**VOORBEELDBRIEF (OUD) LEERLINGEN EN OUDERS OVER MISBRUIK GEGEVENS**

Onderwerp: Let op phishing e-mails vanuit Iddink

Beste leerling en ouder(s)/verzorger(s),

U bent de laatste tijd geïnformeerd over de cyberaanval op Iddink Learning Materials B.V. van 11 april. In een eerder brief waarschuwden wij u voor mogelijke phishingmails. Helaas hebben wij vernomen dat er op dit moment phishingmails worden verstuurd uit naam van Iddink Learning Materials. Dit betekent dat er actief misbruik wordt gemaakt van de gegevens die bij de hack gestolen zijn.

Een phishingmail is een nepmail die vaak wordt verstuurd namens (zogenaamd) een officiële instantie met het verzoek om informatie te geven of om een bedrag te betalen. Het versturen van phishingmails is een populaire manier onder criminelen om persoonlijke gegevens en geld van mensen te ontfutselen (ze ‘vissen’ naar deze informatie). In dit geval is de phishingmail zogenaamd afkomstig van Iddink Learning Materials of bijvoorbeeld van de school.

Iddink verstuurt op dit moment geen e-mail naar leerlingen en hun ouders. Als dat wel het geval is, dan zullen we u hierover (vooraf) duidelijk informeren.

**We verzoeken u daarom nogmaals extra alert te zijn op mogelijke phishingberichten. Iddink Learning Materials B.V. en onze school vragen u op dit moment niet om persoonlijke gegevens te verstrekken via e-mail en een link, of om betalingen te doen.**

**Ons advies aan u is:**

* Let op e-mails, sms-berichten of telefoontjes waarin om persoonlijke gegevens wordt gevraagd, zelfs als het lijkt alsof het bericht van Iddink of de school is. Iddink en de school vragen nooit om op deze manier persoonlijke gegevens te verstrekken.
* Ga niet in op verzoeken in een e-mail om in te loggen of om te betalen voor schoolboeken. De school zal de leerlingen en hun ouders vooraf informeren als er actie wordt gevraagd om schoolboeken en lesmateriaal te bestellen of te betalen.
* Pas op voor e-mails die hyperlinks of bijlagen bevatten, klik niet op deze links tenzij je hebt vastgesteld dat de e-mail betrouwbaar is en de link te vertrouwen is (dit kan bijvoorbeeld door de link te controleren via [www.checkjelinkje.nl](http://www.checkjelinkje.nl)).
* Pas op voor e-mails of sms-berichten met spelfouten, vreemde afzenders, ander dan Nederlands taalgebruik of iets anders ongewoons.

Zoals we u eerder hebben gemeld, blijft het belangrijk om verschillende wachtwoorden te gebruiken. Gebruikt u het wachtwoord van Iddink ook op andere websites? Dan is het belangrijk dat u het wachtwoord overal wijzigt in een nieuw, uniek wachtwoord.

Meer informatie en advies over veilig internetten staat op de website van de Rijksoverheid [www.veiliginternetten.nl](http://www.veiliginternetten.nl).

Mocht u nog vragen hebben, neem dan contact op met [contactpersoon school toevoegen]. Voor vragen over het datalek bij Iddink kunt u contact opnemen met de functionaris voor gegevensbescherming (FG) van onze school (fg@SCHOOL.NL)

Ik hoop u met dit bericht voldoende te hebben geïnformeerd.

Met vriendelijke groet

[afzender school toevoegen]

[functie toevoegen]