Weet u hoe u internetcriminelen te slim af bent?

Wegwijzer Workshop Veilig Online Bankieren

Habithuis
Huis van Makelaars,
Verzekering & Financiering

Habithuis
Anjelierenstraat 7
2231 GT Rijnsburg
T (071) 402 41 41
E info@habithuis.nl
I www.habithuis.nl

RegioBank De buurtzame bank

Internetcriminelen kunnen uw codes op allerlei manieren ontfutselen

Via social media of WhatsApp
Vraagt iemand die bekend lijkt om geld of uw code? Bel die persoon dan op. Vraag of het daadwerkelijk klopt dat hij of zij dat is en deze vraag stelt. Dit gaat vaak via WhatsApp of Facebook.

Via phisingmails en manipulatie
Phisingmails zijn nepmails om u naar valse websites te lokken in de hoop dat u uw persoonlijke gegevens invult. Phishing is een vorm van manipuleren. In deze samenvatting staat veel informatie over alle vormen van manipulatie. Neem deze punten goed door. Vergeet niet: voor wat, hoort wat!

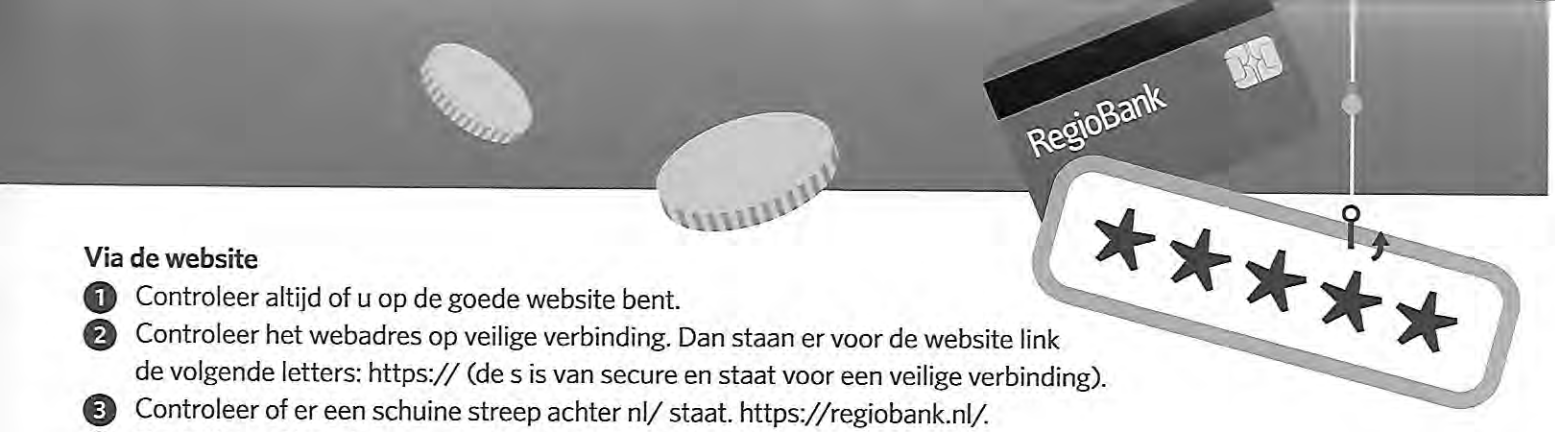
Er zijn verschillende manieren om te zien of een mail vals is.
1. Het e-mailadres van de afzender ziet er gek uit. Bijvoorbeeld @345xjyz.nl.
2. U krijgt een e-mail op een e-mailadres dat u niet aan ons heeft gegeven.
3. Aanhef van de e-mail. Vaak is deze niet persoonlijk. Geachte relatie, klant of meneer/mevrouw kunnen signalen zijn van phising.
4. Uw e-mailprovider of spamfilter geeft aan dat de e-mail 'spam' is.
5. Staat er een link in het e-mailbericht? **Zweef** met uw muis over de link. **Niet klikken!** U ziet dan vaak een adres dat niet klopt. Of niet op de website van de afzender komt.
6. Veel taalfouten.
7. De e-mail is in een andere taal, zoals in het Engels.
8. Lokken met gratis producten. Vergeet niet, voor niets gaat de zon op!
9. Als ze u onder druk zetten. Bijvoorbeeld: vervang nu uw bankpas voor 1 juli!
10. Persoonlijke e-mails van RegioBank kunt u terug zien in Mijn berichten als u inlogt op Internet Bankieren.
11. Klik nooit op een link en deel nooit uw persoonlijke gegevens.

Als u wordt gevraagd om meteen iets te doen dan klopt dit vaak niet. Wij zullen nooit via de e-mail vragen om iets direct te doen. Wij vragen nooit om pincodes, inlogcodes of gebruikersnaam. Ook vragen wij nooit via de e-mail in te loggen.

Valse e-mail gehad?
Meld altijd dat u een valse e-mail hebt gehad. Als het om een valse RegioBank e-mail gaat, kan u dit aan ons laten weten. Maar u mag het ook doorsturen naar **valse-email@regiobank.nl**.

Via Telefoon
Criminelen proberen uit naam van RegioBank telefonisch persoonlijke gegevens van u te krijgen door zogenaamde phishingtelefoontjes. Deze telefoontjes worden gepleegd door iemand die zich voordoet als een medewerker van RegioBank. Ze vragen de responscodes van uw digipas. Trap hier niet in. Responscodes voert u alleen in wanneer u internetbankiert en deelt u nooit met anderen, dus ook niet aan de telefoon.

