Jagen op de onnozele consument

door Thomas Olivier. zaterdag 16 augustus 2008 | 03:29

Criminelen worden steeds slimmer in het ontfutselen van pincodes, banknummers en creditcardgegevens aan de argeloze internetgebruiker. Klanten van de Postbank lopen extra risico, want deze bank heeft het betalingssysteem alleen beveiligd met gebruikersnaam en wachtwoord. Ook klanten van andere banken moeten echter alert blijven. „Er zijn altijd mensen dom genoeg om er toch in te trappen."

Begin juni 2005: honderdduizenden klanten krijgen een mailtje van hun bank. Denken ze. 'Dear Postbank Costumer', luidt de aanhef. Of de 'Lieve Postbankklant' even via een link naar de site van de bank wil surfen om wat gegevens in te voeren zoals pincodes en inlogcodes voor internetbankieren, uiteraard voor zijn eigen veiligheid.

Een maand geleden: Postbankklanten krijgen opnieuw een mail met het verzoek gegevens in te vullen. De link stuurt de klant naar een website die bedrieglijk veel op de Postbanksite lijkt, inclusief links naar de échte website van de bank. Pikant detail: een verwijzing leidt naar de pagina van de Postbank over veilig internetbankieren.

In ruim drie jaar tijd heeft phishing, zoals deze praktijk heet, definitief voet aan de grond gekregen in Nederland. Het hengelen naar bank- en creditcardgegevens was eens voorbehouden aan computerfreaks die beveiligingssystemen voor de roem kraken. Nu is het big business. Internationaal opererende criminelen gaan steeds slinkser te werk en gebruiken betere technieken.

Wie nog steeds in de rammelende Postbankmails trapt, is niet van deze tijd, zegt Ella Broos van GOVCERT, het Computer Emergency Response Team van de Nederlandse overheid. "Maar er zijn altijd mensen dom genoeg om er toch in te trappen", stelt Jeroen Oostendorp, directeur van computerbeveiliger Cleanport.

Het mag dan dom zijn om gevoelige informatie zomaar door te geven via internet, het levert criminelen ontegenzeggelijk geld op gezien de groeiende populariteit van het fenomeen.

Broos: "Er is een illegale economie op internet ontstaan. Criminelen gebruiken de gestolen gegevens direct of verkopen ze weer door aan andere bendes."

Het einde van de opgaande trend is nog niet in zicht. Tussen maart 2007 en maart 2008 kwam GOVCERT 59 keer in actie om vervalste websites van Nederlandse banken uit de lucht te halen, in 2006 was dat nog 46 keer. Daar komt bij dat criminelen niet stil zitten. Klanten van webwinkels en veilingsites als eBay zijn ook niet veilig meer.

De internetcrimineel is de afgelopen jaren veel professioneler geworden, vertelt Oostendorp. Het rammelende mailtje is vervangen door geavanceerde manieren om de computer van een slachtoffer binnen te dringen. "De websites worden steeds beter, de logo's in mailtjes kloppen perfect en het Nederlands is vlekkeloos."

Hoogleraar computerbeveiliging Bart Jacobs van de Radboud Universiteit in Nijmegen kijkt niet op van het groeiende vakmanschap. Bendes versturen een miljoen e-mails. Slechts een zeer klein deel hapt, maar toch levert dat geld op. "Criminelen lopen op internet veel minder risico dan wanneer ze met een afgezaagd geweer een bankfiliaal binnenstappen."

Ook bij GOVCERT zien ze professionalisering van oplichters op de digitale snelweg. Broos noemt het

boven in beeld - als het origineel. Om die reden moest postorderbedrijf Wehkamp vorige maand halsoverkop een miljoen klanten waarschuwen.

ABN AMRO-klanten waren vorig jaar slachtoffer van een nog kwalijker truc. Door in het geniep virussen te installeren op computers van klanten konden criminelen de communicatie tussen ABN AMRO en internetters volgen en beïnvloeden. Het maakt de beveiliging van Nederlandse banken met paslezer, pincode en wachtwoord kwetsbaar.

De methoden die boeven uit de kast halen, worden telkens geavanceerder. Door een webpagina om de tien minuten te verplaatsen naar een provider in een ander deel van de wereld, wordt het voor instanties als GOVCERT veel moeilijker zo'n site uit de lucht te halen. Zolang de site bestaat, hebben de oplichters vrij spel.

Vooral landen waar internet nog niet tot volle wasdom is gekomen, zijn een walhalla voor webbendes. In Rusland, Oost-Europa en Brazilië is het beheer van en het toezicht op de providers een stuk minder goed geregeld. Oostendorp: "Probeer daar maar eens iemand aan de lijn te krijgen en uit te leggen dat een website platgelegd moet worden."

De strijd tegen de webboeven is bijna onbegonnen werk doordat criminelen constant een stapje voorlopen. "Hun professionele werkwijze maakt het heel moeilijk phishing helemaal te stoppen" , legt Broos van GOVCERT uit. "Criminelen zoeken naar steeds nieuwe manieren van misleiding." Oosterpoort, stellig: "Dit verdwijnt niet meer." De vernuftige technieken die internetdieven uit de kast halen, vormen slechts één kant van het verhaal. Beveiligingsexpert Jacobs legt een deel van de schuld ook bij de computergebruiker, die zich nauwelijks bewust is van de gevaren op de digitale snelweg. "Als iemand op straat om je huissleutels vraagt, dan geef je die ook niet zomaar af. Dat doet niemand. Op internet worden soms wel klakkeloos geheime gegevens verstrekt."