Oplichters aarzelen niet om munt te slaan uit de actualiteit rond COVID-19. Wees dus voorzichtig, want deze toestand biedt oplichters de ideale gelegenheid om nieuwe slachtoffers te maken. Doorgaans contacteren zij hun slachtoffers via allerlei kanalen, zoals e-mails, sociale netwerken en ongevraagde telefoontjes, en gebruiken zij dus technieken die sterk op phishingtechnieken lijken.

De FSMA heeft vernomen dat malafide personen die phishingtechnieken nu ook gebruiken om misbruik maken van de actualiteit rond COVID-19. Zo circuleren er valse berichten op het internet en worden sms'en verstuurd met onder meer:

- valse aanbiedingen om beschermingsmaskers te kopen;
- valse geldinzamelingen voor slachtoffers van het virus;
- links naar valse informatiesites;
- valse aanbiedingen van vaccins.

Meer dan ooit is voorzichtigheid geboden. Denk twee keer na voor u op een link klikt, wees voorzichtig met ongevraagde berichten die u ontvangt, en hou rekening met de aanbevelingen van het Centrum voor Cybersecurity .

De nieuwe communicatiekanalen bieden 'oplichters 2.0' de mogelijkheid om nog meer slachtoffers te maken. Sociale netwerken zoals Twitter, Facebook, Instagram of LinkedIn blijken dé kanalen bij uitstek om valse beleggingsaanbiedingen te verspreiden, zoals aanbiedingen in cryptomunten, in binaire opties en forex-producten/CFD's of in 'beleggingswijnen', aanbiedingen van vermogensbeheerovereenkomsten of kredietaanbiedingen.

In dit verband heeft de FSMA de afgelopen weken vooral veel meldingen ontvangen over:

- **Bitcoin Evolution / Bitcoin Revolution**: Deze entiteiten hebben niet de vereiste vergunning om beleggingsproducten of –diensten aan te bieden in of vanuit België. Om slachtoffers te benaderen, maken ze voornamelijk gebruik van de techniek van valse persartikels die verwijzen naar bekende personen, zonder dat die daar zelf van op de hoogte zijn (zie uitleg hieronder).

Hoe circuleren valse beleggings-/kredietaanbiedingen op sociale netwerken?

Volgende technieken blijken bij oplichters het populairst om frauduleuze aanbiedingen via sociale netwerken te verspreiden:

- **Gesponsorde links op Facebook en Instagram**

Slachtoffers van beleggingsfraude geven vaak aan telefonisch te zijn gecontacteerd nadat zij op een gesponsorde link of post op Facebook of Instagram hadden geklikt.

Via dergelijke links of posts lijken vooral frauduleuze beleggingsaanbiedingen in cryptomunten, in binaire opties en forex-producten/CFD's en in 'beleggingswijnen', alsook frauduleuze aanbiedingen van vermogensbeheerovereenkomsten te worden gepromoot (zie de waarschuwingen daarvoor op de FSMA-website).

In tegenstelling tot gewone posts, die niet noodzakelijk in het oog springen in de *newsfeed*, verschijnen gesponsorde posts in functie van leeftijd, geslacht of interessesfeer, en in functie van de pagina's die door de betrokkene of het doelpubliek worden geconsulteerd.

Reclameberichten die 'erg rendabele' beleggingen promoten, verschijnen in de betrokken advertentieruimten of in de *newsfeed* van de gebruiker. Vaak wordt de gebruiker gevraagd zijn contactgegevens te vermelden, zodat hij later opnieuw kan worden gecontacteerd.

Doorgaans worden die reclameberichten geïllustreerd met een afbeelding of een video en gaan ze vergezeld van valse commentaren en automatisch gegenereerde *likes*. De kernboodschap is intrigerend maar blijft steeds uiterst vaag.

De pagina's met die gesponsorde reclameberichten lijken speciaal voor dergelijke reclamecampagnes te zijn aangemaakt. Ze hebben uiteenlopende namen, die in meer of mindere mate refereren aan de financiële wereld, maar vermelden doorgaans geen telefoonnummer, website, adres of naam van een vennootschap.

- **Eenvoudigweg via advertenties op Facebook**

Frauduleuze aanbiedingen, meestal van kredieten, worden door oplichters soms eenvoudigweg verspreid via advertenties op Facebookgroepen die bijvoorbeeld gespecialiseerd zijn in aan- of verkoop van vastgoed of tweedehandsartikelen. De oplichters kiezen er groepen uit met vooral Belgische consumenten.

- **Valse persartikels waarin bekende personen aan het woord zijn**

Op het internet doen ook valse persartikels de ronde met zogezegde 'verklaringen' of 'interviews' waarin bekende personen financiële beleggingen, vooral in cryptomunten, aanprijzen. Die artikels circuleren op websites met *fake news* en op Facebook waar ze via gesponsorde reclame opduiken.

De bedoeling van die praktijk is uw vertrouwen te winnen met foto's van bekende mensen uit de sport-, zaken- of mediawereld. Op die manier trachten zij u te overhalen om in te gaan op hun aanbiedingen die helaas te mooi zijn om waar te zijn.

- **Oplichters chatten met hun slachtoffers op sociale media**

Oplichters 2.0 gebruiken de sociale media ook om hun slachtoffers persoonlijk te contacteren, hetzij door hun een 'vriendschapsverzoek' te sturen, hetzij door hun rechtstreeks een bericht te sturen via de chatboxen van Facebook, Instagram en zelfs LinkedIn.

