ING gaat in de fout!

Bijna dagelijks moeten we ervaren dat we te maken hebben met e-mails die ingezet worden voor phishing. Die mails zien er steeds gelikter uit en het wordt ook steeds moeilijker voor consumenten om valse mails te onderscheiden van echte.
In die phishing mails worden ons prachtige zaken aangeboden, van gerichte informatie tot gratis producten. Het enige dat we hoeven te doen, is op een linkje klikken. Ja, zo makkelijk is het. Maar tegelijkertijd wordt onze computer, tablet of smartphone geïnfecteerd en gebeuren er de vreemdste dingen, waaronder het plunderen van onze bankrekeningen.
En in die wereld bestaat ING het, en helaas zijn zij niet de enige partij laat staan bank, om een nieuwsbrief te sturen met talloze linkjes daarin. Nu weiger ik sowieso al om op linkjes in mails van banken en andere belangrijke instellingen te klikken, gezien de risico's, maar als ik dan naar de website ga om te kijken of de inhoud van de mail daar als bericht getoond wordt, dan is er niks te vinden.
Met andere woorden, het is klikken of de boodschap missen! En een volgende keer is het klikken en geplunderd worden! Dit is ongelooflijk arrogant, ondoordacht en dom van de ING. Naast de ING wil ook ABNAMRO niet achterblijven als het om het versturen van onveilige mails gaat; zij blijken keer op keer hardleers als het om cybersecurity gaat. En als hun klanten dan vroeg of laat de dupe worden van phishing, wassen ze hun handen in onschuld.
En de oplossing is zo simpel! Gewoon NOOIT meer linkjes plaatsen in de mail, de klant verwijzen naar de website en daar het bericht plaatsen. Tegelijkertijd de klanten duidelijk maken waarom deze procedure voortaan gevolgd wordt en ze dus mailtjes die afkomstig lijken van een bank en linkjes bevatten, derhalve consequent moeten negeren. Kunnen de banken zoiets niet zelf bedenken?
De Nederlandse banken, met ING voorop, moeten dus nog veel leren op het gebied van cybersecurity. En dat bij instellingen waar security juist een topprioriteit zou moeten hebben!