WhatsApp; voorkom fraude

Handleiding van Helpmij.nl

Auteur: leofact

maart 2019

WhatsApp is een zeer populaire berichtendienst getuige het enorme aantal gebruikers. Het is met 11,9 miljoen gebruikers met voorsprong de grootste berichtendienst van Nederland en wereldwijd zijn er meer dan 1,5 miljard actieve gebruikers. Complete families over de hele wereld staan in verbinding met elkaar via deze populaire app.

Ook bedrijven bieden vaak een mogelijkheid aan om contact via WhatsApp te leggen. Een vraag is op die manier eenvoudig en snel gesteld. Behalve voor het gemak gebruiken we de berichtendienst ook voor onze veiligheid. Veel wijken zetten daarvoor de WhatsApp buurtpreventie in. De borden die daarvoor waarschuwen, zijn inmiddels overbekend. Ook in het betaalverkeer maken we in toenemende mate gebruik van deze vertrouwde dienst. Dat gebeurt meestal in de vorm van een link naar een iDeal betaling. Bijvoorbeeld via Tikkie; een app waarmee je eenvoudig een rekening deelt met een groep mensen.

Keerzijde

De mateloze populariteit heeft echter een keerzijde; criminelen zijn er brood in gaan zien om je via WhatsApp geld afhandig te maken. In een toenemend aantal gevallen lukt het ze om op die manier flinke bedragen buit te maken. Het gaat daarbij soms om duizenden euro's. Het betreft hier internetcriminaliteit en die is vaak lastig op te sporen. Dit omdat de dader zijn snode plannen overal ter de wereld kan uitvoeren. Deze vorm van criminaliteit is overigens mogelijk bij alle berichtendiensten, inclusief e-mail. Reden genoeg dus om zeer terughoudend te zijn met betaling via deze diensten.

Nooit meer doen?

Na het lezen van deze serieuze waarschuwingen kom je mogelijk tot de conclusie dat je beter nooit meer betalingen kunt doen die op deze manier binnen komen. Dat is echter een beetje te kort door de bocht. Met een alerte houding en gewapend met de juiste kennis kun je op een relatief veilige manier toch nog gebruik maken van deze mogelijkheid om betalingen te doen. Het geeft immers ook gebruiksgemak en, laten we wel wezen; ook als je met de portemonnee op zak loopt, moet je alert zijn. Het bij je dragen van contact geld trekt net zo goed criminelen aan.

Hoe deze vorm van WhatsApp-criminaliteit werkt en vooral wat je eraan kunt doen, lees je in dit artikel.

Hoe werkt het?

Er zijn op het moment verschillende manieren waarmee een poging kan worden gedaan om je geld af te troggelen:

- **Via een iDeal-link naar een vals adres van een Phishing-site**
  De crimineel neemt contact met je op, bijvoorbeeld via Marktplaats en laat je een betaling doen via een toegestuurde link. Vaak wordt als smoes opgegeven dat op die manier je identiteit wordt gecontroleerd. Er wordt dan gevraagd om een eurocent over te maken. Je wordt dan echter niet naar de iDeal-website gestuurd, maar naar een nagemaakte site die nauwelijks van de echte is te onderscheiden. Het gaat de crimineel dan niet om de betaling, maar om de gegevens die je daar invoert. Deze gegevens gebruikt hij vervolgens om je rekening leeg te halen voor je er nog iets tegen kunt doen.

- **Een betaalverzoek van een onbekende**

Je krijgt een betaalverzoek, bijvoorbeeld via Tikkie, waarin wordt gevraagd om een bepaald bedrag over te maken. Dit komt echter van een onbekende die jou probeert te verleiden om geld over te maken met als enige doel om daar op een eenvoudige manier rijker van te worden.

- **Een zielig verhaal**
  Iemand benadert je met een zielig verhaal of juist met een verhaal waar jij geld aan kan verdienen. Dat kan bijvoorbeeld een erfenis zijn van die onbekende oom in het buitenland. Je moet dan eerst wel even een bepaald bedrag overmaken….

