphone there's not much that can be done to secure it, so please don't use it for confidential messaging.

Planning an action

Encrypting

A good place to start is to use an encrypted messaging services and encrypt your phone. Just doing that makes a big difference.

It's actually quite easy for the police to access phone calls, SMS's, read them, see who you are writing to and where you're at; even if they don't have your phone. By switching to an encrypted messaging service such as Signal, you can write privately without anyone taking a peek. But that won't work if the police confiscate your mobile and crack your lock screen password. You must ALWAYS remember to delete the Signal app before an action if you're taking your phone with you.

To make it harder to crack your password, you can encrypt your device. That's done in "settings" and takes a few hours. Each time you power off your mobile, all information will be encrypted and when you restart it you'll need to enter a password which will then decrypt it all once more. It's important to power off before each action!

Don't use finger or facial recognition

If you use finger or facial recognition to open your phone, the police can easily access it. If you won't voluntarily open it, they can legally force you to do so. You'll need to have a different password and it should be a strong one. A text code is the best password but numbers can work too - by the way, make sure it's not easy to guess.

Drop online communication

The best thing you can do for your online security regarding the police is to reduce your online footprint in the first place. Meet at a café, leave the phone at home and plan the action in person. Try not to write anything about the action online, especially if you're worried that the cops will be interested. If there's no evidence to dig up, you can sleep safely at night.

For the action

Leave your phone at home!

So simple BUT so easily forgotten. There've been many actions in which rebels have had their phones with them and brought them home safely, but the situation can escalate and suddenly you've lost your primary connection to the world and have given the police an opportunity to gather lots of evidence against you and your friends.

If you really need a phone during an action, to keep in contact with the others, livestream or take pictures, you should use a burner phone or an action phone. A burner or an action phone is one you only use at an action and is completely clean for other data. It doesn't matter if the police confiscate it, because there won't be any sensitive data on it. You can use an old, factory-restarted mobile as a burner, but XR generally has burner dumbphones and smartphones in stock.

If you suspect your home might be ransacked

The Police rarely choose to search the homes of activists in connection with their arrest and so far, it's only occurred a few times in connection with actions of high legal risk

(permanent painting on buildings, etc. or IT cases), but then you never know what the police will do and they might choose to escalate up to "Vendepunktet".

It's a good idea to make sure your home is police-friendly before taking action. Burn your notes, delete Signal and get your calendar, computer, phone and other devices out of the way. A hiding place in another room can be fine but in some cases the police will choose to search the entire house. They can search one's home without at first obtaining a judge's order if it's deemed necessary to do so immediately. But you can always demand a trial afterwards and we recommend that you do so!

If it's decided that you were subjected to an illegal search or that you will later be acquitted, you can receive a large sum by compensation. We recommend you donate all compensation in solidarity with the activist network BødeBanken.