REACTIE ING

Het is lastig om de processen bij verschillende banken met elkaar te vergelijken. Er zijn eisen vanuit de wet aangaande de veiligheid rond digitaal bankieren. De Nederlandse Bank (DNB) houdt hier toezicht op. Elke bank geeft binnen deze wettelijke kaders hieraan zijn eigen invulling. Het punt blijft dat alle banken twee factor authenticatie dienen toe te passen om in te loggen in internetbankieren. Bij ING betekent dit dat je na het invoeren van de gebruikersnaam en wachtwoord een tweede stap moet doen met de Mobiel Bankieren App of ING Scanner.

De informatie die bij phishing wordt opgehaald kan van alles zijn. Dit kan algemene informatie zijn, maar ook specifieke rekeninginformatie. Bij de voorbeelden die wij kennen van phishing, klikt de klant op een link (bijvoorbeeld via een e-mail of per sms), waarmee deze een website opent en daarbij in de veronderstelling is dat dit de ING-website is, maar in feite een nagebootste website betreft. De klant vult de informatie in en tegelijkertijd gebruikt de fraudeur deze informatie om – indien rekeninginformatie is gegeven – in te loggen in internetbankieren. Vervolgens neemt de fraudeur contact op met de klant, doet zich voor als bankmedewerker, verifieert de gegeven informatie en komt daarmee zo geloofwaardig over dat de klant uit eigen beweging geld overmaakt en daarmee een transactie autoriseert. De fraudeur, die ook is ingelogd, kan de transactie wel zien, maar heeft niet de middelen om zelf de transactie goed te keuren.