Veilig internetbankieren: richtlijnen van de banken

Beveiligingscodes beschermen, apparaten beveiligen en alleen zelf uw bankpas gebruiken. Welke veiligheidsregels verlangt de bank en wat doet u zelf om veilig te kunnen internetbankieren?

Vijf principes voor veilig internetbankieren

De Nederlandse banken houden zich aan vijf principes voor veilig internetbankieren. Deze principes zijn begin 2014 opgesteld door de Nederlandse Vereniging van Banken (NVB) in overleg met de Consumentenbond. In 2019 zijn ze aangepast in verband met de Europese betaalwet PSD2.
De vijf principes die de NVB heeft opgesteld luiden:

- **Houd uw beveiligingscodes geheim**
  - Gebruik beveiligingscodes alleen zelf en schrijf ze niet op.
  - Kies een beveiligingscode die niet eenvoudig te raden is.
  - Geef beveiligingscodes nooit per telefoon, e-mail of andere wijze door. Banken en andere dienstverleners vragen nooit om deze codes.

- **Zorg ervoor dat uw bankpas nooit door een ander wordt gebruikt**
  - Klanten moeten zich tijdens het gebruik van de bankpas niet laten afleiden.
  - Berg de bankpas altijd op een veilige plaats op. Controleer regelmatig of u de bankpas nog in uw bezit hebt.

- **Zorg voor een goede beveiliging van de apparatuur die u gebruikt voor bankzaken**
  - Voorzie de geïnstalleerde software en het besturingssysteem op de computer, tablet en/of smartphone van de laatst mogelijke (beveiligings-)updates.
  - Installeer geen illegale programma's.
  - Beveilig de toegang tot de apparaten met een wachtwoord, pincode of anderszins.
  - Zorg ervoor dat niemand anders op uw apparaten kan internetbankieren.
  - Log altijd uit bij internetbankieren.

- **Controleer uw bankrekening**
  - Controleer minimaal elke twee weken uw digitale rekeninginformatie. Wie nog papieren afschriften ontvangt moet die het liefst binnen twee weken na ontvangst controleren.

- **Meld incidenten direct aan de bank en volg aanwijzingen van de bank op**
  Denk daarbij aan:
  - Uw bankpas is gestolen of kwijt.
  - U weet of vermoedt dat anderen uw beveiligde gegevens hebben gebruikt.
  - In het rekeningoverzicht staan transacties waarvoor u geen toestemming hebt gegeven.
  - Uw mobiele apparaat met daarop een banktoepassing is gestolen of kwijt.

Mocht u toch slachtoffer worden van fraudeurs, dan hebt u grotere kans op schadevergoeding door de bank als u zich aan deze principes houdt.

Hoe strikt zijn die vijf principes?

De vijf principes van banken zijn in feite richtlijnen die de klanten van de bank helpen op een veilige manier digitaal te bankieren. Maar zoals ze zelf zeggen: 'De banken zijn zich ervan bewust dat de gemiddelde consument zich niet 100 procent tegen internetcriminelen kan beveiligen. Daar houden de banken rekening mee in hun beoordeling of klanten recht hebben op vergoeding van de schade.'
Wat betekent dat? Ook mensen die zich niet houden aan de vijf principes kunnen, wanneer zij fraudeslachtoffer zijn, een schadevergoeding krijgen. Per geval onderzoekt de bank of er sprake is van grove nalatigheid. Pas als dat wordt aangetoond, vervalt het recht op een schadevergoeding.

Veilig bankieren met de pc, tablet en smartphone

Wat moet u nu precies doen om veilig te kunnen internetbankieren? Het spreekt voor zich dat u de eigen computer goed beveiligt. Zo'n beveiliging is niet alleen nodig bij internetbankieren. U wilt sowieso geen indringers op uw pc. In het artikel 'In 10 stappen veilig' leest u er alles over. En verder vindt u op de website onder het thema Veiligheid tal van artikelen die u helpen uw apparaten goed te beveiligen.
Hieronder sommen we op waar u op moet letten, wilt u veilig kunnen bankieren én internetten:

- **Update besturingssysteem**
  Zorg dat u altijd de laatste updates van uw besturingssysteem hebt geïnstalleerd.
- **Antivirusprogramma**
  Installeer eventueel een antivirusprogramma en zorg dat u altijd de laatste updates hebt. Voer elke maand een scan van uw systeem uit.
- **Software**
  Ook andere programma's die u op de pc hebt gezet, kunnen veiligheidslekken bevatten. Installeer daarom altijd de laatste updates van software.
- **Draadloos thuisnetwerk**
  Zorg dat uw draadloze netwerk (wifi) is beveiligd met een sterk wachtwoord.
- **Wifi-netwerk**
  Maak alleen verbinding met vertrouwde wifi-netwerken. Bij openbare en onbeveiligde wifi-netwerken kunnen anderen mogelijk zien wat u op internet doet en welke gegevens u verstuurt.

- **Verdachte e-mails en bestanden**
  Open geen e-mails die u niet vertrouwt. Klik niet op onbekende bijlages in e-mails. En krijgt u een e-mail waarin u wordt verzocht met uw (bank)gegevens in te loggen op een systeem, ga er niet op in. Officiële instanties vragen nooit om uw gegevens. Vertrouwt u het niet, neem dan contact op met uw bank.
- **Webadres**
  Banken maken gebruik van beveiligde adressen. Controleer dit: ziet u in de adresbalk 'https:"//' en een slotje? Dan hebt u te maken met een beveiligd adres.

Ook mobiele apparaten moeten beveiligd worden. Lees daarover in het artikel 'Veilig mobiel internetbankieren'.

BRON: SeniorWeb/NVB