Onderwerp: Belangrijk: je gegevens bij Gymnastiekvereniging DOS Castricum zijn mogelijk in verkeerde handen

Beste DOS leden,

We laten je weten dat er een datalek is geweest bij AllUnited. Dat is het systeem waarmee Gymnastiekvereniging DOS Castricum de ledenadministratie bijhoudt. Daarbij zijn ook jouw gegevens buitgemaakt. Dat vinden we heel vervelend. In dit bericht lees je wat er is gebeurd en waar je op moet letten.

Wat is er gebeurd?

Op maandagavond 9 november 2026 heeft een onbekende aanvaller misbruik gemaakt van een fout in de software van AllUnited. Daardoor kon hij gegevens uit de database kopiëren. Dat ging om gegevens van alle verenigingen die AllUnited gebruiken, ook die van onze vereniging. AllUnited heeft het lek op 10 november ontdekt en dezelfde dag gedicht.

Om welke gegevens gaat het?

- Naam, adres en woonplaats
- E-mailadres en telefoonnummer
- Geboortedatum en geboorteplaats
- Rekeningnummer (IBAN)
- Als je een AllUnited account hebt: je inloggegevens
- Overige gegevens in je ledenrecord, zoals lidnummer, team, functie of opmerkingen

Ben je ouder of verzorger van een jeugdlid? Dan gaat het ook om de gegevens van je kind.

Wat kunnen de gevolgen zijn?

Criminelen kunnen deze gegevens gebruiken om je te misleiden. Ze kunnen bijvoorbeeld:

- Berichten sturen die van Gymnastiekvereniging DOS Castricum of AllUnited lijken te komen;
- Vragen om contributie, een boete of een ander bedrag te betalen via een link;
- Een betaalverzoek sturen;
- Zich met jouw gegevens als jou voordoen.

Wat kun je doen?

- Let op bij betaalverzoeken.
- Indien van toepassing, wijzig je wachtwoord als je het wachtwoord van AllUnited / de ClubApp / ons ledenportaal ook op andere plekken gebruikt. Je wachtwoord bij ons wordt opnieuw ingesteld; daarover krijg je een apart bericht.

Hieronder lees je hoe zulke nepberichten er mogelijk uitzien.

Wat doen wij en AllUnited?

- AllUnited heeft het lek gedicht.
- AllUnited stelt alle wachtwoorden opnieuw in en voert extra beveiliging en controles in.
- Wij hebben het datalek gemeld bij de Autoriteit Persoonsgegevens.
- We versturen NOOIT betaalverzoeken per e-mail dus wees daar alert op.

Vragen?

Neem contact op met Marcia Schermer (secretaris) via info@doscastricum.nl. We vinden het vervelend dat dit is gebeurd. We houden je op de hoogte als er nieuwe informatie is. Ontvangt u een verdachte mail namens ons, dan horen we dat graag zodat we de andere leden dan kunnen waarschuwen.

Groet,

Bestuur DOS Castricum

Zo werkt phishing: uitleg voor clubs en leden

De voorbeelden zijn verzonnen, net als de namen en bedragen.

Waarom dit nu speelt
Van elk lid heeft de aanvaller de naam, het adres, de geboortedatum, het telefoonnummer, het e-mailadres, het rekeningnummer en de club. Met al die echte gegevens kan hij berichten maken die er net zo uitzien als een bericht van je club of je bank. Daar trappen mensen veel sneller in dan in een slordige spammail.
Voorbeeld 1: een mail ‘van de club’
Van: Ledenadministratie VV De Zwaluwen ledenadministratie@zwaluwen-leden.nl
Onderwerp: Je contributie is niet geïncasseerd

Beste Sanne de Vries,

De incasso van je contributie (€ 87,50) van je rekening NL•• •••• •••• ••12 34 is niet gelukt. Betaal binnen 48 uur via de link hieronder. Anders wordt je lidmaatschap stopgezet en kun je niet meer meedoen met de training op dinsdag.

[Nu betalen]

Wat klopt er niet:

Het afzenderadres lijkt op dat van de club, maar is het niet.
Er staan echte gegevens in: je naam, de laatste cijfers van je rekening en je trainingsdag. Dat bewijst niets, want die gegevens zijn gestolen.
Er is haast (‘binnen 48 uur’) en een dreiging (‘lidmaatschap stopgezet’).

De link gaat naar een betaalpagina van de oplichter, niet van de club.

Voorbeeld 2: een sms of WhatsApp

Hoi Sanne, hier Mark van de ledenadministratie van De Zwaluwen. Je geboortedatum 14-03-1988 klopt niet in ons systeem. Wil je even inloggen via deze link om het te controleren?

Wat klopt er niet:

De club vraagt nooit via een link om in te loggen of iets te ‘controleren’.
Dat de afzender je geboortedatum kent, maakt het bericht niet echt.

Voorbeeld 3: een telefoontje ‘van de bank’
Iemand belt en zegt dat hij van je bank is. Hij noemt je naam, je adres en je rekeningnummer en zegt dat er verdachte afschrijvingen zijn. Om je geld veilig te stellen moet je een code doorgeven of geld overmaken naar een ‘veilige rekening’.

Wat klopt er niet:

Een bank vraagt nooit om codes en laat je nooit geld overmaken naar een andere rekening. Hang op en bel je bank zelf, via het nummer op je pas of de website.

De vier regels

Je club vraagt nooit per mail, sms of WhatsApp om je wachtwoord, een code of je rekeningnummer.
Twijfel je? Klik niet op de link, maar ga zelf naar de website van je club of bel de club.
Kijk je rekening na op afschrijvingen die je niet kent. Een incasso kun je in je bankapp terugdraaien: binnen 8 weken zonder reden, en binnen 13 maanden als je er nooit toestemming voor gaf.
Toch betaald of iets ingevuld? Bel meteen je bank en meld het bij de Fraudehelpdesk.