- **Accountdiefstal**
  Dit is een geraffineerde vorm van oplichting die via WhatsApp wordt uitgevoerd. Je wordt via WhatsApp benaderd door een bekende die in moeilijkheden lijkt te zitten. Deze persoon is bijvoorbeeld in het buitenland beroofd of in het ziekenhuis terecht gekomen en heeft nu dringend geld nodig; of je dat maar ASAP wilt overmaken. Het lastige is dat dit bericht echt van je eigen kennis of familielid lijkt te komen. Die persoon was waarschijnlijk inderdaad op vakantie in het genoemde land en daardoor lijken de appjes maar al te waar. Mogelijk wil je uit een reflex maar al te graag de gevraagde hulp bieden. Helaas zal ook nu weer blijken dat je naar je geld kunt fluiten. Er is wederom sprake van een oplichter. Die heeft op slinkse wijze het account van de voor jou bekende persoon overgenomen. Hierdoor kan deze ellendeling alle chats lezen en weet hij precies wat er allemaal speelt. Hij hoeft vervolgens maar een contactpersoon uit te zoeken en een mooi verhaal te verzinnen dat klopt met de chats waar hij nu inzage in heeft. De crimineel neemt hiervoor het WhatsApp-account over van de voor jou bekende persoon door net te doen alsof hij het account overzet naar een nieuwe telefoon. Vervolgens laat hij je via de chat weten dat je bekende nu een nieuw nummer heeft. Daarna probeert hij je met een mooi verhaal in de val te lokken. Verderop lees je hoe deze crimineel ook jouw account zou kunnen overnemen en hoe je dit eenvoudig voorkomt.

Tegenspel

Het blijkt dus helaas mogelijk dat je op geraffineerde wijze flinke bedragen afhandig wordt gemaakt. Helpmij Magazine zou echter Helpmij Magazine niet zijn wanneer we niet een aantal tips hadden waarmee je kunt voorkomen dat je zelf (weer?) slachtoffer wordt van deze vervelende en slimme lieden:

1. **Check de afzender**
   Controleer altijd de afzender van een betaalverzoek. Google eventueel de naam en het telefoonnummer om te controleren of er sprake is van een bekende oplichter. Wantrouw onbekende verzoekers.

2. **Check de link**
   Controleer altijd eerst waar een link heen gaat, door de muis erboven te laten zweven of deze even “vast te houden” op een telefoon. Vreemde link? Twijfel? Niet klikken!

3. **Check de reden**
   Controleer de reden van het betaalverzoek, ook als het om een bekende gaat. Was je wel bij dat etentje, ben je daar wel lid van, klopt dit bedrag wel?

4. **Check het verhaal**
   Is het verzoek ingepakt in een verhaal? Controleer dat dan: is het van een onbekende? Negeer het gewoon! Is het van een bekende? Controleer dan of het inderdaad om die persoon gaat. Zeker als er net een nieuw nummer is toegevoegd. Bel dat nummer en bel voor de zekerheid ook het oude nummer. Stel specifieke vragen die alleen de bekende kan weten. Let er daarbij wel op dat de criminelen ook bijvoorbeeld Facebook checken om informatie te achterhalen. Helemaal geen contact te krijgen? Doe dan niets of probeer via andere wegen de ware identiteit te achterhalen van de persoon die je heeft benaderd. Laat hem jou bellen, of neem contact op met gezamenlijke kennissen of familieleden. Pas dan wel op dat ook zij niet in dezelfde val zijn getrapt.

5. **Meld fraude**
   Merk je iets op wat niet in de haak is, meldt het dan altijd en doe eventueel aangifte (zie de linken onderaan dit artikel). Waarschuw daarnaast eventuele andere betrokkenen. Ze zullen je dankbaar zijn!

