Beste collega,

Iddink Learning Materials BV is op donderdag 11 april getroffen door een cyberaanval. Hierover heeft Iddink ons na de aanval geïnformeerd. Iddink is voor onze school de leverancier van schoolboeken, (digitaal) leermateriaal en schoolspullen. Iddink heeft over deze cyberaanval [een persbericht](https://www.iddinkgroup.com/over-ons/pers-nieuws/) verstuurd.

In de database van Iddink is informatie opgenomen van ouders en leerlingen voor de bestelling en levering van lesmateriaal en schoolspullen. Recent is gebleken dat ook informatie van medewerkers van scholen, die voor de school orders of bestellingen plaatsen voor (digitaal) leer- en lesmaterialen, is opgenomen in de database van Iddink. Dat betekent dat de gegevens van deze medewerkers die hebben ingelogd bij Iddink, in handen kunnen zijn gekomen van hackers. Het gaat hierbij om accountinformatie zoals gebruikersnaam/inlognaam, naam van de medewerker, school/opleiding en contactgegevens (telefoonnummer, e-mailadres).

We hebben de leerlingen en hun ouders van onze school eerder geïnformeerd dat als zij een of meerdere bestellingen hebben geplaatst bij Iddink, hun gegevens betrokken kunnen zijn bij de cyberbaanval. Via dit bericht brengen wij jou op de hoogte dat ook jouw gegevens betrokken kunnen zijn bij de cyberaanval als jij – in het verleden – voor of namens school hebt ingelogd bij Iddink.

De informatie van onze medewerkers had natuurlijk niet in verkeerde handen mogen komen. Iddink werkt hard aan het oplossen van het probleem en om te achterhalen welke informatie is verkregen. De gegevens van medewerkers moeten, net als de gegevens van onze leerlingen en ouders, veilig blijven.

Omdat er mogelijk misbruik kan worden gemaakt van de verkregen informatie, willen we je waarschuwen om alert te zijn op bijvoorbeeld phishing mails of andere manieren van misbruik waarmee hackers proberen informatie of geld van jou te krijgen. Controleer of e-mail betrouwbaar is en klik niet zomaar op een link in een e-mail die je niet vertrouwt.

Als je gebruik hebt gemaakt van een wachtwoord om in te loggen bij Iddink en dat wachtwoord is hetzelfde wachtwoord dat je gebruikt om in te loggen bij andere websites en diensten (bijvoorbeeld online bankieren), dan is het advies om dat wachtwoord te wijzigen. Het is verstandig om steeds een ander, uniek wachtwoord te gebruiken. Dan weet je zeker dat hackers geen misbruik kunnen maken van de gestolen informatie.

We hopen en verwachten dat dit geen negatieve consequenties zal hebben. Mocht je wel nadeel ondervinden van deze ransomware-aanval bij Iddink, dan kan je daarover contact opnemen met je leidinggevende of directeur/rector.

Omdat er onbedoeld persoonlijke informatie terecht is gekomen bij personen die deze informatie niet mochten krijgen, hebben we een melding gedaan van dit datalek bij de privacytoezichthouder Autoriteit Persoonsgegevens. Je kunt over het datalek zelf, en over de melding contact opnemen met onze functionaris voor gegevensbescherming [NAAM] (via [MAIL]).

Ik hoop je met dit bericht voldoende te hebben geïnformeerd. Mocht je vragen hebben, dan kun je uiteraard contact met mij opnemen.

Met vriendelijke groet

[SCHOOLBESTUUR/RECTOR/DIRECTEUR]

[CONTACTGEGEVENS]