



Hoe bescherm je online jouw geld en jezelf?

Tips voor veilig online bankieren

Bescherm jezelf en je geld: zo bankier je veilig

Social media

Vraagt een bekende je in een berichtje om met spoed geld over te maken? Laat je niet misleiden. Bel diegene op het nummer dat je altijd gebruikt en controleer het verhaal. Niet gesproken? Niet betalen!

Phishing en valse website

Je krijgt een e-mail of sms die van ons lijkt te komen. Daarin staat dat je direct actie moet ondernemen. Bijvoorbeeld klikken op een link of je betaalpas opsturen. Doe dat niet. Wij vragen nooit om via een link in te loggen, een overboeking te doen of te annuleren.

Marktplaats

Een (ver)koper vraagt je om alvast een klein bedrag over te maken om zeker te weten dat je betrouwbaar bent. Trap er niet in. Stuur ook geen kopie van jouw identiteitsbewijs op, deel geen codes en maak geen verzendlabels aan via een link. Grote kans dat het foute boel is.

Telefoon (helpdeskoplichting)

Iemand belt je op en doet zich voor als bankmedewerker. Ook het nummer lijkt te kloppen. Vraagt de medewerker je geld over te boeken naar een veilige 'kluisrekening', codes te delen of even met je mee te kijken? Verbreek de verbinding en bel ons om het verhaal te checken. **Bel ons, ook buiten kantooruren: 030 291 42 90.**



- ✓ Controleer altijd met wie je communiceert. Het webadres is: <https://www.regiobank.nl/>. Controleer de spelling en kijk of er een schuine streep achter staat: .nl/ Controleer of de browserbalk (gedeeltelijk) groen is.
- ✓ Verdacht bericht gekregen? Stuur het door naar valse-email@regiobank.nl en verwijder het bericht daarna.
- ✓ Verdacht telefoontje? Verbreek de verbinding en bel ons direct, ook 's avonds en in het weekend.