Phishing voorkomen is beter dan genezen

Handleiding van Helpmij.nl

Auteur: leofact

december 2016

Phishing, oftewel het achterhalen van gebruikers- en andere gegevens via misleidende e-mails of websites, komt steeds vaker voor. Vrijwel iedereen komt er mee in aanraking en de meeste computergebruikers weten ondertussen dat je beslist niet op verdachte e-mails moet klikken, laat staan op de links die daar in staan. Wikipedia phishing

Verdacht zijn e-mailtjes die veel taalfouten bevatten en één of andere link aanbieden om bij een bank, of andere interessante instelling in te loggen. Dat kan bijvoorbeeld je DigiD of Apple ID zijn. Dit soort gegevens zijn voor de internetcrimineel zeer lucratief en dat gaat helaas ten koste van jouw privacy en je bankrekening.

Vergoeding

Wanneer je onverhoopt slachtoffer bent van phishing kun je vaak succesvol een beroep op je bank doen voor vergoeding van de opgelopen schade. Deze schade declareren is echter een hoop gedoe en de banken wijzen in toenemende mate op de eigen verantwoordelijkheid van hun klanten om de schade door phishing te voorkomen. Vergoeding wordt daardoor steeds minder een vanzelfsprekendheid. Daarnaast maken de internetcriminelen een snelle ontwikkeling door; zij leren snel van hun fouten en de phishing e-mail wordt steeds moeilijker te herkennen als zijnde malafide.

Herkenning

Het herkennen van phishing e-mail is gebaseerd op drie belangrijke pijlers:

1. Er wordt gevraagd om op een link te klikken om ergens in te loggen. Wen je zelf aan om nooit op dergelijke links te klikken. Open je eigen webbrowser en ga zelf naar het adres van de gevraagde site om in te loggen. Zo weet je zeker dat je bij de juiste site bent van bijvoorbeeld je huisbankier.
2. De tekst bevat fouten en is vaak in krom Nederlands opgesteld. Juist op dit punt worden er flink vorderingen gemaakt door de internetcriminelen. Dit maakt herkennen steeds lastiger.
3. Er is sprake van een vreemde afzender en/of de te volgen link gaat naar een vreemd adres. Ook hier op dit gebied wordt het lastiger om de malafide e-mail eruit te pikken. In toenemende mate laat de phishing e-mail adressen zien die van de geïmiteerde afzender lijken te komen.

Voorbeeld

In een poging om één en ander meer duidelijk te maken heb ik een e-mail genomen die van de SNS bank afkomstig lijkt. In dit geval heb ik gedaan wat je normaal juist niet moet doen en de link tot op zekere hoogte gevolgd. Dit heb ik gedaan op een iPad en op zo'n een manier zodat ik zelf zo weinig mogelijk risico heb gelopen. Dit is echter echt een actie die valt onder de categorie "Don't try this at home"! Gewoon niet proberen.

De bedoelde e-mail zoals hieronder afgebeeld, is qua tekst nog redelijk herkenbaar als een phishing e-mail. Het is een recent uitgebrachte nieuwe versie van phishing. Op de site van de SNS wordt hier al voor gewaarschuwd. Deze kun je hier vinden: SNS phishing voorbeelden.

Dit voorbeeld is van de SNS, maar iedere bank heeft last van phishing e-mail en heeft dan ook een dergelijke pagina.

In dit voorbeeld e-mailtje blijkt de tekst in feite een afbeelding te zijn. Hierdoor kan de e-mail voorbij je spamfilter komen, die kijkt immers naar bepaalde kernwoorden in de tekst. Gelukkig blokkeren de meeste e-mailprogramma's standaard de afbeelding en moet je meestal bewust de afdeling downloaden om deze te kunnen zien. Dit beperkt het gevaar van deze aanval al behoorlijk. Wanneer je afbeelding tonen standaard aan hebt staan, kan dat echter een ander verhaal worden.

