Pas op voor de nieuwe zakkenrollerij

Het aantal gevallen van pinpasfraude en oplichting met elektronisch bankieren is sterk gedaald. Maar criminelen zijn vindingrijk en weten met slimme trucs toch uw rekening leeg te halen.

Tekst **Judith van Ruiten** | Foto **Hollandse Hoogte** | Illustratie **iStock**

Tientjestruc

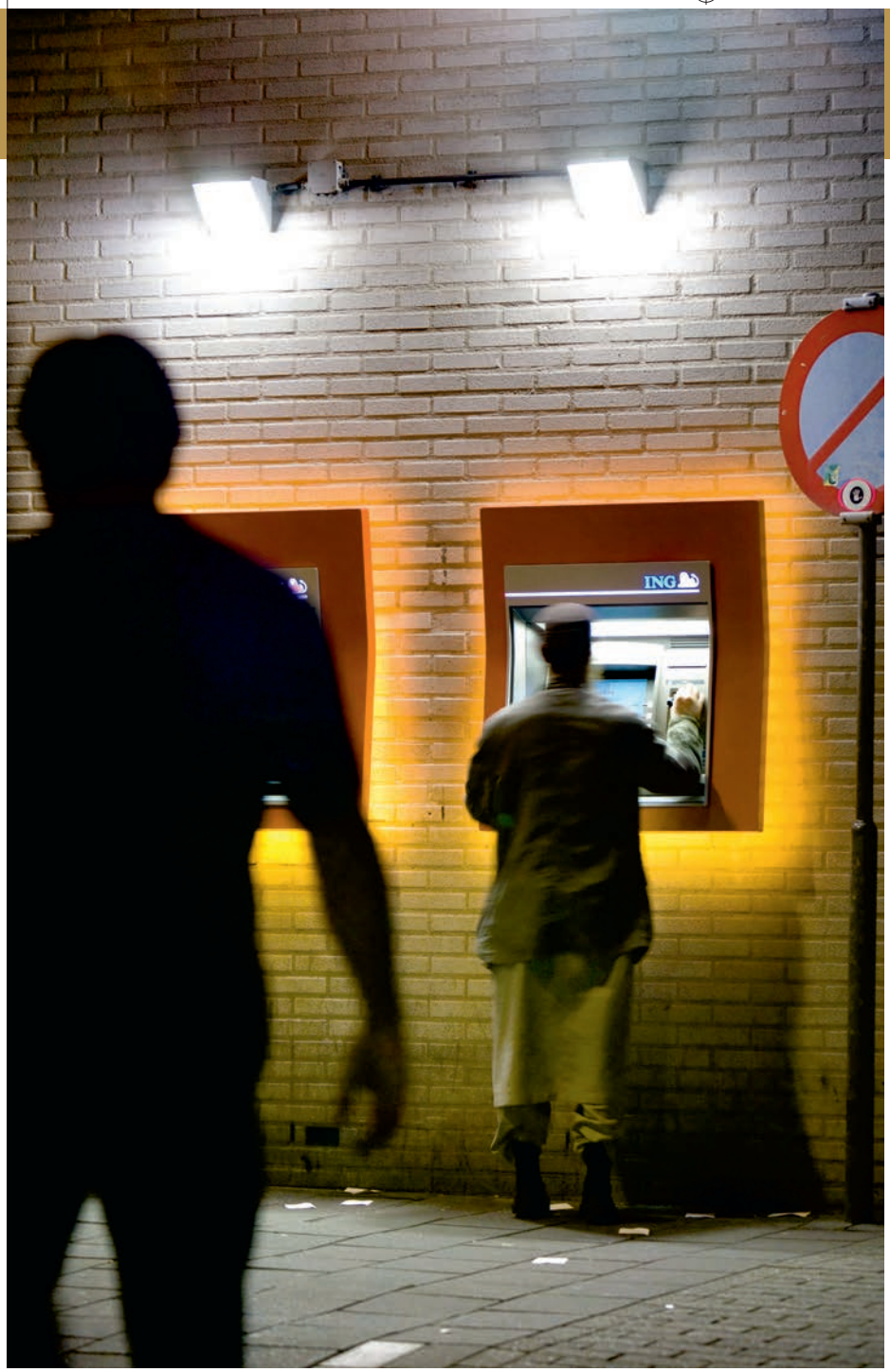
Banken kunnen het niet vaak genoeg herhalen: scherm uw pincode goed af met uw hand tijdens het invoeren. Want als u pech hebt, gluurt iemand mee over uw schouder. Als u vervolgens geld wilt opnemen bij een bankautomaat, leidt deze persoon of een handlanger u af. Hij laat bijvoorbeeld een tieneurobiljet of iets anders waardevols op de grond vallen zodat u dat gaat oprapen. Ondertussen verwisselt hij als een soort Hans Klok uw pinpas of creditcard met een vals exemplaar in dezelfde kleur. De crimineel heeft nu zowel uw pas als pincode te pakken en kan zijn slag slaan.

