hcc SENIORENACADEMIE ig
leert u de computer kennen

Nederlandse Vereniging van Banken

Veilig internetbankieren en online betalen

Hoe vergroot u uw online weerbaarheid?

Pascal Middelhof

Jope Welter

Van harte welkom!

Agenda

1. Internetbankieren in Nederland
2. Criminaliteit in het elektronisch betalingsverkeer
3. Tips voor veilig internetbankieren en online betalen

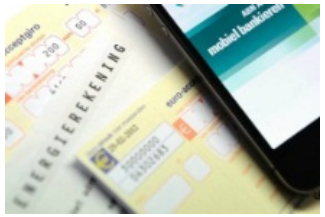
1. Internetbankieren en online betalen in Nederland

Nederland koploper qua gebruik internetbankieren

- Begin jaren ’90 introduceerden banken elektronisch bankieren
- Zeven op de tien (10,2 mln.) Nederlanders van 12 jaar en ouder regelden in 2012 hun dagelijkse bankzaken via internet
- 93% van de overboekingen gedaan via internetbankieren en nog 7% via papieren opdrachten. Van alle Acceptgiro’s werd in 2012 bijna 80% via internetbankieren betaald
- Sinds 2005 is aandeel internetbankierende Nederlanders met meer dan helft toegenomen. Vooral ouderen hebben inhaalslag gemaakt
- Hiermee heeft Nederland samen met Finland het hoogste aandeel inwoners dat internetbankiert in EU (EU-gemiddelde 37%)
- Internetbankieren is qua functionaliteit sterk ontwikkeld, veilig, betrouwbaar en kostenefficiënt. Beschikbaarheid is zeer hoog (24/7), al zijn incidentele verstoringen nooit volledig uit te sluiten

Gebruik mobiel bankieren is *booming*

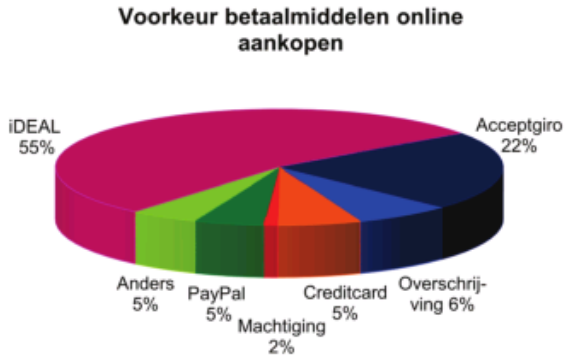
- Aantal gebruikers in 2012 verdubbeld.
- Eind 2012 had 42% van smartphonebezitters een mobiel bankieren-app geïnstalleerd
- Opvragen van actuele saldo is populairst. Nederlandse jongeren denken met mobiel bankieren meer grip op hun geld te hebben
- 41% van de Nederlanders bankiert mobiel, t.o.v. 25% van de Europese consumenten
- Inmiddels wordt mobiel bankieren vaker gebruikt dan internet bankieren



Betalen online aankopen

- iDEAL is favoriete betaalmethode voor Nederlandse online kopers. In 2012 betaalde 54% hun online aankoop via iDEAL
- Belangrijkste voordelen van iDEAL zijn: veiligheid, feit dat betaling meteen is afgehandeld en gemak
- 93% van de webwinkeliers in Nederland accepteert iDEAL
- Voor online aankopen bij buitenlandse webshops gebruiken Nederlanders meestal hun credit card (54%), gevolgd door PayPal (25%) en overschrijving (14%)

iDEAL Online betalen via uw eigen bank



2. Criminaliteit in het elektronisch betalingsverkeer

Criminaliteit in betalingsverkeer is niets nieuws…

Heel vroeger…

Vroeger…

Tegenwoordig…

Fraudevormen - *Phishing*

- Verzamelnaam voor digitale activiteiten waarmee criminelen proberen persoonlijke informatie te ontfutselen
- Met deze informatie kan fraude met internetbankieren, pinpassen, creditcards of identiteit worden gepleegd
- Vaak gericht op grote groep personen, maar kan ook specifiek op één persoon of kleine groep zijn gericht (*spear phishing*).
- Vaak gebruik gemaakt van *social engineering*; misbruiken van menselijke eigenschappen zoals nieuwsgierigheid, vertrouwen, hebzucht, angst en onwetendheid.