Als een oplichter met een nieuw slachtoffer begint te chatten, spreekt hij niet onmiddellijk van een belegging. Wel integendeel. Hij probeert eerst een vertrouwensrelatie op te bouwen, zoals bij vriendschapsfraude. Vaak zal de oplichter pas na een paar uur, enkele weken of zelfs maanden gechat te hebben terloops laten vallen dat hij een 'gouden beleggingstip' heeft.

Sommige oplichters openen ook valse rekeningen door misbruik te maken van de identiteit en de foto van personen die zeer actief zijn op sociale media. Voor zover ons bekend, komt dit vooral voor bij Instagram-accounts.

Word geen slachtoffer van beleggingsfraude op sociale netwerken

- **Wees op uw hoede voor (beloftes van) buitensporige winst.** Als een rendement u te mooi lijkt om waar te zijn, is dat meestal ook werkelijk zo!
- **Neem de door de vennootschappen verstrekte informatie niet voor zoete koek aan.** Vaak beweert een vennootschap over een vergunning te beschikken om financiële diensten aan te bieden, terwijl dat niet het geval is. Controleer steeds de informatie die u wordt verstrekt (handelsnaam, maatschappelijke zetel, …). Is de vennootschap buiten de Europese Unie gevestigd, wees er dan bewust van dat er moeilijkheden kunnen optreden mocht u in een conflictsituatie terechtkomen.
- **Ga na of de vennootschap een vergunning heeft**. Raadpleeg daartoe de lijsten op de website van de FSMA – Check je aanbieder. **Wees ook beducht voor 'cloned firms'.** Dat zijn vennootschappen die zich laten doorgaan voor andere, legitieme vennootschappen zonder dat ze een band hebben met elkaar. U kan deze fraude op het spoor komen door de e-mailadressen of de contactgegevens van de betrokken vennootschappen te vergelijken.
- **Raadpleeg de waarschuwingen** die op de websites van de FSMA, andere buitenlandse toezichthouders en IOSCO worden gepubliceerd. Ga na of de vennootschap die u financiële diensten aanbiedt, in een waarschuwing wordt genoemd. Zoek niet alleen op naam van de vennootschap(pen) die u financiële diensten aanbied(t)(en), maar ook op naam van de vennootschap(pen) waaraan u eventueel geld moet storten.
- Op de website van de FSMA kan u voor die opzoeking gebruik maken van de zoekfunctie. Bovendien zijn alle 'vennootschappen' waarover de FSMA een waarschuwing heeft gepubliceerd, vermeld op de lijst van ondernemingen die op onregelmatige wijze actief zijn op het Belgisch grondgebied. Ook die lijst is op de website van de FSMA te vinden.
- **Opgelet**: staat de vennootschap die u zoekt, niet op de lijst met waarschuwingen, dan nog mag u er niet van uitgaan dat ze een geldige vergunning heeft om financiële diensten aan te bieden. De FSMA stelt alles in het werk om waarschuwingen zo snel mogelijk te publiceren, maar de kans bestaat dat zij niet weet dat een vennootschap illegale activiteiten ontplooit op Belgisch grondgebied. Dat komt onder meer omdat malafide vennootschappen geregeld van naam veranderen.
- **Wees op uw hoede voor '*cold calling*'**: u wordt ongevraagd via telefoon of e-mail gecontacteerd met een financieel aanbod, dus zonder dat u daar als belegger vooraf om hebt verzocht. Dit is vaak de eerste stap van een frauduleuze praktijk.
- **Kijk uit als u wordt gevraagd om geld over te maken naar een land dat geen enkele band heeft** met de vennootschap, noch met uw thuisland als belegger.
- **Beleg nooit in een product als u niet perfect begrijpt wat het precies inhoudt.**
- **Wees achterdochtig** als u wordt gevraagd een **bijkomende som** te storten of een belasting te betalen als voorwaarde voor de uitbetaling van winst. Deze opvragingen zijn vaak een teken van fraude.

Aarzel niet om, bij de minste twijfel over het regelmatige karakter van een aanbod van financiële diensten, de FSMA te contacteren via het **contactformulier voor consumenten** op haar website. Aarzel ook niet om de FSMA te verwittigen als u in aanraking komt met een verdachte vennootschap waarover de FSMA nog geen waarschuwing heeft gepubliceerd.

Wat moet u doen als u toch blijkt te zijn opgelicht?

Als u het slachtoffer denkt te zijn van oplichtingspraktijken, **stort dan in geen geval nog bijkomende sommen** aan uw contactpersoon. **Opgelet:** dit geldt ook en vooral als u de terugbetaling van uw geld wordt beloofd in ruil voor een laatste storting. Oplichters gebruiken die techniek vaak om hun slachtoffers te overhalen nog een laatste keer geld te storten.

Contacteer ook onmiddellijk **uw lokale politiediensten** om een klacht in te dienen, en **meld de oplichting aan de FSMA via het contactformulier voor consumenten**.

De FSMA onderstreept hoe belangrijk het is om **zo snel mogelijk een klacht in te dienen en die klacht grondig te documenteren** (betrokken vennootschap, bankrekeningen waarop u geld heeft gestort, …).

Aarzel ook niet om de FSMA te verwittigen mocht u in aanraking komen met een verdachte vennootschap waarover de FSMA nog geen waarschuwing zou hebben gepubliceerd.