Via Marktplaats
Ook op Marktplaats kunnen criminelen toeslaan.
1. Maak nooit geld over om geld te krijgen.
2. Deel nooit codes of gebruikersnamen.
3. Geef nooit gegevens van uw identiteitsbewijs.
4. Bedragen voor bepaalde producten zijn te mooi om waar te zijn.
   Bijvoorbeeld een nieuwe accuboor t.w.v. € 500 aangeboden voor slechts € 160.
5. Vergeet niet: producten kopen via marktplaats brengt altijd risico's met zich mee.
   Als u vooraf betaalt gokt u erop dat het product wordt geleverd. U weet namelijk niet wie de verkoper is.



Via de website

1. Controleer altijd of u op de goede website bent.
2. Controleer het webadres op veilige verbinding. Dan staan er voor de website link de volgende letters: https:// (de s is van secure en staat voor een veilige verbinding).
3. Controleer of er een schuine streep achter nl/ staat. https://regiobank.nl/.
4. Controleer of het slotje op de adresbalk of onderin het scherm staat.
5. Bij het inloggen: de responscode die u ziet op uw digipas en die u moet invoerenbegint altijd met een 0 (nul). Is dit niet het geval? Sluit de pagina dan zo snel mogelijk af!
6. Bij het betalen: de beveligingscode bij het bevestigen van de betaalopdracht mag nooit met een 0 (nul) beginnen. Is dit niet het geval? Sluit de pagina dan zo snel mogelijk af!

Klopt het niet? Stop direct met Internet Bankieren en installeer de nieuwste versie van uw browser en de laatste updates voor uw besturingssysteem. Blijft u problemen hebben? Neem dan contact met ons op: 030 - 291 42 90.

Veilig Pinnen

1. Houd bij het pinnen in winkels altijd uw hand om het scherm. Zo voorkomt u dat mensen achter u mee kunnen kijken.
2. Bewaar uw pinpas op een veilige plek.
3. Schrijf nooit uw pincode achter op uw pinpas of achter op uw digipas.
4. Bewaar de pincodes en pasjes nooit op dezelfde plek.

Identiteitsbewijs

Stuur nooit zomaar een foto of kopie van uw identiteitsbewijs op. Soms is het nodig voor een organisatie om iemands identiteit vast te stellen, zoals van een klant. Bijvoorbeeld om fraude te voorkomen. Een organisatie kan dit op verschillende manieren doen. Welke manier is toegestaan, hangt af van de toepasselijke wet en van de noodzaak.

Identiteitsbewijs niet altijd nodig

Een organisatie mag niet zomaar aan iemand vragen om zijn identiteitsbewijs te laten zien. Of een kopie maken van het identiteitsbewijs. Kan de organisatie de identiteit van deze persoon ook op een andere, minder vergaande manier vaststellen? Dan moet de organisatie voor die manier kiezen. Bijvoorbeeld als een klant zijn gegevens wil inzien bij een webshop. Dan heeft de webshop meestal genoeg aan het klantnummer in combinatie met naam en adres om de identiteit van de klant te controleren. Of als de klant zijn account wil verwijderen bij de webshop. De klant kan dan inloggen en aangeven dat hij zijn gegevens wil verwijderen.

Identiteitsbewijs tonen

Heeft een organisatie echt het identiteitsbewijs van iemand nodig om zijn identiteit te controleren? Dan is het vaak genoeg als diegene zijn identiteitsbewijs, zoals zijn paspoort of identiteitskaart, laat zien. Dit wordt ook wel 'legitimeren' of 'identificeren' genoemd. De organisatie mag dan géén kopie maken van het identiteitsbewijs. We hebben u laten zien dat er een **ID app** bestaat. Deze kunt u gebruiken voor de identificatie bijvoorbeeld in hotels, campings of waar u ook moet identificeren. Mocht u een kopie willen gebruiken, streep dan altijd uw BSN nummer door. De app is beschikbaar gesteld door de overheid en is goed beveiligd.

Verplichte kopie identiteitsbewijs

Slechts enkele organisaties zijn verplicht om een kopie van uw ID-kaart te vragen. Dit zijn bijvoorbeeld:

- Overheidsinstanties.
- Banken.
- Notarissen.
- Casino's.
- Levensverzekeraars.
- Uw werkgever moet in de loonadministratie een kopie van uw ID-bewijs bewaren.

Tips & Tricks

De gouden tip
Vraag uzelf af of u onder druk wordt gezet. Moet u snel reageren en wordt er gedreigd met negatieve gevolgen? Vertrouw het dan niet. U mag ervan uitgaan dat uw bank u nooit zo benadert en ook de meeste andere normale communicatie verloopt zonder dergelijke druk. Voelt iets verdacht? Bel of e-mail ons gerust.

Krijgt u een e-mail?
Controleer voor zover mogelijk de afzender en eventuele links die in de e-mail gebruikt worden. Bent u er niet zeker van of het klopt? Negeer de boodschap, klik niet op de links, stuur de e-mail dan door naar valse-email@regiobank.nl en gooi hem daarna weg. Als het phising is, kan de bank de criminele website uit de lucht halen en voorkomen dat er meer slachtoffers vallen.

Controleer altijd met wie u communiceert
Krijgt u een verdacht berichtje of telefoontje? Check dan het e-mailadres of het telefoonnummer.

Bel ons als u iets niet vertrouwt
Denkt u dat u slachtoffer bent van fraude of ziet u iets verdachts? Meld fraude en incidenten zo snel mogelijk: 030 - 291 42 90.

Meer informatie?
Bekijk ook de RegioBank website over veilig bankieren: regiobank.nl/veiligbankieren

RegioBank De buurtzame bank.
Zelfstandig Adviseur