Card trapping

Als uw pincode eenmaal is afgekeken, is er nog een andere doortrapte manier om u te beroven. Door middel van het zogeheten *card trapping*, waarbij de pas blijft vastzitten in een door de crimineel geprepareerde pasgleuf. Als de pashouder ten onrechte denkt dat de pas is ingeslikt en wegloopt, haalt de crimineel deze met een tangetje tevoorschijn. Ook hij heeft nu de originele pas en pincode. Bingo.
Is uw pincode eenmaal afgekeken, dan zijn er overigens ook minder inventieve manieren om aan uw pas te komen. Door uw portemonnee te rollen bijvoorbeeld.
De invoering van contactloos betalen maakt het zakkenrollers nog makkelijker. Zij kunnen tot €50 met uw pinpas afrekenen zonder dat zij gebruik hoeven te maken van een pincode. Banken vergoeden de schade alleen als u tijdig meldt dat de pas is gestolen.

Cash trapping

Cash trapping is voor de iets luiere crimineel, die geen zin heeft om een pincode af te kijken of een portemonnee te stelen.
Hierbij plakt hij met tweezijdig plakband de bankbiljettengleuf van binnenuit dicht. Als de pashouder vervolgens geld opneemt, gaat de gleuf niet open. Als hij aan een storing denkt en vertrekt, opent de crimineel de gleuf en vertrekt met een goedgevulde portemonnee.
De politie adviseert mensen die via een van de bovengenoemde methoden worden opgelicht, om direct de bank en politie te bellen. Laat u dus niet opjagen door de persoon achter u die 'zogenaamd' haast heeft om geld op te nemen, maar blijf waar u bent en wacht op verdere instructies.



Laat u nooit opjagen bij een bankautomaat door iemand achter u.

Babbeltruc

Een ander belangrijk advies luidt om uw pincodes niet thuis te laten rondslingeren, maar uit uw hoofd te leren. Bent u zo'n sloddervos, dan bent u een gewild slachtoffer van de babbeltruc. Dat begint met een praatje aan de deur van iemand die zich voordoet als medewerker van een betrouwbaar bedrijf of instelling. Bijvoorbeeld een medewerker van de bank, een energiemaatschappij of thuiszorginstelling. Als die persoon met u mee naar binnen loopt, glipt een handlanger als een soort van illusionist naar boven. Hij stopt soms zelfs ongezien iets tussen de deur om die te kunnen openen, terwijl u denkt die te hebben gesloten. Als u aan de praat wordt gehouden, trekt de handlanger boven de boel ondersteboven om er met waardvolle spullen en wellicht uw bankgegevens vandoor te gaan.

Of uw gesprekspartner werkt alleen en probeert al vragend gaandeweg achter uw bankgegevens te komen. Banken zeggen het keer op keer: geef nooit uw pincode en internetbankiergegevens af. Ook banken zullen hier nooit om vragen. Doet u dit wel, dan komt u mogelijk niet in aanmerking voor een schadevergoeding. Lees voor meer informatie het kader 'De vijf B's van veilig internetbankieren' op de volgende pagina. ▶

De 5 B's van veilig internetbankieren

Om fraude te voorkomen, is het belangrijk dat u zich houdt aan de vijf B's van veilig bankieren, die de banken hebben opgesteld in samenwerking met de Consumentenbond. Doet u dat u niet, dan loopt u het risico geen schadevergoeding te ontvangen.

BEWAAK UW PAS

Ook uw pas is strikt persoonlijk. Leen die dus niet uit en laat u niet afleiden als u uw pas gebruikt.

BEVEILIG UW APPARATUUR

Gebruik om uw bankzaken te regelen een computer of laptop met daarop een virusscanner, firewall en anti-spyware. Voer beveiligings-updates altijd direct uit.

BESCHERM UW CODES

Vraagt iemand naar uw beveiligingscodes? Geef deze dan niet af. Uw codes zijn strikt persoonlijk.

BEKIJK UW AFSCHRIJVINGEN

Alleen u kunt beoordelen of er terecht geld van uw rekening is afgeschreven. Bekijk daarom minimaal één keer per twee weken uw afschrijvingen. Is er geld van uw rekening afgeschreven zonder dat u daarvoor toestemming heeft gegeven? Neem dan direct contact op met de bank.

BIJ TWIJFEL, BEL DE BANK

Kijk voor een verdere toelichting van de veiligheids-regels op www.veiligbankieren.nl.

