Wat doen wij om Zoom veilig te gebruiken?

Privacy staat hoog op onze agenda en daarom nemen wij maatregelen om Zoom op een verantwoorde manier te gebruiken.

Zoom kwam aan het begin van het jaar in opspraak omdat het bedrijf data van gebruikers zou delen met Facebook, dit werd onder andere mogelijk door de 'inloggen met Facebook'-functionaliteit. Daarnaast waren er verschillende incidenten op het gebied van 'Zoombombing'. Meerdere mensen konden inloggen in een Zoom meeting waarvoor zij niet uitgenodigd waren doordat de meeting-id was gelekt. Maar… Zoom heeft er alles aan gedaan om de software goed te beveiligen waardoor bovenstaande problemen niet meer voorkomen. Zo geeft Zoom in haar privacy statement aan geen data van gebruikers te delen en meerdere maatregelen te hebben getroffen om de software veilig te maken.

Op deze pagina leggen wij uit hoe wij Zoom op een verantwoorde manier gebruiken en hoe jij als deelnemer aan de online sessies het programma verantwoord kan gebruiken.

Wat doen **wij** om de veiligheid te verantwoorden?

- Om de veiligheid te vergroten hebben wij een betaalde versie van Zoom en hebben wij een verwerkersovereenkomst met Zoom afgesloten. De online sessies zijn standaard versleuteld.
- Voor elke online sessie genereren wij een wachtwoord die ingevoerd moet worden bij virtuele binnenkomst. Dit is de eerste stap die wij nemen om ongewenst bezoek buiten de virtuele deur te houden.
- Daarnaast maken wij voor alle online sessies gebruik van een virtuele wachtkamer om ongewenst bezoek te voorkomen. De moderator van de online sessie controleert aan de hand van de aanmeldlijst of de naam van een deelnemer en de naam bij aanmelding overeenkomen. Wij vragen de deelnemers dan ook om in ieder geval 15 minuten van tevoren in te loggen.
- 15 minuten na de aftrap van een online sessie worden de virtuele deuren gesloten.,Het is dan niet meer mogelijk om toe te treden tot een online sessie.
- Ook hebben wij aanvullende instellingen zo ingesteld dat het gebruik van Zoom op een zo privacyvriendelijk mogelijke manier gebruikt wordt en voldoet aan de regels omtrent de AVG.

Meer informatie over hoe Zoom haar veiligheid garandeert aan haar gebruikers? Bekijk het hier.

Wat zou **jij** kunnen doen om jouw veiligheid bij het gebruik van Zoom te kunnen bewaken?

- Allereerst is het goed om na te denken over hetgeen dat besproken gaat worden in een Zoom meeting. Aangezien het een online cursus is en geen bedrijfsgevoelige informatie gedeeld zal worden, is het geen probleem voor jou om Zoom te gebruiken.
- Een veiligheidsmaatregel die iedereen altijd zou moeten hebben: een webcamplakkertje.
- Verspreid de inloggegevens niet. Dat gaat ten koste van je eigen privacy en die van anderen. Aangezien wij de wachtkamer beheren aan de hand van de deelnemerslijst kan iemand die zich niet aangemeld heeft ook niet deelnemen.
- Sluit het programma Zoom goed af nadat wij de online sessie hebben beëindigd.