

Veiligheid in de Buurt

- Tegenwoordig maken criminelen handig gebruik van de mogelijkheden van Kunstmatige Intelligentie (AI) en Internet / WhatsApp
- Hieronder enige voorbeelden van oplichting en wat u er tegen kunt doen
 - ◆ Phishing en Internet Fraude
 - ◆ WhatsApp Fraude
 - ◆ Babbeltrucs
 - ◆ Inbraak en Diefstal

Phishing / internetfraude

- Phishing is oplichting via het internet, er zijn verschillende varianten. Criminelen bouwen websites na van banken, grootwinkelbedrijven **of sturen u gerichte e-mails of berichten.**
- In alle gevallen probeert de oplichter u te verleiden uw inloggegevens af te geven.
- Met deze geheime gegevens kan de oplichter onder uw naam inloggen. Op die manier kan de oplichter bijvoorbeeld geld van uw rekening afschrijven, of aankopen doen onder uw naam en rekeningnummer.



Phishing / Internetfraude voorbeeld:

Van: Rabobank [mailto:bankzakenl@rabobank.nl]

Verzonden: zondag 9 oktober 2016 17:58

Aan: [e-mailadres]

Onderwerp: Laatste herinnering: Uw aanvraag is nog niet verwerkt, voorkom een geblokkeerde betaalpas



Rabobank

Geachte relatie,

Uit onze administratie is gebleken dat u nog geen gebruik maakt van onze nieuwe betaalpas. De nieuwe betaalpas is beter beveiligd tegen frauduleuze praktijken en voldoet zich aan de Europese veiligheidsvoorschriften betreft bankzaken. Met de nieuwe betaalpas kunt u vertrouwd, veilig en gemakkelijk betalen en geld opnemen zoals u gewend bent en contactloos betalen in meer dan 12.000 winkels in heel Europa. Ook bent u beter beschermd tegen skimming en pinpas-fraude bij geldautomaten.

Het gebruik van uw huidige betaalpas wordt gedeactiveerd. In verband met de veiligheid van onze klanten is het verplicht uw huidige betaalpas te vervangen. Wij bieden onze klanten de mogelijkheid aan om dit kosteloos te doen. [Klik hier](#) om kosteloos uw nieuwe betaalpas aan te vragen en volg de benodigde stappen om uw aanvraag te voltooien. U ontvangt uw nieuwe betaalpas binnen **2 werkdagen** per post toegezonden.

Zolang u nog niet in bezit bent van een nieuwe betaalpas kunt u helaas nog geen gebruik maken van onze nieuwe dienstverlening.

Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd en van dienst te zijn geweest.

Alvast hartelijk dank voor uw medewerking.

Met vriendelijke groet,
Rabobank

Afdeling Internetbankieren
<http://rabobank.nl.condoclima.com/rabooaanvraag/inloggen.html>

- Urgentie: laatste herinnering.
- Urgentie: Binnen 2 werkdagen.
- Klik “**hier**”.
- Het domein is niet van de “Rabobank” maar van “Condoclima” zoals onderin te zien.

Wat te doen bij: Phishing / Internetfraude

- Klik **nooit** op links in een phishing e-mail. Waarschuw ook altijd de Fraudehelpdesk en de organisatie uit wiens naam u de mail krijgt.
- Gebruik een goede virusscanner en browser.
- Pas op bij een algemene aanhef als 'Geachte klant' bij betaal- of bankzaken.
- Let op taalfouten



WhatsApp-fraude

- De oplichters doen alsof ze een familielid, vriend of kennis zijn en halen slachtoffers over door smoesjes te gebruiken om privégegevens te delen of geld over te maken. De schade van WhatsApp-fraude bij sommige slachtoffers is soms tienduizenden euro's per dag.



Wat te doen bij: WhatsApp-fraude

- Om WhatsApp-fraude te voorkomen, zou je het beste de desbetreffende persoon eerst telefonisch even kunnen spreken voordat je geld overmaakt.
- Soms wordt het bedrog pas dagen later door de oplichter voortgezet. Bel die bekende via het nieuwe nummer en als dat niet lukt, gebruik dan het oude nummer. Vervang het oude telefoonnummer pas nadat je hem of haar mondeling hebt gesproken én herkend.
- Zit er een link voor een betaalverzoek in een hulpvraagbericht (bijvoorbeeld voor een Tikkie)? **Klik daar dan niet op!**



Babbeltrucs

- Onbekenden bellen bij u aan en gebruiken een mooie smoes om binnen te komen. Vervolgens stelen zij uw geld of andere waardevolle bezittingen.
- Soms gebeurt dat in combinatie met bedreiging of geweld.
- Babbeltrucs zijn bedoeld om mensen op te lichten. Het gebeurt voornamelijk aan de deur en bij pinautomaten.



LET OP **BABBELTRUCS**

- Laat onbekenden nooit binnen
- Bewaar waardevolle spullen op een veilige plek of huur bijvoorbeeld een kluis bij de bank
- Merkt u dat er iets is weggenomen?
Doe dan altijd aangifte!

politie.nl/babbeltrucs

Wat te doen bij: een Babbeltruc

- Wees voorzichtig en doe niet zomaar voor iedereen open. Kijk eerst wie er voor de deur staat. Als u toch besluit om de deur open te doen, gebruik dan een kierstandhouder.
- Twijfelt u? Bel dan 0900-8844. In nood kunt u bellen met 112.



Wat te doen bij: een woninginbraak

- Bel altijd 112 bij een verdachte situatie. U kent uw eigen buurt het beste, dus als u het niet vertrouwt, is dat niet voor niets.
- Laat als het donker is en u niet thuis bent een lamp aan. Dan lijkt het alsof er iemand aanwezig is. Stel hiervoor bijvoorbeeld een automatische lichtsakelaar in.
- Sluit ramen en deuren goed af, ook als u maar even weg bent. Draai de deur ook altijd op slot.
- Gebruik goedgekeurde sloten, ook ivm uw verzekering
- Heeft u een achterom? Doe de poort ook goed op slot en zorg voor verlichting in de tuin.
- Leg kostbare apparatuur, zoals laptops en iPads, uit het zicht.
- Heeft u struiken rondom het huis? Zorg ervoor dat deze kort zijn, zodat het huis voor burens en voorbijgangers goed te zien is.
- Zorg dat er geen ladders, containers of andere hulpmiddelen bij uw woning staan die het makkelijk maken om naar binnen te klimmen.
- Een schuifpui is inbraakgevoelig. Breng hiervoor een geschikt slot aan.
- Verstop geen huissleutels onder een deurmat of in een bloempot. Dit zijn ook voor inbrekers geen 'geheime' plaatsen.
- Hang geen adreslabel aan uw sleutel(bos) of zichtbaar aan uw koffers op reis
- Kondig niet uw vakanties aan op FaceBook etc.