**Identiteitsdiefstal bij Belgische banken in het kader van een frauduleuze aanbieding van termijnrekeningen: opgelet voor oplichters!**

**De FSMA heeft de voorbije maanden verschillende gevallen opgemerkt van identiteitsdiefstal bij Belgische banken door Duitstalige oplichters. Deze willen je laten geloven dat ze een vergunning hebben om producten aan te bieden.**

**Duitstalige oplichters misbruiken de naam van Belgische banken om je te laten geloven dat ze op volledig legitieme wijze termijnrekeningen mogen aanbieden aan consumenten.**

**Daarbij misbruiken ze de naam en andere wettelijke gegevens van tussenpersonen die doorgaans vergund zijn in Duitsland of Zwitserland, om je ervan te overtuigen dat ze wel degelijk vergund zijn. Verder willen ze je laten geloven dat je een termijnrekening opent bij een Belgische bank. De oplichters gebruiken zeer gedetailleerde documentatie om de indruk te wekken dat ze in naam en voor rekening van die bank handelen. Vaak bieden ze je kortingen of bonussen aan. Zo lichten ze je op: je denkt te maken te hebben met vergunde actoren, terwijl de oplichters de identiteit van die actoren gewoon misbruiken.**

**In sommige gevallen maken de oplichters een website aan met een webadres dat overeenstemt met de naam van de tussenpersoon van wie ze de identiteit misbruiken.**

**Wat kan je doen om niet in de val te trappen?**

**Deze frauduleuze praktijk valt moeilijk te herkennen en te voorkomen. Daarom raden we je aan om de volgende stappen te ondernemen, zodat je er zeker van bent dat je contactpersoon wel degelijk is wie hij beweert te zijn:**

* Ga na of de **contactgegevens** op de websites van verschillende regelgevers over die ondernemingen dezelfde zijn als de contactgegevens op de websites van die ondernemingen zelf.

**Opgelet:** oplichters gebruiken vaak ook het postadres van de vergunde onderneming. Een juist postadres volstaat dus niet om ervan uit te gaan dat de identiteit van je contactpersoon correct is!

* Gebruik onlinezoekmachines om er zeker van te zijn dat de vergunde onderneming geen andere website heeft.

**Opgelet!** Oplichters gebruiken vaak een internetadres dat sterkt lijkt op dat van de officiële website van de onderneming waarvan ze de identiteit stelen. Er is bv. een streepje toegevoegd in het adres, er wordt een andere extensie gebruikt (bijvoorbeeld .com in plaats van .be), of **de identiteit wordt misbruikt van een tussenpersoon die geen website gebruikt**.

* **Toets de officiële informatie aan de feiten.** Als je contactpersoon bijvoorbeeld beweert voor een buitenlands tussenpersoon te werken, maar je producten van een instelling naar Belgisch recht aanbiedt, kan je het best de coherentie van de verstrekte informatie controleren (Zijn de voorgestelde rentevoeten realistisch? Zijn de contractgegevens up-to-date?). Ook als je contactpersoon voor een in België gevestigde bank beweert te werken, maar je met een buitenlands telefoonnummer opbelt, moet er een alarmbelletje gaan rinkelen.
* Ga met onlinetools na **wanneer de website die je contactpersoon gebruikt, werd gecreëerd**. Als dat heel recent blijkt te zijn, heb je een gegronde reden om aan zijn geloofwaardigheid te twijfelen.
* Als je contactpersoon je vraagt geld te storten op een rekening die is geopend op naam van een andere persoon of onderneming, is dat een duidelijke aanwijzing van fraude.
* Als je de minste twijfel hebt over de identiteit van je contactpersoon, aarzel dan niet om contact op te nemen met de FSMA. Dat kan via het contactformulier voor consumenten.

Brussel, 4 november 2024

|  |  |
| --- | --- |
| Perscontact | Jim LannooWoordvoerder/Adjunct-directeurCommunicatie en Financiële Educatie |
| T direct | + 32 2 220 57 06 |
| E-mail | Press@fsma.be |