WWW.MINDYOURSTEP.INFO

Betalen met je persoonsgegevens

Waar moet je op letten bij het downloaden en gebruiken van apps?

De vraag

We maken steeds meer gebruik van apps.
Terwijl je naar het station loopt check je via 9292 welke bus je moet hebben, je stuurt via Whatsapp een berichtje naar het thuisfront wanneer je thuis bent, vervolgens maak je via je Bankieren app geld over zodat je via de app van Thuisbezorgd een pizza kan bestellen. En eenmaal thuis aangekomen zet je een foto van je bestelde pizza op Instagram en Facebook.

Enorm handig die apps dus. Maar er kleven ook risico's aan het gebruik hiervan. Waar moet je op letten bij het downloaden en gebruiken van apps?

De uitdaging

Apps willen steeds meer van je weten. Ze vragen tegenwoordig veel meer informatie van je dan eigenlijk noodzakelijk is voor het gebruik van de app. Grote kans dat je, zonder dat je het door hebt, apps toegang geeft tot je foto's, muziek, locatie, camera, microfoon en/of contacten terwijl dit helemaal nergens voor nodig is. Alle informatie die via deze kanalen over jou wordt verzameld, wordt ergens opgeslagen. Gevolg hiervan is dat je dus niet weet wie deze informatie over jou bezit en waar die gegevens voor worden gebruikt.
Hiernaast staan er ook namaak-apps in de appstore. De makers van deze namaak-apps hopen dat onwetende mensen de app installeren, zodat ze op die manier persoonsgegevens kunnen verkrijgen. Deze apps worden vaak zo geloofwaardig gemaakt, dat gebruikers zonder dat ze door hebben hun betaal- en persoonsgegevens invoeren.

De oplossing

Waar moet je op letten bij het gebruiken en downloaden van apps? We geven je een aantal tips:

- Voor sommige apps moet je inloggen via Facebook. Maak hier een nepprofiel voor aan, waarin je geen gegevens van jezelf vermelt. Apps met toegang tot Facebook kunnen namelijk zelfs wachtwoorden opslaan of verzoeken versturen via Facebook. Hiernaast geef je de app hiermee veel meer informatie dan eigenlijk noodzakelijk is.
- Is er een nieuwe update voor een app beschikbaar? Voer deze meteen uit!
- Betaalde apps kunnen net zo veilig/onveilig zijn als onbetaalde apps. Dus wees ook alert bij het downloaden en gebruiken van betaalde apps.
- Denk bij het downloaden van iedere app goed na tot welke onderdelen je een app toegang wilt verlenen. Vraagt een app te veel persoonlijke gegevens? Download deze dan niet.
- In sommige gevallen is een app niet wat het lijkt. Controleer daarom hoe vaak een app is gedownload en hoeveel sterren de app heeft, voordat je hem zelf installeert.
- Waarschijnlijk klik je de privacyvoorwaarden snel weg zodra deze op je scherm verschijnen. Toch is het handig deze door te lezen, zodat je precies weet wat voor gegevens de app van je nodig heeft en opslaat.
- Pas je privacy instelling per app aan. Je kan bij 'instellingen' in je telefoon, precies zien waar je reeds gedownloade apps toegang voor hebt gegeven. Check dit regelmatig kritisch.
- Zorg dat je een virusscanner gebruikt voor je telefoon. Mocht je dan toch per ongeluk een gevaarlijke app hebben gedownload, dan kan de virusscanner in de meeste gevallen de virus of malware onderscheppen.

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.