

WhatsApp

Extra bescherming tegen fraude

De media staat op dit moment vol van meldingen over WhatsAppⁱ-fraude.

<https://nos.nl/artikel/2351982-fraude-met-whatsapp-stijgt-fors-vier-keer-zoveel-meldingen-als-in-2019.html>

Bewustwording van deze fraude is een eerste stap. Naast de vorm van fraude die wordt beschreven in bovenstaande link is er ook een vorm van fraude die probeert om je WhatsApp-account over te nemen. In deze blog wordt uitgelegd hoe je een extra bescherming kan inbouwen om dit zoveel mogelijk tegen te gaan.

Toch slachtoffer geworden? Schaam je niet en doe aangifte!

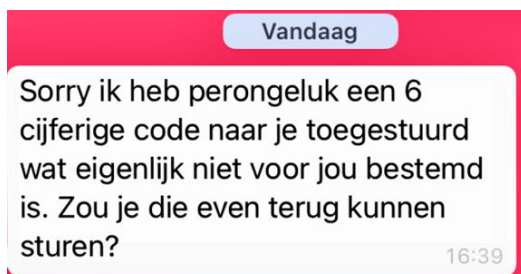
<https://www.politie.nl/aangifte-of-melding-doen/aangifte-van-vriend-in-noodfraude.html>

Extra bescherming

Cybercriminelen proberen via een WhatsApp-bericht te vissen naar je accountgegevens. Een hele kwalijke zaak, want als de cybercriminelen je WhatsApp-account hebben overgenomen is het een koud kunstje om al je contacten binnen jouw WhatsApp-omgeving te bestoken met fraudeleuze berichten. Daarnaast zullen ze zeker proberen om ook toegang te krijgen tot de accounts van al je contacten.

Hoe ziet zo'n aanval eruit?

Je krijgt een bericht van een bestaand WhatsApp-contact. Een vriend of bekende stuurt je ineens een bericht met onderstaande strekking:



En natuurlijk help je een bekende snel uit de nood. De code is snel gestuurd, maar kort daarna is je WhatsApp-account onder controle van cybercriminelen.

Wat is er gebeurd?

Het WhatsApp-account van je contactpersoon is in handen gekomen van cybercriminelen. Die hebben het adresboek van je contactpersoon uitgelezen en zijn zo aan jouw naam en telefoonnummer gekomen. En die informatie is gebruikt om voor jouw account een herstelcode aan te vragen.

Kijk hiervoor eens op de website van WhatsApp waarin o.a. onderstaande is beschreven over deze herstelcode: *“Om je account te beschermen, stuurt WhatsApp je een melding wanneer iemand een WhatsApp-account probeert te registreren met jouw telefoonnummer. Bescherm je account en deel nooit je verificatiecode met anderen.*

Wanneer je deze melding ontvangt, wil dat zeggen dat iemand jouw telefoonnummer heeft ingevoerd en een registratiecode heeft aangevraagd. Dit gebeurt vaak als iemand je nummer per ongeluk heeft ingevoerd in een poging hun eigen nummer te registreren, maar het kan ook gebeuren als iemand je account probeert over te nemen.”

<https://faq.whatsapp.com/general/received-verification-code-without-requesting-it/?lang=nl>