Accountdiefstal

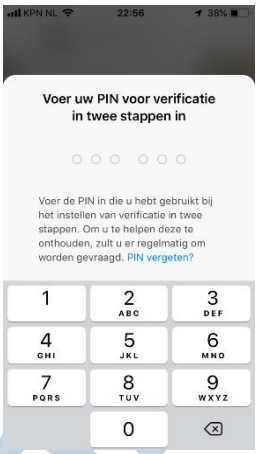
Je kunt op vrij eenvoudige wijze voorkomen dat je zelf slachtoffer wordt van een WhatsApp account-diefstal. Wanneer je weet hoe dat in zijn werk gaat, is het eenvoudiger te herkennen.
De crimineel gaat als eerste uit van je telefoonnummer. Daar is hij mogelijk achter gekomen via Phishing of via een hack van een collega-crimineel; gegevens worden onderling doorverkocht. Vervolgens probeert hij het account naar een eigen nummer over te zetten. Daarvoor is een code nodig. Deze probeert hij met een slim smoesje van je los te peuteren. Bijvoorbeeld met het verhaal dat hij een fout heeft gemaakt in het telefoonnummer bij het overzetten van het account van zijn opa of oma. Als je daar in trapt en de code doorgeeft, kan hij vervolgens je account overnemen en vanuit de back-up al je chats en contactpersonen laden. Eventueel kan hij die ook nog eens op Facebook op zoeken. Wanneer hij al die informatie vervolgens bij elkaar brengt, is het niet ze heel moeilijk meer om een goed, geloofwaardig verhaal te verzinnen om bij één (of meerdere) contactpersonen geld los te peuteren. Lukt het niet bij de één, dan misschien bij de ander….

Account beveiligen

Wanneer je met deze kennis gewapend bent, is het niet moeilijk om te bedenken hoe je jezelf beveiligd tegen het ongewenst overnemen van je account; geef nooit en te nimmer een pin of andere code door aan derden. Wie dan ook! Op deze manier voorkom je al veel vormen van (identiteits-) fraude.

Daarnaast kun je bij WhatsApp een tweede beveiligings-laag inschakelen opdat het vrijwel onmogelijk wordt dat je account ongewild wordt overgenomen. Schakel daarvoor bij de instellingen (via het tandwieltje in WhatsApp zelf) onder **Account** > **Verificatie in twee stappen** in. Je dient dan

een pincode van 6 cijfers in te voeren. Je account is nu dubbel beveiligd. Deze vorm van beveiliging is aan te bevelen bij alle accounts waarbij dat maar mogelijk is.



Ieder voordeel…

Natuurlijk moet je deze pincode goed onthouden. WhatsApp wil je daar (iets té) graag bij helpen en vraagt daarom op onverwachte momenten die pincode wanneer je de app opent. Dit met de gedachte dat als je de code maar vaak genoeg moet invoeren, je deze vanzelf goed onthoudt. Dat blijkt te kloppen. Helaas gaat je irritatieniveau daar waarschijnlijk ook flink van omhoog als je weer eens een keer die pincode in moet voeren, terwijl je deze al lang uit je hoofd weet. Wil je dit niet, dan kun je sinds de laatste update van WhatsApp voor iOS in plaats van een pincode Touch ID instellen bij een daarvoor geschikte iPhone (vanaf de 5S). Dat doe je ook onder **Account** bij de instellingen van WhatsApp zelf, maar nu kies je voor de optie **Privacy** > **Schermvergrendeling**. Schakel hier **Touch ID** in. Mocht het een internet-snoodaard ooit lukken om je account over te nemen dan zal hij er niets mee kunnen zonder jouw vingerafdruk.

Ten slotte

Internetcriminaliteit is een vervelende manier om je geld of gegevens af te troggelen door onbekende en ongrijpbare daders. Een gelukje is dat bij deze vorm je hersens niet kunnen worden ingeslagen zoals bij “gewone” criminaliteit helaas weleens gebeurt. Daarnaast kun je jezelf met enige oppassendheid goed tegen WhatsApp-criminaliteit beveiligen. Na het lezen van dit artikel ben je gewaarschuwd, weet je hoe het te voorkomen en ben je hopelijk beter bewapend wanneer het jou eens overkomt. Ondanks alles toch erin getrapt? Pak ze terug en doe aangifte!

Linken

- Fraudehelpdesk: WhatsApp-oplichters
- Fraudeheldesk: fraude melden
- Politie: Internetoplichting
- Politie: fraude met betaalmiddelen
- Politie: controleer gegevens
- Politie: aangifte doen
- iDeal: fraude herkennen
- ConsuWijzer: veilig online winkelen
- Nepvariant van Tikkie

Afbeeldingen van PXshare, Pixabay, Wikimedia, Flickr en eigen afbeeldingen