Fraude voorkomen, zó herken je een echte bankmedewerker

Oplichters gebruiken diverse methoden om geld te stelen. Ze proberen vaak je vertrouwen te winnen door je te verleiden om persoonlijke informatie te delen. Steeds meer mensen worden helaas telefonisch opgelicht door neppe bankmedewerkers. Lees hier hoe je een oplichter herkent, hoe je veilig bankiert en wat voor manieren van oplichting er zijn.

Hoe herken je een oplichter?

Er zijn een aantal algemene tekenen die kunnen wijzen op oplichting:

1. Haastig gedrag: Oplichters proberen je te dwingen snel beslissingen te nemen, let op of de persoon haastig of opdringerig is.
2. Verzoek om geld of bankgegevens: Oplichters vragen vaak om geld of persoonlijke informatie, zoals creditcardgegevens of bankinformatie. Geef dit nooit zomaar weg.
3. Te mooi om waar te zijn: Oplichters bieden vaak belachelijk hoge prijzen of prijzen die te mooi lijken om waar te zijn.
4. Dreigementen: Sommige oplichters dreigen met gevolgen als je niet meteen actie onderneemt, zoals arrestatie of het afsluiten van je energie.
5. Onvoldoende bewijs: Als iemand beweringen doet zonder concrete bewijzen of referenties, kan dit een teken zijn van misleiding.
6. Onbekende nummers: Oplichters bellen vaak van onbekende nummers of met een nummer dat lijkt op een bekend nummer.
7. Verzoek om persoonlijke informatie: Oplichters vragen vaak om persoonlijke informatie, zoals je social securitynummer of wachtwoorden. Geef dit nooit zomaar weg.

Als je twijfelt of je met een oplichter te maken hebt, hang op of verlaat de situatie en zoek hulp bij een vertrouwde bron, zoals de politie of je bank. Het is beter om veilig te spelen dan spijt te hebben.

Bankmedewerkers vragen je nooit om:

- Beveiligingscodes door te geven
- Een pas per post te sturen

- Geld over te schrijven via een link of via Internet Bankieren
- Direct geld over te boeken via een link in een e-mail of sms
- Software te downloaden waarmee wij iemand jouw bankomgeving kan bekijken
- Jouw pas af te geven als een medewerker bij je langskomt

Verschillende soorten oplichting

1. Phishing (vervalsing via e-mail)

Bij phishing ontvang je van oplichters een e-mail of sms (smishing) die sterk lijkt op een bericht van de bank of een bedrijf. Hierin word je gevraagd op een link of bijlage te klikken, waarmee je terechtkomt op een valse website.

2. Betaalpasfraude

Bij betaalpasfraude word je verzocht jouw betaalpas per post te sturen. Dit moet je nooit doen. Wees ook altijd alert tijdens het pinnen van geld. Oplichters kunnen je soms afleiden en snel je pas verwisselen.

3. Nep-betalingsverzoeken

Verkoop of koop je soms producten online, bijvoorbeeld via Marktplaats? Oplichters kunnen zich voordoen als kopers en je vragen zich te identificeren. Zij sturen vervolgens een vals betalingsverzoek via WhatsApp of een andere chat-app. Oplichting via Marktplaats is de laatste tijd sterk afgenomen door maatregelen van Markplaats zelf.

Tips om veilig gebruik te maken van veilingsites

4. Links of bijlagen met malware

Door op een link of bijlage in een email van een oplichter te klikken, kan je jouw computer besmetten met een virus, ook wel malware genoemd. Hierdoor krijgen oplichters toegang tot je bankzaken en kunnen ze jouw geld stelen.

5. Boilerroom fraude

Bij boilerroom fraude word je telefonisch of via e-mail benaderd met een beleggingsvoorstel. De contactpersoon belooft snel rendement en wellicht levert de eerste investering winst op. Maar je wordt snel verleid om hoge bedragen te beleggen.

6. Fraude met facturen

Oplichters willen dat je geld overmaakt naar hun eigen bankrekeningen en proberen dit op verschillende manieren te bereiken, zoals door een vals factuur te sturen, namens een bekend bedrijf.

7. Telefoonfraude

Oplichters kunnen je benaderen door te telefoneren en zich voor te doen als medewerker van de bank of van een bekend bedrijf. Dit gebeurt vaak na het invullen van jouw gegevens via een vervalste e-mail.

Wat te doen als je bent opgelicht?

Heb je zelf geld overgeboekt, maar blijkt later dat u bent opgelicht? Omdat u zelf de betaalopdracht heeft gedaan, zijn banken niet verplicht de financiële schade te vergoeden. Toch hebben de banken besloten dat zij klanten die in het verleden slachtoffer zijn geworden van bankhelpdeskfraude, onder bepaalde voorwaarden, een schadevergoeding aan te bieden. Een van die voorwaarden is, dat het slachtoffer aangifte heeft gedaan bij de politie. Wil je weten of je hiervoor in aanmerking komt, neem dan contact op met je eigen bank.

De 5 stappen voor veilig bankieren

1. Bewaar je beveiligingscodes vertrouwelijk (geef nooit je pincode weg!)
2. Zorg dat jouw (digitale) betaalpas niet in verkeerde handen valt
3. Bescherm de apparaten die je voor jouw bankzaken gebruikt
4. Controleer je betaalrekening regelmatig
5. Meld incidenten direct aan de bank en volg hun instructies op

Lees ook

- Dit kun je het beste doen om ticketfraude te voorkomen
- Tips om Social Media veilig te gebruiken
- Internetoplichting en fraude herkennen doe je óók met deze tips

Auteur: *Ilse Bloemendal*

Bron: Oplichting: echte bankmedewerkers herkennen – Startpagina Blog