Belangrijke mededeling: datalek bij AllUnited

Wees alert op verdachte mails, links en banktransacties. Lees hieronder wat je kunt doen

Wij willen onze leden en betrokkenen informeren over een beveiligingsincident bij AllUnited, het administratiesysteem dat Sportvereniging Hou Vast gebruikt voor de ledenadministratie.

Wat is er gebeurd?

Op maandagavond 9 november heeft een onbevoegde persoon misbruik gemaakt van een kwetsbaarheid in de software van AllUnited. Via een inschrijfformulier op de website van een vereniging heeft deze persoon toegang gekregen tot een server van AllUnited. Vervolgens zijn persoonsgegevens uit de database gekopieerd.

Het incident werd op dinsdag 10 november ontdekt. AllUnited heeft de betreffende kwetsbaarheid dezelfde dag verholpen.

Helaas heeft dit incident ook gevolgen voor Sportvereniging Hou Vast. De gegevens van onze vereniging maakten onderdeel uit van de database die is getroffen.

Welke gegevens zijn mogelijk buitgemaakt?

Volgens de informatie die wij van AllUnited hebben ontvangen, kunnen de volgende persoonsgegevens zijn buitgemaakt:

- **Leden:** naam, adres, geboortedatum, telefoonnummer, e-mailadres en IBAN (bankrekeningnummer).
- **Aanvullende ledengegevens:** ook andere gegevens die in de ledenadministratie zijn opgeslagen, waaronder eventuele vrije notities en tijdelijke wachtwoorden.
- **Inschrijvingen via onze website:** naam, e-mailadres, telefoonnummer, geboortedatum en IBAN.
- **Gebruikers van de verenigingsadministratie:** naam, e-mailadres, telefoonnummer en het versleutelde wachtwoord.

Wat kun je zelf doen?

Hoewel AllUnited de kwetsbaarheid inmiddels heeft verholpen, adviseren wij onze leden om de komende periode extra alert te zijn op mogelijk misbruik van hun persoonsgegevens.

Wij adviseren het volgende:

- **Wees alert op verdachte berichten.** Let goed op onverwachte e-mails, sms-berichten en telefoontjes waarin om persoonlijke gegevens, wachtwoorden of bankgegevens wordt gevraagd. Klik niet zomaar op links en open geen verdachte bijlagen.
- **Deel nooit persoonlijke gegevens.** Geef nooit zomaar wachtwoorden, pincodes of bankgegevens door via e-mail, telefoon of sms. Ook niet wanneer iemand beweert namens de vereniging, AllUnited of de bank contact op te nemen.
- **Controleer je bankrekening.** Omdat ook IBAN-gegevens mogelijk zijn buitgemaakt, adviseren wij je de komende tijd je bankafschriften en rekening regelmatig te controleren. Let op onbekende of verdachte afschrijvingen. Neem bij twijfel direct contact op met je bank.
- **Wijzig waar nodig je wachtwoord.** Gebruik je hetzelfde wachtwoord voor meerdere websites of diensten? Wij adviseren dit wachtwoord op die andere websites te wijzigen. Kies daarbij steeds een uniek en sterk wachtwoord.
- **Wees alert op gerichte oplichting.** Omdat mogelijk ook persoonlijke gegevens zoals naam, adres, geboortedatum en telefoonnummer zijn buitgemaakt, kunnen oplichters deze informatie gebruiken om berichten geloofwaardiger te laten lijken. Laat je hierdoor niet onder druk zetten.

Hoe nu verder?

Wij vinden het bijzonder vervelend dat dit heeft kunnen gebeuren. De bescherming van de persoonsgegevens van onze leden vinden wij belangrijk en wij betreuren dat deze gegevens mogelijk in verkeerde handen zijn gekomen.

AllUnited heeft de beveiligingsfout inmiddels verholpen. Wij volgen de berichtgeving en verdere ontwikkelingen rondom dit incident nauwlettend.

Mocht er nieuwe relevante informatie beschikbaar komen, dan zullen wij onze leden hierover informeren via onze website.

Heb je vragen of zorgen naar aanleiding van dit bericht? Neem dan contact op met het bestuur van Sportvereniging Hou Vast.

Bestuur Sportvereniging Hou Vast



2. 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

1. Je club vraagt nooit per mail, sms of WhatsApp om je wachtwoord, een code of je rekeningnummer.
2. Twijfel je? Klik niet op de link, maar ga zelf naar de website van je club of bel de club.
3. 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.