



#### PREMIUM

Gwen Busseniers legt uit hoe oplichters te werk gaan via valse weggeefacties om je cryptomunten afhandig te maken. © Getty Images/ Steven Richardson

**“Ik maakte mijn vrouw wakker en vertelde dat ik een grote fout had gemaakt”: Sebastian verloor een half miljoen euro aan bitcoin in enkele seconden tijd**

Bekende koppen die als wilde weldoeners met bitcoins strooien om je rijker te maken? Vergeet het maar. Toch lopen heel wat nietsvermoedende mensen – met een hardnekkige droom om snel en eenvoudig rijk te worden – in de zogenaamde ‘giveaway’-scam en valse spelformules op het internet. Gwen Busseniers van de

CryptoSchool en auteur van 'Bitcoin & Crypto' over de spelregels die je daar net niet in doen lopen.

Thomas Rosseel 16-06-22, 09:09 Laatste update: 16-06-22, 15:52

- 
- 

Mij overkomt het niet. Het is snel gezegd en gedacht als het gaat over oplichting via het internet. Sebastian redeneerde ook zo, tot een doordeweeks avondje op Twitter uitdraaide op een ware nachtmerrie. Sebastian had enkele jaren eerder voor het eerst geïnvesteerd in bitcoin: zo'n 40.000 euro. De tien bitcoins in zijn wallet waren doorheen de jaren uitgegroeid tot bijna een half miljoen euro. De man deed eerder – met schaamrood op de wangen – zijn verhaal bij de BBC.

“Het moment waarop ik bijna een half miljoen euro verloor, zal ik me altijd blijven herinneren, met evenveel woede als schaamte. Ik liet me leiden door hebzucht”, blikte de man terug. Die avond kreeg hij een Twitter-melding met nieuws over Elon Musk. De Tesla-topman is zelf een fervent crypto-investeerder. “Musk twitterde: ‘Dojo 4 Doge?’ en ik vroeg me af wat het betekende. Daaronder stonden reacties, van mensen met een quasi identiek profiel als Musk, met een link naar een nieuw evenement. Ik klikte erop en zag dat Musk er bitcoin weggaf.”



De advertentie voor de giveaway-scam oogde professioneel. © rv

### **Het maximale**

Sebastian was op een professioneel ogende website beland, waar de bitcoin-weggeefactie volop bezig leek te zijn. “Er was een timer die aftelde en de website beloofde de deelnemers dat ze hun geld konden verdubbelen”, schetst Sebastian. De wedstrijd werd zogezegd geleid door het Tesla-team van Elon Musk, dat mensen uitnodigde om bedragen te sturen van 0,1 bitcoin (toen een kleine 5.000 euro waard) tot 20 bitcoins (zo’n 1.000.000 euro in die periode). “Ik controleerde nogmaals het verificatielogo naast de naam van Musk en besloot uiteindelijk mijn 10 bitcoins te sturen. Haal er het maximale uit”, dacht ik.

Terwijl de timer de minutenlang afliep, wachtte Sebastian tot het bedrag in zijn bitcoin-portemonnee zou belanden. Iedere 30 seconden vernieuwde hij zijn scherm. “Ondertussen zag ik Musk een nieuwe cryptische tweet sturen en voelde ik me gerustgesteld dat de weggeefactie echt was. Tot de timer op de website naar nul was herleid. Toen realiseerde ik me dat het allemaal een groot fake verhaal was. Mijn hart klopte zo hard. Ik ging naar boven en ging op de rand van het bed zitten om het mijn vrouw te vertellen. Ik maakte haar wakker en vertelde dat ik een grote fout had gemaakt, een hele grote fout.” Sebastian spendeerde uren aan e-mails naar de oprichterswebsite en het tweeten van het valse Twitter-account van Musk, maar tevergeefs.

“Uiteindelijk begon ik te accepteren dat het geld voorgoed verdwenen was”, zucht Sebastian.

### **Wat zegt Gwen?**

“Giveaway-scams zijn de meest voorkomende vorm van crypto-scam. Ze worden meestal gepost op Facebook, Twitter, Medium en YouTube”, weet cryptokenner Gwen Busseniers. “Door de virale aard waarmee informatie zich op het internet verspreidt, proberen oplichters mensen te misbruiken door gratis bitcoins of andere digitale valuta’s aan te bieden. De meeste van die oplichtingen hebben vergelijkbare onderdelen. Een hacker compromitteert of bootst een socialemedia-account van een prominente publieke figuur of crypto-exchange na. De account van de oplichter begint om verschillende redenen bitcoin of ethereum te vragen, of vraagt dat jij een account aanmaakt om er iets voor terug te krijgen. Of de oplichter vraagt om een account aan te maken met de belofte: stuur één, krijg twee terug”, omschrijft Gwen de werkwijze.

