Beste klant,

Door een ransomware-aanval is een datalek ontstaan bij Rima Adviesgroep.
Daardoor kunnen wij niet in ons systeem en is informatie van onze klanten gelekt.
Onze IT-specialisten hebben de criminelen direct uit het systeem gezet. Ook is er een meerfactor-authenticatie ingesteld voor extra beveiliging.

Graag informeren wij u verder over de mogelijke gevolgen van deze aanval.

Welke informatie is gelekt?

Ons klantenprogramma is met een extra wachtwoord beveiligd, daarom is niet duidelijk welke informatie precies gelekt is.
Het is mogelijk dat het om onderstaande gegevens gaat:

- Naam
- Adres
- Telefoonnummer
- E-mailadres
- Documentatie

Wat betekent dit voor jou?

Criminelen kunnen jouw contactgegevens misbruiken, bijvoorbeeld voor 'phishing'.
Phishing is het stelen van (betaal)gegevens via nepberichten.
Je kunt een e-mail ontvangen waarvan het lijkt dat deze bijvoorbeeld van een bank, pakketdienst of een incassobureau komt. Meestal proberen ze je in deze berichten te overtuigen op een link te klikken. Via deze link kunnen ze gegevens van je ontfutselen. Het is ook mogelijk dat je een virus of nieuwe ransom-ware binnenhaalt.

Criminelen kunnen je ook bellen of je een sms/appje sturen. De crimineel doet zich dan bijvoorbeeld voor als bankmedewerker of familielid. Je kunt de vraag krijgen om geld over te maken, wachtwoorden te noemen of software te downloaden op jouw computer.

Criminelen kunnen zich ook voordoen als jou. Je ontvangt bijvoorbeeld pakketjes die je niet besteld hebt, je contacten ontvangen e-mails van jou die je niet verstuurd hebt en je ontdekt dat er met je DigiD is ingelogd op een moment dat je dat niet hebt gedaan.

Wat kan je zelf doen?

- ➲ Let de komende tijd goed op bij het openen van links in e-mails, sms'jes en appjes;
- ➲ Wees alert op telefoontjes van banken/bedrijven en signalen van identiteitsfraude;
- ➲ Wijzig wachtwoorden van belangrijke websites zoals mijn.overheid.nl of DigiD.

Onderstaande tips kunnen je daarbij helpen:

- Negeer e-mails of berichten van een onbekende afzender;
- Controleer (afzenders van) een e-mail op taal- en typefouten. Nepberichten bevatten vaak fouten;
- Open geen bijlages van een onbekende afzender;
- Laat je niet misleiden door woorden als 'urgent', 'dringend' en 'betalingsachterstand';
- Bel geen telefoonnummers in een bericht, maar zoek het juiste nummer op en bel zelf. Dit geldt ook als je gebeld wordt;

- Krijg je een wachtmelding bij het internetbankieren of duurt het erg lang voordat de nieuwe pagina opent, sluit dan de website;
- Gebruik een goede virusscanner en browser op je apparaten.

Wat kan je doen als het onverhoopt tóch misgaat?

Meestal kan het niet zo veel kwaad als je per ongeluk klikt op een phishinglinkje. Het gaat pas echt fout als je iets invult op of downloadt van de nepwebsite waar je op terecht komt of als je een foute bijlage opent. Heb je al bepaalde gegevens prijsgegeven?

- ➲ Trek direct aan de bel bij het betrokken bedrijf;
- ➲ Waarschuw direct je bank als het om bankgegevens gaat;
- ➲ Ben je geld kwijtgeraakt? Doe dan aangifte bij de politie;
- ➲ Ben je slachtoffer geworden van identiteitsfraude? Doe ook dan aangifte bij de politie en vraag een nieuw legitimatiebewijs aan bij je gemeente;
- ➲ Heb je een wachtwoord ingevuld op een nepwebsite? Verander dit wachtwoord dan meteen in een nieuw sterk wachtwoord. (Als je dit ook elders gebruikt, pas het dan ook daar aan.).

Meer informatie?

Wat kan ik doen tegen phishing? | Rijksoverheid.nl
Identiteitsfraude | Rijksoverheid.nl