- Video '*Wat is phishing?*'
- Video '*Wat is social engineering?*
- Video '*Een real life voorbeeld*'

Fraudevormen - *Malware*

- Malware (malicious software) is vijandige, schadelijke of irritante software
- Criminelen ontwerpen speciale software die een computer infiltreert zonder dat de eigenaar dat merkt, laat staan toestemming voor geeft
- Kan de computer binnenkomen via e-mail, afbeeldingen of links op websites, USB-sticks, etc.
- Voorbeelden: *Keyloggers* en *screenloggers*, *session hijacking*, *web trojans*, *pharming*, *content-injection*, *man-in-the middle*, etc.

- Video '*Wat is malware?*'

Fraudevormen - *Skimming*

- Kopiëren van pasgegevens door plaatsen extra kaartleesapparaatje op pasinvoer van geld- of betaalautomaat.
- Criminelen kijken vervolgens pincode af (*shouldering*), waarna zij geld van de rekening van de gedupeerde opnemen.

- Video '*Skimmers*'

Cashen via *geldezels*

- Laat zijn bankrekening tegen beloning misbruiken om geld (o.a. verkregen door phishing, malware en/ of skimming) weg te sluizen.
- Sluist hierbij (on)bewust frauduleus verkregen geld door naar criminelen.
- Door gebruik van zo'n 'tussenstation' is de identiteit van de crimineel moeilijker te achterhalen.
- Geldezels worden vrijwel altijd gepakt; hun identiteit is makkelijk te achterhalen. Immers, hun bankrekeningnummer is bekend.

Fraudeomvang

Internetbankieren

- In 2012: € 34,8 mln. (≈ 0,001% van totale transactieomzet)
- Aantal geslaagde incidenten: 11.000 ≈ 0,0000037% van totaal aantal transacties. Gem. schade per incident: € 3.200,-
- Schade vertoont sinds 2e helft 2012 spectaculaire daling

Skimming pinpassen

- In 2012: € 29,0 mln. ≈ 0,02% van totale transactieomzet
- Incidenten waarbij sprake was van *cashing* door criminelen: 51.000 stuks. Gem. schade per incident: € 570,-
- In 1e halfjaar 2013 spectaculaire daling.

Maatregelen tegen fraude internetbankieren

- IT systemen veilig inrichten en houden (veilig, maar ook gebruiksvriendelijk), bijv. door toepassing *two-factor authentication* bij internetbankieren
- Fraudedetectiesystemen (7*24 transactiemonitoring): vele frauduleuze transacties worden sneller en vaker gedetecteerd en gestopt
- *Geo-blocking*: Overboekingen via internetbankieren buiten Europa standaard geblokkeerd
- Informatie-uitwisseling tussen banken rond (potentiële) fraudezaken
- Registratie van fraudeurs (met name *money mules*) in interbancair waarschuwingssysteem

Maatregelen tegen fraude internetbankieren

- Collectieve NVB bewustzijnscampagnes: Veilig Bankieren (TV commercial *Phishing*, veiligbankieren.nl en geldezelcampagne)
- Nieuwe campagne in ontwikkeld om consumenten nog weerbaarder te maken (dec. 2013 live)
- Banken hanteren een ruimhartig vergoedingenbeleid; vergoeden schade bij fraude altijd, tenzij klant grof nalatigheid is

- Video: '*NVB commercial Phishing*'

