

Betalen met je persoonsgegevens

wat accepteer je wel en wat niet bij het downloaden van een app?

De vraag

Super handig als je telefoon automatisch je creditcardgegevens invult, foto's ordent op gezichtsherkenning, je login-gegevens van social media onthoudt en op basis van je agenda aangeeft hoe lang de reistijd naar je volgende afspraak is. In de meeste gevallen zijn deze apps zelfs gratis.. of betaal je er onbedoeld toch een hoge prijs voor? Want weet jij eigenlijk wat je accepteert bij het downloaden van een app? En tot welke van jouw gegevens de app nu automatisch toegang heeft?

Steeds meer apps hebben zonder dat jij het doorhebt toegang tot je (persoons-)gegevens via onder andere je locatiegegevens, belgegevens, foto's en internetgeschiedenis. Zonder overigens duidelijk uit te leggen wat er met deze informatie gedaan wordt. Wist je bijvoorbeeld dat veel van die (persoons-)gegevens worden gebruikt of gedeeld met derde partijen die je op hun beurt hierdoor gerichte reclame bieden voor hun producten en diensten? Kortom, deze (gratis) apps 'betaal' je dus met de goedkeuring voor het gebruiken en/of delen van je eigen (persoons-)gegevens. Op deze wijze worden met jouw gegevens opbrengsten gegenereerd op manieren die voor jou onbekend of misschien zelfs wel ongewenst zijn. Daarnaast hechten niet alle apps evenveel waarde aan je privacy. De verzameling van je gegevens is bij veel apps niet goed beveiligd. Dit biedt criminelen de kans achter je (persoons-)gegevens te komen. Denk bijvoorbeeld aan je locatiegegevens, dit is voor inbrekers ontzettend waardevolle informatie.

De uitdaging

Uiteraard bieden al deze apps je ook een hoop voordelen. Zo zijn er apps ontwikkeld voor het bieden van ontspanning tot het invullen van je belastingaangifte. Van het bedienen van de verwarming thuis tot het communiceren met vrienden aan de andere kant van de wereld. Bij al deze apps is het echter belangrijk om te weten hoe je ze veilig kunt gebruiken en daarmee voorkomt dat jouw (persoons-)gegevens 'op straat komen te liggen' en gemakkelijk bereikbaar zijn voor onbevoegden.

De oplossing

Het is bijna onmogelijk om te voorkomen dat apps je (persoons-)gegevens gebruiken. De enige oplossing is om ze simpelweg niet te gebruiken. Wanneer je dit wel doet, wees je dan bewust van een aantal zaken. De volgende tips kunnen je daarbij helpen:

- ▲ Krijg inzicht in de machtigingen die je geeft bij het downloaden van een app. Dan kun je op jouw beurt besluiten of jij het eens bent met het verzamelen, gebruiken en doorgeven van je (persoons-)gegevens.
- ▲ Check de recensies en het aantal downloads van een app voordat je deze installeert.
- ▲ Houd je apps up-to-date. Zodra er een achterdeurtje in je app niet goed is dichtgedaan, maken hackers hier direct gebruik van.
- ▲ Laat apps je accountgegevens niet automatisch invullen. Dit verkleint het risico dat anderen toegang hebben tot je accountgegevens.
- ▲ Blokkeer Wi-Fi-tracking door je Wi-Fi actief uit te zetten als je niet in de buurt bent van een bekend netwerk.
- ▲ Installeer een antivirus app met een privacy-scanner, deze geeft inzicht in en controleert de machtigingen van apps.
- ▲ Besef, bij het gebruik van apps op openbare Wi-Fi-netwerken, tot welke gegevens de app toegang heeft en eventuele hackers via het Wi-Fi-netwerk dus ook.

Meer weten?

Bezoek onze website www.mindyourstep.info voor meer tips en tricks op privacy- en informatieveiligheidsvlak.
Of neem direct contact op met Marijn Berndes via marijn@soulmade.nl of door te bellen naar 0162-430345.