## Gemini 5,000 BTC Airdrop!



Tyler Winklevoss [Follow](#)



Gemini has come along way in the past year and we couldn't do it without you.

Een voorbeeld waarbij oplichters de (legitieme) exchange Gemini gebruiken om je te misleiden. © rv

Voor nietsvermoedende slachtoffers die crypto sturen naar wallets van de nepaccounts, is het geld voor altijd verloren, legt Gwen uit. “Van zodra een slachtoffer geld naar een ‘weggeefadres’ stuurt, is het voor altijd verdwenen. Vanwege de finaliteit van cryptocurrency-transacties is er geen manier om ze ongedaan te maken. Dat maakt dit soort ‘weggeefacties’ zeer effectief voor kwaadwillende actoren.”

### Urgentie

Oplichters gaan bovendien vaak een stap verder door een gevoel van urgentie in te bouwen. “Door middel van bijvoorbeeld een ‘live video’ op YouTube of een verklaring dat ze maar een beperkt aantal munten ‘weggegeven’. Het doel daarvan is om slachtoffers aan te moedigen snel en

zonder onderzoek te handelen”, zegt Gwen. “Voor alle duidelijkheid: noch Gemini, noch enige andere gerenommeerde cryptocurrency-exchange zal je vragen om betalingen over te maken via sociale media-accounts. Om cryptocurrency te storten naar Gemini moet je er altijd voor zorgen dat je het walletadres rechtstreeks van Gemini.com ontvangt.”

Net als weggevertjes zijn ‘weggeefprijzen’ oplichtingspraktijken waarbij men probeert om mensen een actie te laten ondernemen, of informatie prijs te geven. “Een voorbeeld is het opgeven van je naam, adres, e-mail en telefoonnummer om een prijs te ontvangen. Met die informatie kan een hacker zich als jou voordoen en toegang krijgen tot jouw accounts”, zegt Gwen.

### **Piramide en ponzi**

Onze expert geeft ook wat meer duiding bij de zogenaamde piramide-oplichting. “Een piramideconstructie belooft rendement aan deelnemers, op basis van het aantal mensen dat zij uitnodigen om mee te doen. Zo kan het stelsel viraal en snel groeien, maar meestal leidt het niet tot enige vorm van zinvol rendement voor de leden of genodigden. Nodig dus nooit je persoonlijke netwerk uit met als enige doel beloningen of rendementen van een product of dienst te verzamelen, en investeer niet met je eigen kapitaal op aandringen van anderen om het proces te versnellen”, tipt Gwen.

Een mooi voorbeeld is het nog steeds actieve piramidespel Bank of Tron. Dat beweert een platform te zijn om te investeren in de cryptocurrency TRON of TRX. Bank of Tron heeft investeringsplannen waarvan wordt gezegd dat ze een dagelijkse winst tussen 3,7 en 6,7 procent genereren. “Die cijfers zijn belachelijk voor iedereen met kennis van investeringen, aangezien ze gelijk staan aan jaarlijkse winsten van 1.350 tot 2.445 procent, wat absurde cijfers zijn. Er is geen melding gemaakt van een product of dienst die het bedrijf levert”, zegt Gwen.



mohammad karamad

1 review GB



Jun 25, 2020

### **I will be rich sooon**

Right know i received my capital and benefit after 25 days this is amazing, i am going to continue investing in bank of tron , specially on 1st plan because it will gives benefit forever, if someone wants to use this great opportunity it is free for test

Laat je niet vangen aan de positieve recensies over Bank of Tron. Die zijn ook fake. © rv

Tot slot nog een woordje over de ponzifraude, waarbij er enkele kleine verschillen zijn met de piramidespelen. “Het grootste verschil is dat het bij ponzifraude de organisatoren zijn die voor nieuwe deelnemers zorgen. Bij piramidespelen zorgen de deelnemers voor nieuwe deelnemers”, zegt Gwen. “Trap dus niet in aanbiedingen waar een of meerdere personen je, in ruil voor een storting, een gegarandeerd rendement bieden. De nieuwe betalingen worden gebruikt om huidige investeerders te betalen. Het eindresultaat is doorgaans dat veel mensen veel geld verliezen”, besluit ze.