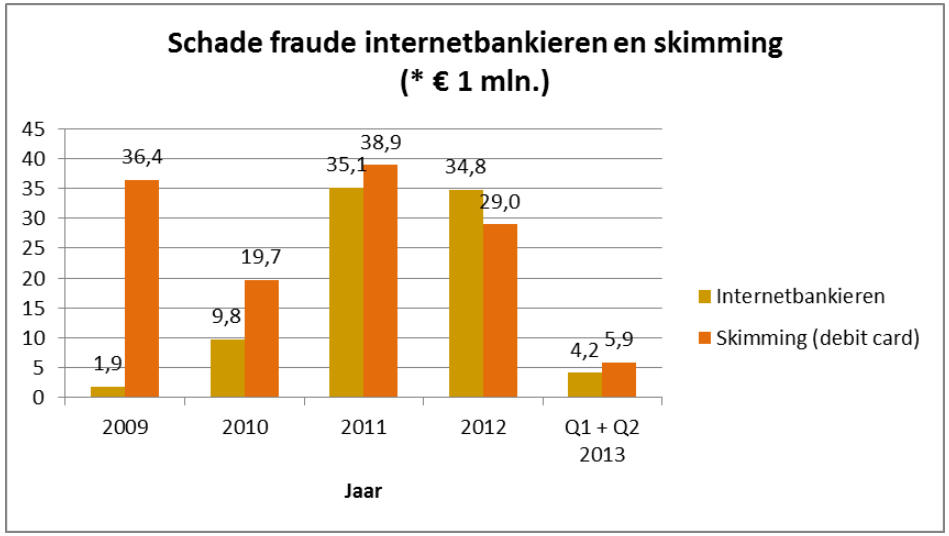
Maatregelen tegen skimming

het nieuwe pinnen.nl

- Invoering EMV chip: Het nieuwe pinnen. Betalingen via chip i.p.v. magneetstrip. '*Dippen*' i.p.v. '*swipen*'
- Beveiliging onbemande betaal- en geldautomaten (voorzetmondjes e.d.)
- Detectiesystemen (7*24 transactiemonitoring) op frauduleuze geldopnames
- *Geo-blocking*: Opnames bij geldautomaten met betaalpas buiten Europa standaard geblokkeerd. Cashing voor criminelen wordt stuk lastiger
- Samenwerking in het Landelijk Skimmingpoint (t.b.v. de opsporing)
- Banken vergoeden skimmingschade altijd, tenzij de klant grof nalatigheid is

Fraude – Conclusie

- Fraude via internetbankieren en skimming onder controle; laatste tijd flink afgenomen
- Helaas onmogelijk voor banken om zich volledig tegen cybercriminaliteit te wapenen, hoeveel inspanningen en middelen er ook in beveiliging gestoken worden
- Wedloop met cybercriminelen; hanteren telkens nieuwe technieken om organisaties die zij aanvallen te verrassen
- Klanten worden steeds meer bewust en alert



3. Enkele tips voor veilig internetbankieren en online betalen

Wees alert en kritisch

- Wees ervan bewust dat criminelen op uw gegevens (en geld) uit zijn
- Wees altijd heel kritisch voor u (persoonlijke) gegevens afgeeft aan willekeurige (onbekende) personen
- Bedenk dat uw bank u nooit zal vragen om beveiligingscodes op onverwachte momenten of plekken, dus nooit per e-mail en /of telefoon
- Zorg ervoor dat niemand kan meekijken als u uw beveiligingscodes intoetst.
- Schrijf of sla de codes niet op. Of, als u denkt de codes te vergeten, alleen in een voor anderen onherkenbare vorm die alleen door uzelf is te ontcijferen
- Heeft u toch persoonlijke gegevens gegeven aan een phisher of stuit u op onverwachte zaken bij het internetbankieren? Meld dit dan direct bij uw bank (call center en/of bankkantoor)

Wees alert en kritisch als

- Aanbiedingen te mooi zijn, om waar te zijn
- Er iets mis lijkt te gaan tijdens het surfen en er direct een pop-up verschijnt om u uit de brand te helpen
- U de mededeling krijgt dat er iets mis is gegaan bij bezoek aan een site en vervolgens advies krijgen om op een link te klikken om het probleem op te lossen
- Een e-mail van een bekende u vreemd voorkomt
- U e-mail krijgt van een afzender die u niet kent
- Er via internet persoonlijke gegevens aan u worden gevraagd
- Controleer regelmatig uw bankrekening

Zorg dat PC, tablet en smartphone in orde zijn

- Gebruik antivirusprogramma, firewall, anti-spywareprogramma en zorg dat die up-to-date blijven
- Gebruik spamfilter en verwijder e-mails waarover u twijfelt
- Gebruik de meest recente updates van besturingssysteem (Windows, Mac OS, etc.) en zet de automatische update-functie aan
- Gebruik de meest recente versies van software die u gebruikt. Gebruik indien mogelijk ook de automatische updatefunctie
- Beveilig uw PC, tablet en smartphone met een toegangscode

Alles nog eens rustig nalezen?

www.veiligbankieren.nl

VEILIG BANKIEREN