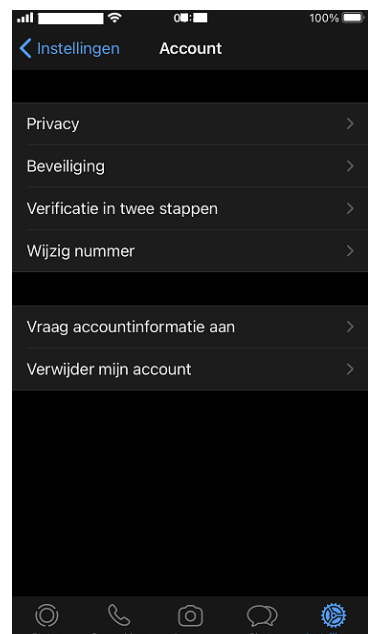
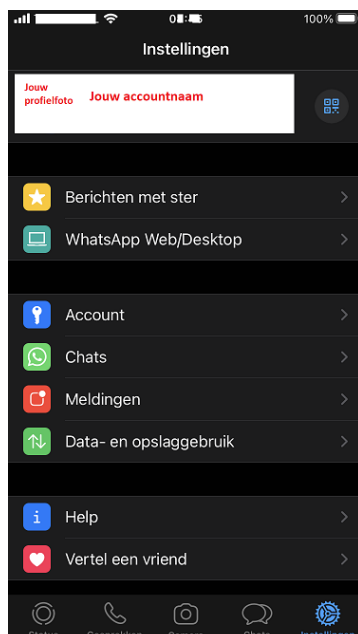
De cybercriminelen hebben dus een herstelcode van jouw account aangevraagd en vervolgens via een bestaand contactpersoon gevraagd om de herstelcode met hen te delen.

En geloof me, in een onbedachtzaam moment kan het iedereen overkomen dat ze de gevraagde code delen met een bekende.

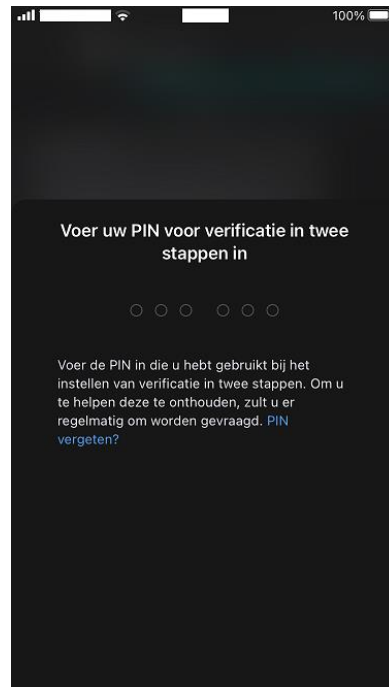
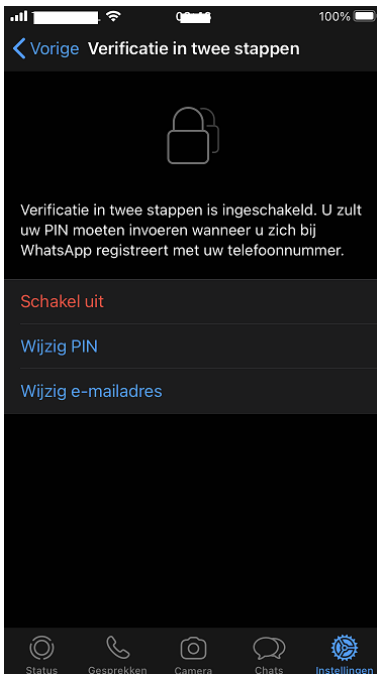
Extra bescherming

Om diefstal van je accountgegevens tegen te gaan heeft WhatsApp een extra laag van bescherming ingebouwd die vrij eenvoudig is te activeren. Het advies is dan ook om deze bescherming (tweefactor authenticatie) aan te zetten!

Klik in WhatsApp op het Instellingen, en vervolgens op Account. Dit geeft de volgende twee schermen:



Klik vervolgens op Verificatie in twee stappen:



Kies een 6-cijferige pincode en onthoud deze goed. Deze pincode zorgt voor een extra laag bescherming en zorgt ervoor dat cybercriminelen er niet met jouw WhatsApp-account vandoor kunnen gaan.

In WhatsApp kan zal je ook op gezette tijden de gekozen pincode moeten invoeren. Op deze manier maken we het de cybercriminelen een stuk moeilijker en onze digitale omgeving een stuk veiliger.

Harry Steen, Information Security Officer, Unit4 Bedrijfssoftware

ⁱ WhatsApp is een applicatie waarmee je snel en eenvoudig berichten kan versturen en bellen op smartphones over de hele wereld. Denk goed na of en hoe je gevoelige data deelt met andere. Maak je zakelijk gebruik van WhatsApp? Houd je dan aan het bedrijfsbeleid bij het delen van gevoelige informatie via apps en het internet.