New York Pizza waarschuwt voor 'phishing' mails.
Ondanks al onze veiligheidsmaatregelen hebben wij begin deze week helaas te maken gehad met een hack van de systemen van een van onze leveranciers, waarbij ook uw gegevens geraakt zijn. Wij leggen u graag uit wat er is gebeurd, om welke gegevens het gaat, welke maatregelen wij hebben genomen en wat u zelf kunt doen om te voorkomen dat u slachtoffer wordt van een phishing poging.

LET OP:
Druk niet op links, reageer niet op mails afkomstig van de verzender 'noreply@newyorkpizza.nl'. Mails waarover u twijfelt: reageer er niet op!

Wat is er gebeurd?
Afgelopen zondagnacht op maandagochtend ontvingen wij enkele mails van een hacker. Deze hacker beweert dat hij een grote hoeveelheid klantgegevens heeft ontvreemd van New York Pizza, en dreigde deze gegevens te publiceren of te verkopen.

Wij hebben snel onderzoek ingesteld. Wij hebben moeten vaststellen dat waarschijnlijk ook klantgegevens zijn ontvreemd uit onze databases door de aanvaller. Wij hebben het incident vervolgens meteen als datalek bestempeld en gemeld bij de Autoriteit Persoonsgegevens. Wij zullen tevens aangifte doen bij de politie. Daarnaast zijn wij samen met forensische experts gestart met het dichten van de kwetsbaarheid en hebben wij diverse andere maatregelen genomen ter bescherming van onze klantgegevens. Het incident heeft gelukkig geen impact op ons bestelproces. Onze filialen blijven gewoon open. U kunt dus nog gewoon uw favoriete pizza bij ons blijven bestellen.

Om welke gegevens gaat het?
Uit ons onderzoek is gebleken dat het gaat om uw naam, het bezorgadres, email adres, telefoonnummer, welke pizza's u heeft besteld, uw gecodeerde (gehashte) wachtwoord indien u een account bij ons heeft, en in een klein aantal gevallen ook om uw geboortedatum in verband met verjaardag bestellingen. In onze databases staan overigens geen bankrekeningnummers of creditcard gegevens van onze klanten. U hoeft zich daarom geen zorgen te maken dat die gegevens in verkeerde handen zijn gekomen.

Welke maatregelen hebben wij getroffen?
We zijn zo snel mogelijk gestart met het informeren van onze klanten en medewerkers. Ook hebben wij de partijen met wie wij samenwerken geïnformeerd. Daarnaast hebben wij externe specialisten ingeschakeld die het incident onderzoeken, wie achter de aanval zit, en hoe dit in de toekomst kan worden voorkomen.

Wat betekent dit incident voor u?
Doordat uw gegevens in handen zijn van de aanvaller, loopt u het risico dat de aanvaller uw gegevens publiceert of dat u het slachtoffer wordt van oplichting door middel van bijvoorbeeld een phishing mail. Het is mogelijk dat u telefonisch of per e-mail wordt benaderd. Zij kunnen dan vragen om extra gegevens of u benaderen om een betaling te doen. Ons nadrukkelijke advies is om daar niet op in te gaan en altijd alert te blijven op oplichting of identiteitsfraude. **Indien u een account bij ons heeft adviseren wij u om uw wachtwoord hiervoor te wijzigen.**

U kunt identiteitsfraude melden bij het Centraal Meldpunt Identiteitsfraude (CMI) van de Rijksoverheid: https://www.rijksoverheid.nl/contact/contactgids/centraal-meld-en-informatiepunt-identiteitsfraude-en-fouten-cmi

Ook adviseren wij u altijd aangifte bij de politie te doen als u slachtoffer wordt van cybercriminaliteit.

Contact
Wij kunnen ons voorstellen dat u met vragen zit. U kunt uw vragen mailen naar: vragen@newyorkpizza.nl. Wij bieden eenieder die hier mogelijk hinder van ondervindt onze oprechte excuses aan voor het ontstane ongemak.