Afzender

De volgende stap is om te controleren wie de afzender is. In iOS mail doe je dat met een tap (even vasthouden) op de afzender. Helaas is niet altijd in één oogopslag te zien dat het om een valse afzender gaat. In dit voorbeeld lijkt de mail van de SNS bank te komen.

Naast iOS mail gebruik ik ook outlook voor iOS. Daarin zijn drie klikken/taps nodig om de afzender te zien. In mijn ogen is dit een misser van de Microsoft-programmeurs. Een modern e-mailprogramma zou het de gebruiker zo eenvoudig mogelijk moeten maken om phishing te herkennen, of liever nog; gewoonweg blokkeren.

Link controleren

Twijfel je nog, dan kun je ook zelf controleren of de link in de e-mail wel naar de juiste site gaat. Je doet dat door de link in IOS even "vast te houden" Er opent zich dan een venstertje waarin je het adres getoond krijgt met de mogelijkheid om dit te openen. Dat doe je natuurlijk niet (zie de afbeelding verderop)

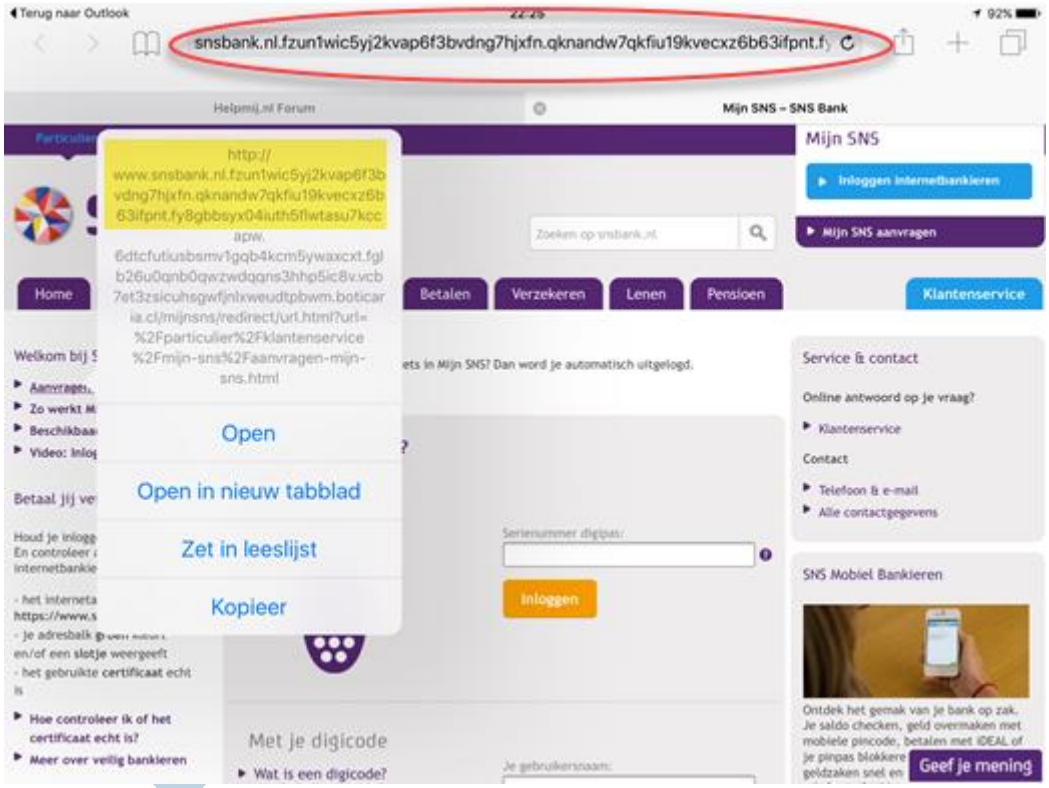
NB: in andere besturingssystemen zweef je even boven de link om het echte adres te zien.

