Banken stellen nieuwe regels voor internetbankieren

Nederlandse banken hebben nieuwe regels voor internetbankieren opgesteld waar klanten aan moeten voldoen als ze in het geval van fraude hun geld terug willen krijgen.

> Zo mag er geen illegale software zijn geïnstalleerd, moet de computer up-to-date zijn en moet de rekening regelmatig worden gecontroleerd. Dat laat de Nederlandse Vereniging van Banken (NVB) weten.
>
> Voorheen hanteerde iedere bank zijn eigen veiligheidsvoorschriften. Nu zullen de Banken bij de behandeling van nieuwe claims van klanten (reeds vanaf 1 januari 2014) in de geest van deze nieuwe regels handelen.

Mocht een klant schade lijden en het blijkt dat hij zich niet heeft gehouden aan de veiligheidsregels, dan kan een bank op basis van haar coulancebeleid overigens alsnog besluiten om een deel van de schade voor haar rekening te nemen.

Veiligheidsregels De NVB heeft de nieuwe veiligheidsregels samen met de Consumentenbond opgesteld. Ze gaan voor particuliere klanten gelden. "Als consumenten zich aan de volgende veiligheidsregels voor elektronisch bankieren en -betalen houden, verminderen zij de kans sterk dat om slachtoffer te worden van fraude. Ook weten ze dan zeker dat de bank de schade vergoedt", stelt de NVB. Het gaat in totaal om vijf regels.

1. Houd beveiligingscodes geheim. Klanten mogen beveiligingscodes alleen zelf gebruiken. Daarnaast mogen ze niet worden opgeschreven. In het geval dit echt niet anders kan moet de code in een onherkenbare vorm voor anderen worden opgeschreven. Als klanten zelf hun beveiligingscode kiezen mag die niet eenvoudig te raden zijn. Bijvoorbeeld geen geboortejaar of naam van een familielid of een postcode. Klanten mogen de beveiligingscode ook nooit per telefoon of e-mail doorgeven.

2. Anderen mogen de bankpas niet gebruiken. Klanten moeten zich tijdens het gebruik van de bankpas niet laten afleiden en de bankpas altijd op een veilige plaats opbergen waar die niet eenvoudig verloren kan worden. Ook moet de klant regelmatig controleren of hij de bankpas nog in zijn bezit heeft.

3. Goede beveiliging van de apparatuur die wordt gebruikt voor bankzaken. Hierbij geldt dat de geïnstalleerde software op de apparatuur, zoals computer, tablet en/ of smartphone, die voor het regelen van de bankzaken wordt gebruikt, is voorzien van actuele (beveiligings)updates. Geïnstalleerde software is bijvoorbeeld het besturingssysteem en beveiligingsprogramma's, zoals virusscanner en firewall. Ook mag er geen illegale software zijn geïnstalleerd. Verder moet de apparatuur die wordt gebruikt voor het regelen van bankzaken met een toegangscode beveiligd zijn. Klanten moeten er daarnaast voor zorgen dat de toepassingen van de bank op hun apparatuur niet door onbevoegden zijn te gebruiken. Als laatste moeten klanten na hun bankzaken uitloggen.

4. Controleer de bankrekening. Klanten moeten in ieder geval elke twee weken hun rekeninginformatie controleren. Alleen als klanten rekeninginformatie op papier ontvangen moeten ze deze twee weken na ontvangst controleren. Als er schade voor de bank ontstaat doordat de klant enige tijd zijn rekeninginformatie niet heeft kunnen controleren, kan de bank de klant vragen aan te tonen waarom dit niet mogelijk was.

5. Meld incidenten direct aan de bank en volg aanwijzingen van de bank op. Het gaat dan om zaken als klanten weten of vermoeden dat iemand anders hun beveiligingscode kent of heeft gebruikt, of dat er transacties op de bankrekening hebben plaatsgevonden waarvoor geen toestemming is gegeven. Ook moet er direct contact met de bank worden opgenomen als de klant iets vreemds of ongebruikelijks ervaart, zoals een andere manier van inloggen. In het geval banken fraude vermoeden kunnen ze daarnaast de klant blokkeren om (verdere) schade te voorkomen. Als de bank in dit geval aanwijzingen geeft, bijvoorbeeld om nieuwe incidenten te voorkomen, dan moet de klant deze aanwijzingen opvolgen. "Ook hierbij zal de bank u nooit om beveiligingscodes vragen", aldus de NVB. Die laat verder weten dat de schade als gevolg van fraude met internetbankieren daalt.

Samenvatting:

1. **Houd beveiligingscodes geheim.**
2. **Anderen mogen de bankpas niet gebruiken.**
3. **Goede beveiliging van de apparatuur die wordt gebruikt voor bankzaken.**
4. **Controleer de bankrekening.**
5. **Meld incidenten direct aan de bank en volg aanwijzingen van de bank op.**