Phishing

Het hengelen naar persoonlijke gegevens door zogenaamd betrouwbare organisaties gebeurt niet alleen aan de deur, maar ook via de telefoon of mail. Zo komen op Facebook de laatste tijd nepadvertenties voorbij van McDonald's, waarin een waardebon van €200 wordt beloofd. In een nepmail van Albert Heijn vraagt de supermarkt mee te werken aan een onderzoek. Wie op de berichten klikt, installeert ongemerkt kwaadaardige software op zijn computer. U merkt er vaak niets van. De computer is hooguit wat trager. Maar ondertussen worden stiekem gegevens verzameld, zoals creditcard- en bankgegevens of de inlogcodes van Marktplaats. Uw mailaccount kan zo worden gebruikt om spam- of phishingberichten te versturen. En uw Marktplaats-account biedt voor criminelen een perfecte dekmantel om valse producten te

verkopen. Zorg er daarom altijd voor dat uw virusscanner actief en up-to-date is.
Kijk ook uit voor mails die van uw bank lijken te komen. Klikt u daarop, dan kunt u op een exacte kopie van de website van de bank komen. Zelfs de aanduiding 'https://' in het internetadres (met de 's' van secure, ofwel 'veilig') met het gele hangslotje kan nep zijn. Ga er gerust van uit dat financiële instellingen niet met hun klanten communiceren via e-mail en zeker niet via deze weg om persoonlijke gegevens vragen.

Skimming

Deze vorm van fraude is binnen Europa zo goed als uitgeroeid dankzij de invoering van de EMV-chip op pinpassen. De fraudegevoelige magneetstrip werd voorheen veelvuldig door criminelen gekopieerd op een valse pas. De pincode werd achterhaald door een cameraatje.
Het euvel is nog niet helemaal opgelost. "Skimmen kan nog wel gebeuren in door criminelen bewerkte apparaten waar de pinpas volledig in verdwijnt, zoals betaalautomaten van banken", weet adjunct-directeur Gijs Boudewijn van Betaalvereniging Nederland. "Maar cashen kan alleen in landen buiten de Europese Unie die nog niet over zijn op de chip."
Dit is de reden voor de invoering van het zogeheten 'geoblocking', het standaard blokkeren van bankpassen buiten Europa. Wie naar dit deel van de wereld op vakantie gaat, moet om te kunnen pinnen zijn pas voor vertrek eerst 'aanzetten'. ■

DE GEDUPEERDE

'40.000 euro in één klap weg'

Jaap van Buren kan zichzelf nu wel voor zijn hoofd slaan. Want al bij de eerste mail van de Rabobank voelde hij argwaan. Maar hij negeerde dat gevoel toen de bank wilde helpen zijn rekeningnummers om te zetten naar IBAN. Hij mailde zowel zijn naam als telefoonnummer door. Niet veel later werd hij gebeld door iemand van de bank. "Ik kreeg een keurige medewerkster aan de lijn die mij wilde helpen mijn rekening om te zetten naar IBAN, omdat ik anders niet meer kon betalen." Dat wilde hij wel en hij gaf zijn inloggegevens door. Vervolgens voerde hij twee codes in die de mevrouw doorgaf en daarna was de klus geklaard.
Maar toen Van Buren 's avonds zijn rekening controleerde, kreeg hij de schrik van zijn leven. Er was bijna €40.000 van zijn rekening afgeschreven. Al het spaargeld van Jaap en Janine van Buren was weg. "De codes die ik had ingetoetst, bleken achteraf gezien geldbedragen te zijn geweest en een rekeningnummer", vertelt Jaap schuchter.
Het stel nam meteen contact op met de bank en de politie. Maar die hadden slecht nieuws. Ze konden waarschijnlijk fluiten naar hun geld, omdat ze nalatig waren geweest en hun bankgegevens hadden prijsgegeven.
Tweeënhalve maand later liep de zaak toch nog met een sisser af. De politie had ontdekt dat het geld was overgemaakt naar een autohandelaar in het zuiden van het land met een rekeningnummer van een Turkse bank.
"Het was netjes geweest als de bank hierover contact had opgenomen, want hij heeft immers een zorgplicht", weet Lotte Reijmer van de Fraudehelpdesk, waar Van Buren melding had gemaakt van de zaak. Van Buren: "Ik heb zelfs gedreigd met een advocaat, maar uiteindelijk hoefde het zover gelukkig niet te komen. We hebben ons geld teruggekregen. Maar dezelfde zijn we niet meer."

De namen van Jaap en Janine van Buren zijn om redenen van privacy gefingeerd.

Lees meer over veilig internetten op **www.plusonline.nl/veiliginternet**