In het geval van ons SNS phishing e-mailtje heeft de crimineel kans gezien om SNS bank in de afzender te verwerken. Het echte adres is anders, maar het is mogelijk net gelijkend genoeg om je om de tuin te leiden.

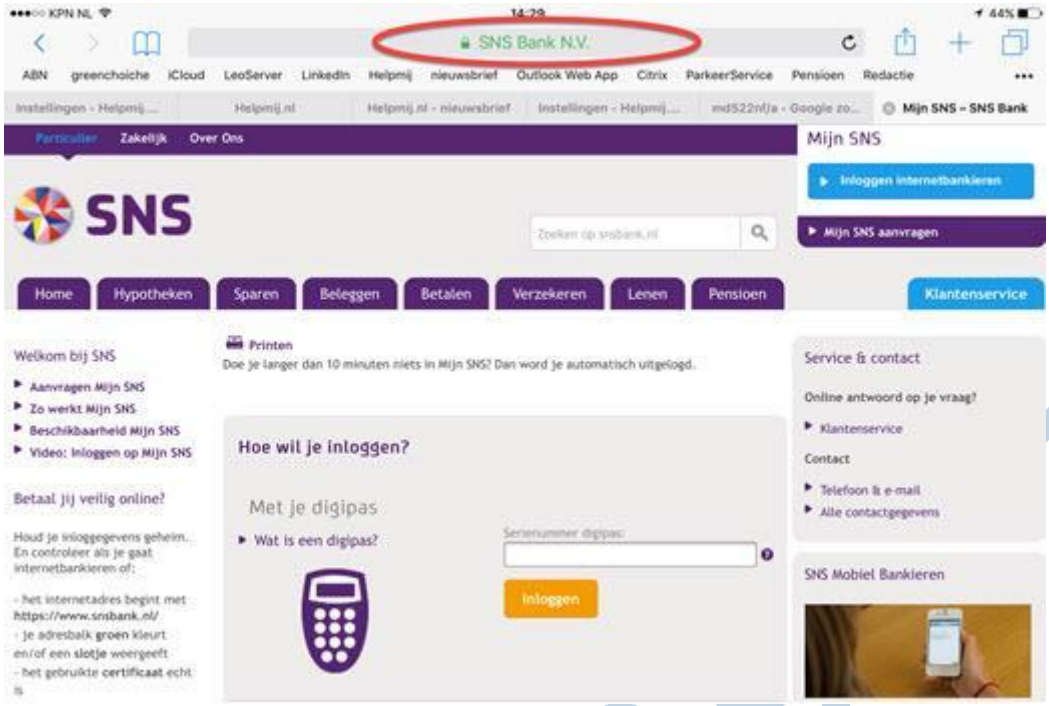
Nooit klikken

Dat laatste maakt dat ik het eerdere advies herhaal, om nooit ergens in te loggen via een link, die in e-mail wordt aangeboden. Tik zelf het adres in de adresbalk van je webbrowser, of volg je favorieten als je de betreffende site ooit eerder als favoriet hebt toegevoegd.

Ter demonstratie heb ik dat nu wel gedaan. Je ziet dan dat je op een goed gelijkende SNS-inlogpagina terecht komt. Wat hopelijk wél opvalt, is dat de adresbalk niet het noodzakelijke groene slotje bevat ten teken dat het beveiligingscertificaat in orde is.



Verder valt op dat je bij controle van een link op de site merkt dat dit niet naar een oorspronkelijk SNS-adres gaat, ook al lijkt dat er wel een beetje op. De afbeelding hieronder toont de originele site van de SNS bank:



Naar ik hoop helpen deze voorbeelden en tips bij het tijdig herkennen van phishing en zorgt dit ervoor dat je het aas herkent voor je toehapt en daardoor nooit slachtoffer wordt van deze criminele en ronduit vervelende manier om geld uit je zak te kloppen.