

Uniforme veiligheidsregels

Particulieren



VEILIG BANKIEREN 

Waarover gaan deze regels?

Elektronisch bankieren en elektronisch betalen moeten veilig zijn. Denk aan internet- en/of mobiel bankieren, betalen bij betaalautomaten in winkels en geld opnemen bij de geldautomaat. De bank heeft hierin een belangrijke taak, maar u ook. Wat u moet doen, vindt u in deze veiligheidsregels.

Waarom is het belangrijk dat u zich houdt aan deze regels?

U vermindert sterk de kans dat u het slachtoffer wordt van fraudeurs als u de regels opvolgt. Het is voor consumenten wettelijk geregeld dat een bedrag dat zonder uw toestemming van uw bankrekening is afgeschreven, door de bank wordt vergoed. Daarbij mag de bank u volgens de wet in bepaalde gevallen een eigen risico van maximaal € 150,- in rekening brengen. De bank is echter niet altijd verplicht het bedrag, eventueel verminderd met het eigen risico van maximaal € 150,- aan u te vergoeden. Wanneer u zich aan de onderstaande vijf veiligheidsregels houdt, loopt u niet het risico dat de gehele schade voor uw eigen rekening komt.

Wat moet u doen?

1. **Houd uw beveiligingscodes geheim.**
2. **Zorg ervoor dat uw bankpas nooit door een ander gebruikt wordt.**
3. **Zorg voor een goede beveiliging van de apparatuur die u gebruikt voor uw bankzaken.**
4. **Controleer uw bankrekening.**
5. **Meld incidenten direct aan de bank en volg aanwijzingen van de bank op.**

Elk van deze veiligheidsregels worden hieronder toegelicht.

Toelichting veiligheidsregels

1. Houd uw beveiligingscodes geheim.

Denk hierbij aan het volgende:

- Zorg ervoor dat beveiligingscodes nooit aan een ander bekend kunnen worden. Beveiligingscodes zijn niet alleen de pincode die u in combinatie met de bankpas gebruikt. Het zijn ook alle andere codes die u moet gebruiken om elektronische betalingen te doen en/of gebruik te maken van internet- en mobielbankieren. Dat kunnen bijvoorbeeld de codes zijn die een door de bank verstrekte codecalculator aangeeft.
- U mag deze beveiligingscodes alleen zelf gebruiken. U moet dat doen op de manier die de bank aangeeft.
- Schrijf of sla de codes niet op. Of, als het echt niet anders kan, alleen in een voor anderen onherkenbare vorm die alleen door uzelf is te ontcijferen. Bewaar in dit geval de versleutelde informatie niet bij uw bankpas of bij apparatuur waarmee u uw bankzaken regelt.
- Als u zelf een beveiligingscode kunt kiezen, zorg dan dat die niet gemakkelijk te raden is. Kies bijvoorbeeld geen geboortjaar, naam van een familielid of postcode.
- Zorg ervoor dat niemand kan meekijken al u uw beveiligingscodes intikt. Het gaat hier niet alleen om uw pincode, maar ook om alle andere codes die u moet gebruiken om elektronische betalingen te doen en/of gebruik te maken van internet- en mobiel bankieren.

- Geef nooit een beveiligingscode door per telefoon, e-mail of op een andere wijze dan de bank u heeft voorgeschreven. Dat geldt ook als u telefonisch, per e-mail of persoonlijk door iemand wordt benaderd die aangeeft medewerker van de bank te zijn.
De bank zal u op deze wijze **nooit** om beveiligingscodes vragen.

2. Zorg ervoor dat uw bankpas nooit door een ander gebruikt wordt.

Denk hierbij aan het volgende:

- Laat u niet afleiden als u de bankpas gebruikt en controleer of u uw eigen bankpas daarna terugkrijgt.
- Berg de bankpas altijd op een veilige plaats op en zorg ervoor dat u hem niet gemakkelijk kunt verliezen. Controleer regelmatig of u de bankpas nog in uw bezit heeft.

3. Zorg voor een goede beveiliging van de apparatuur die u gebruikt voor uw bankzaken.

Denk hierbij aan het volgende:

- Zorg dat de geïnstalleerde software op de apparatuur, zoals computer, tablet en/ of smartphone, die u voor het regelen van uw bankzaken gebruikt, is voorzien van actuele (beveiligings)updates. Geïnstalleerde software is bijvoorbeeld het besturingssysteem en beveiligingsprogramma's, zoals virusscanner en firewall.
- Installeer geen illegale software.
- Beveilig de toegang tot de apparatuur die u gebruikt voor het regelen van uw bankzaken met een toegangscode.
- Zorg er daarnaast voor dat door de bank verstrekte toepassingen op de apparatuur die u gebruikt voor het regelen van uw bankzaken niet door onbevoegden kunnen worden gebruikt.
- Log altijd uit als u klaar bent met het regelen van uw bankzaken.

4. Controleer uw bankrekening.

Controleer altijd zo spoedig mogelijk uw elektronische of papieren rekeninginformatie of u transacties ziet waarvoor u geen toestemming heeft gegeven. Doe dit in ieder geval elke twee weken als de bank voor u elektronische rekeninginformatie ter beschikking stelt. Als u alleen rekeninginformatie op papier ontvangt, controleer deze dan in ieder geval binnen twee weken na ontvangst. Als er schade voor de bank ontstaat doordat het voor u enige tijd onmogelijk is geweest uw rekeninginformatie te controleren, dan kan de bank u vragen aan te tonen dat dit in alle redelijkheid niet mogelijk was.

5. Meld incidenten direct aan de bank en volg aanwijzingen van de bank op.

Denk hierbij aan het volgende:

- Neem in de volgende gevallen in elk geval direct met de bank contact op:
 - u heeft uw bankpas niet meer in uw bezit of weet niet waar deze is;
 - u weet of vermoedt dat iemand anders uw beveiligingscode kent of heeft gebruikt;
 - u ziet dat er transacties op uw bankrekening hebben plaatsgevonden, waarvoor u geen toestemming heeft gegeven;

Uniforme veiligheidsregels

Particulieren



VEILIG BANKIEREN 

- u heeft uw mobiele apparaat met betaaltoepassing van de bank niet meer, tenzij u dit apparaat aan een ander heeft overgedragen en eerst de betaaltoepassing heeft verwijderd;
- Neem ook direct contact op met de bank bij iets dat u als vreemd of ongebruikelijk ervaart, zoals een andere manier van inloggen.

De bank kan zorgen voor een blokkade om (verdere) schade te voorkomen. Als de bank u aanwijzingen geeft, bijvoorbeeld om nieuwe incidenten te voorkomen, dan moet u deze aanwijzingen opvolgen. Ook hierbij zal de bank u nooit om beveiligingscodes vragen.