Speel op safe

De websites van Nederlandse banken zijn zo goed beveiligd, dat de kans vrijwel nihil is dat ze worden gekraakt. De zwakke schakel is de internetgebruiker zelf. Lees waarop u moet letten als u gaat internetbankieren.

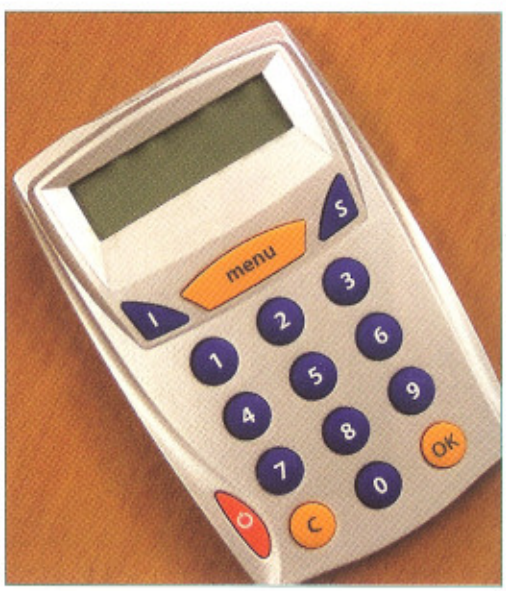
Dick van Vugt (SeniorWeb)

"Is het wel veilig?" Dat is volgens Dick van Vugt, voorzitter van het leercentrum van SeniorWeb in het Land van Heusden en Altena, de belangrijkste vraag die mensen bezighoudt als ze beginnen aan een cursus internetbankieren. De Brabantse afdeling van SeniorWeb biedt vaak cursussen internetbankieren aan, alle verzorgd door de Rabobank.

Moeite met het apparaatje

Van Vugt voegt eraan toe: "Voor internetbankieren blijkt toch basiskennis van de pc nodig. Deelnemers zonder enige computerervaring, kwamen er met het internetbankieren niet goed uit."

Wat Van Vugt ook opviel, was dat de internetbankierders in spe niet zozeer moeite hadden met de website van de bank, maar wel met de bijgeleverde Random Reader. Zo noemt de Rabobank het apparaatje dat u samen met de bankpas nodig hebt om via internet toegang te krijgen tot uw bankrekening. De bankpas gaat in het apparaat en vervolgens voert u uw 'gewone' pincode in, die ook gebruikt om geld te pinnen. Daarna is het een kwestie van codes invoeren op het apparaat en op de website. Volgens Van Vugt maken deelnemers veel fouten bij het intoetsen van de vaak lange codes.



Kleine kans op kraak

Behalve de Rabobank, werken ook ABN AMRO en Fortis met een systeem van een los apparaatje in combinatie met de bankpas. Hoewel het omslachtig lijkt, garandeert zo'n apparaatje wel de veiligheid van het geld op de rekening. Want voor toegang tot de rekening is zowel de bankpas als een pincode nodig. Bovendien worden de gegevens die u invoert op de website verstuurd over een versleutelde verbinding, zodat ze voor buitenstaanders onleesbaar zijn.

"Nergens ter wereld is internetbankieren zo veilig als in de Benelux," volgens Eddy Willems van beveiligingssoftwarebedrijf Kapersky. "De kans dat de website van de bank wordt gekraakt is praktisch nihil."

Zwakke schakel

De website van de bank is dus betrouwbaar, maar op andere plekken kan de beveiliging wel 'lek' zijn. De internetgebruiker zelf, en zijn pc en internetverbinding, vormen de zwakke schakel. Laat ten eerste nooit iemand meekijken bij het pinnen op de Random Reader (of hoe uw bank het apparaatje noemt), net zomin als u dat doet bij het pinnen bij de geldautomaat.

Volgens Frank Visser van de Rabobank moeten mensen daarnaast hun pc goed op orde hebben. "Zorg er in de eerste plaats voor dat de firewall en software helemaal up-to-date zijn. Denk daarbij aan de updates van bijvoorbeeld Windows en een bijgewerkt antivirusprogramma."

Behalve een veilige pc, is ten slotte een veilige internetverbinding een must. Want hoewel de bank haar informatie versleuteld verstuurt, kan via een onbeveiligde draadloze (WiFi) verbinding toch iemand meekijken op de pc.

Eddy Willems (Kaspersky)

Eddy Willems adviseert dan ook dat internetgebruikers zich ervan vergewissen dat hun draadloze verbinding beveiligd is. Niet internetbankieren dus op een algemeen toegankelijke WiFi-verbinding die bijvoorbeeld op de camping in de lucht hangt.

Frank Visser van de Rabobank voegt hieraan toe: "Controleer daarnaast altijd of u op een versleutelde website zit. In de browser is dat te zien aan het slotje, maar ook aan https in het webadres in plaats van alleen http."

Mogelijke gevolgen

Niet op safe spelen kan vervelende gevolgen hebben. Op een slecht beveiligde pc kunnen zich programmaatjes installeren die u omleiden naar een website die lijkt op die van de bank. Zo kunnen computercriminelen gegevens van de gebruiker ontfutselen.

Een ander gevaar zijn pop-up schermen waarop de internetbankierder nog even wordt ge-

Frank Visser (Rabobank)

vraagd naar zijn creditcardgegevens. Willems: "Nu zal lang niet iedereen dat doen, maar vooral lichtgelovige gebruikers met weinig computerervaring denken 'als de bank dat vraagt, zal het wel kloppen'."

Nederland heel veilig

Overigens richten kapers van betalingsgegevens zich niet zo heel vaak meer op het geld van de Nederlandse rekeninghouders. Omdat het zo moeilijk is een Nederlandse bankwebsite te kraken, richten computerpiraten zich vaker op sites van banken in andere delen van de wereld, zoals de VS of Zuid-Amerika, waar het volgens Eddy Willems een stuk minder veilig is om geldzaken te regelen via internet.

Test veilig internetbankieren

De Nederlandse banken voeren gezamenlijk een campagne voor het verbeteren van de veiligheid van internetbankieren, genaamd '3x kloppen' (www.3xkloppen.nl).
Volgens de banken neemt een op de vijf consumenten onvoldoende maatregelen bij het internetbankieren: ze werken met een verouderd of geen antivirusprogramma, antispywareprogramma en/of spamfilter. Slechts een deel van de consumenten downloadt regelmatig updates voor deze programma's. Bovendien reageren te veel mensen op onbekende e-mails.
Met de campagne willen de banken mensen informeren over wat zij zelf kunnen doen om veilig te internetbankieren. U vindt alle informatie op de website **www.3xkloppen.nl**. U kunt ook in een test nagaan of u zelf veilig internetbankiert: **www.3xkloppen.nl/doe-de-test**

Martine de Vente