# Bring Your Own Device (BYOD)

## Wat is het?

- Zakelijk en privégebruik lopen door elkaar wanneer je de eigen laptop, tablet of smartphone voor zowel werk als privédoeleinden gebruikt.
- BYOD biedt voordelen, zoals het verhogen van de productiviteit, meer tevreden werknemers en dalende hardware kosten. Maar slechts een kwart van de werkgevers heeft afspraken gemaakt over BYOD. En dat is niet zonder risico voor zowel jou als werkgever, als voor de werknemer.
- Je hebt als werkgever weinig tot geen controle over de beveiliging van de bedrijfsgegevens op het digitale apparaat van je werknemer en er kunnen vragen ontstaan over de verantwoordelijkheid bij datalekken, virussen en andere problemen.

## Welke gevolgen heeft het voor jouw bedrijf?

- Als je werknemer zijn tablet op vakantie verliest of zijn smartphone in de trein laat liggen, loop je daarmee het risico dat je bedrijfsinformatie zoals klantgegevens, patentaanvragen of uitbreidingsplannen kwijtraakt.
- Het gebruik van privé-apparaten in een zakelijke setting kan leiden tot een kwetsbare ICT-bedrijfsvoering. Cybercriminelen kunnen deze kwetsbaarheid gebruiken om binnen te dringen in jouw organisatie om zo bijvoorbeeld ransomware te plaatsen.
- Via onveilige (openbare) wifi-netwerken kan makkelijk toegang verkregen worden tot de zakelijke informatie op het eigen apparaat.

## Hoe kun je het voorkomen?

- Stel een **BYOD-beleid** op om kwetsbaarheden binnen jouw bedrijf te voorkomen.
- Licht je medewerkers voor over de **voordelen én risico's van BYOD**.
- Wijs werknemers op de risico's van inloggen op openbare wifi-netwerken.
- Zorg voor een **incident response plan** (een stappenplan in het geval van incidenten).
- Op de website van het **Digital Trust Center (DTC)** staan nog meer handige tips over BYOD.

**Alert Online** richt zich op het creëren van bewustwording rondom online veiligheid, op het vergroten van kennis over online veiligheid en op het stimuleren van cybersecure gedrag.
De Alert Online spiekbriefjes zijn gebaseerd op de **cyberspiekbriefjes voor Tweede Kamerleden**.
**Kijk voor meer tips en informatie op veiliginternetten.nl**