CENTER FOR CYBERSIKKERHED

Rådgivning mod lokalitetssporing af mobiltelefoner

Baggrund

Fra vores mobiltelefoner, tablets og smarture kan vi i dag finde vej til det nærmeste pizzeria, holde styr på gennemsnitshastigheden på løbeturen, og se hvornår den kommende regnbyge rammer. En stor del af denne funktionalitet kræver, at en app ved, hvor mobiltelefonen befinder sig, og dermed også hvor vi selv bevæger os hen og opholder os i løbet af dagen. Vi tillader med andre ord en betydelig dataindsamling om vores daglige færden i bytte for den ønskede funktionalitet.

Med adgang til lokalitetsdata indsamlet fra apps er det muligt at finde ud af, hvor du bor, hvor du arbejder, hvem du mødes med, og hvor du færdes. Det skal du især være særligt opmærksom på, hvis du har en arbejdsfunktion, hvor det for eksempel af sikkerheds- eller privatlivsårsager er uhensigtsmæssigt at kunne identificere dig i forhold til arbejdsplads, arbejdsopgaver eller privatbolig.

Lokaliteten bestemmes ud fra flere kilder, der ofte anvendes i kombination: GPS, signalstyrke på mobilmaster, WiFi-netværk og Bluetooth. Det er mobiltelefonen, der holder styr på alt dette, og som stiller lokalitetsdata til rådighed for de apps, vi har valgt at installere, eller som er præinstalleret på den mobile enhed.

De apps, der har adgang til din lokalitet, tjener i nogle tilfælde penge på at sælge data om dig og din færden videre til andre. Når man først har givet en app adgang til lokalitetsdata, kan det derfor være svært at gennemskue eller have kontrol over, hvor data ender, hvem der køber adgang til data, og hvad data bruges til. Det gælder både for apps, der er gratis og for betalingsapps.

Hvad kan jeg gøre?

Hvis man vil begrænse, hvor meget af sin daglige færden man risikerer at dele med uvedkommende, bør nedenstående råd følges:

- Hold din mobiltelefon opdateret. Der er ofte bedre privatlivsbeskyttelse på opdaterede telefoner.
- Installer kun de apps du har brug for, og helst fra firmaer du kender.
- Afinstaller de apps du ikke anvender jævnligt.
- Læs grundigt, hvad en app beder om adgang til, og tag aktivt stilling til hvad du vil tillade.

- Giv kun apps adgang til lokalitetsdata, hvis funktionaliteten afhænger af det.
- Giv kun apps adgang til lokalitetsdata, når de anvendes aktivt.
- Gennemse med jævne mellemrum hvilke apps, der har adgang til din lokalitet.
- Sluk din telefon, inden du tager et sted hen, hvor du ikke vil kunne spores.
- Lad mobiltelefonen blive hjemme, hvis du vil være helt sikker på at undgå sporing.

Husk at:

- Ved brug af gratis apps betaler du ofte med dine personlige data.
- Mange apps fungerer fint uden at skulle have adgang til din lokalitet, selvom de beder om det.
- Nogle kort- og træningsapps gemmer lokalitetshistorik, hvis du ikke slår det fra.
- Delte billeder kan indeholde lokalitetsdata, eller afsløre hvor du er ud fra motivet eller dets baggrund.

Hvordan gør jeg?

- Du kan styre adgang til lokalitetsdata på din mobiltelefon ved at følge disse guides:
  - Android (Google): https://support.google.com/android/answer/6179507?hl=da
  - iOS (Apple): https://support.apple.com/da-dk/HT207092
- Du kan begrænse firmaernes evne til at sammenkæde solgte data om dig, ved at slå personligt tilpassede reklamer fra, som beskrevet i disse guides:
  - Android (Google): https://support.google.com/ads/answer/2662922?hl=da
  - iOS (Apple): https://support.apple.com/da-dk/HT202074

Mere information

CFCS og PET har sammen udgivet vejledningen: "Råd om sikkerhed på mobile enheder", der indeholder flere gode råd om mobilbrug. Vejledningen kan findes på CFCS' hjemmeside.

CENTER FOR CYBERSIKKERHED

Kastellet 30
2100 København Ø
Telefon: + 45 3332 5580
E-mail: cfcs@cfcs.dk
1. udgave juni 2021.