Phishing email

Wat is Phishing?

Phishing is een vorm van internetfraude. Het bestaat uit het oplichten van mensen door ze te lokken naar een valse (bank)website, die een kopie is van de echte website, om ze daar – nietsvermoedend – te laten inloggen met hun inlognaam en wachtwoord of hun creditcardnummer. Hierdoor krijgt de fraudeur de beschikking over deze gegevens met alle gevolgen van dien. De fraudeur doet zich hierbij voor als een vertrouwde instantie, zoals een bank. De meeste vormen van phishing gebeuren via e-mail. De slachtoffers worden hierbij met een e-mail naar deze valse website gelokt. De mail bevat een link naar de (valse) website met het verzoek om zogenaamd "de inloggegevens te controleren".

Kenmerken

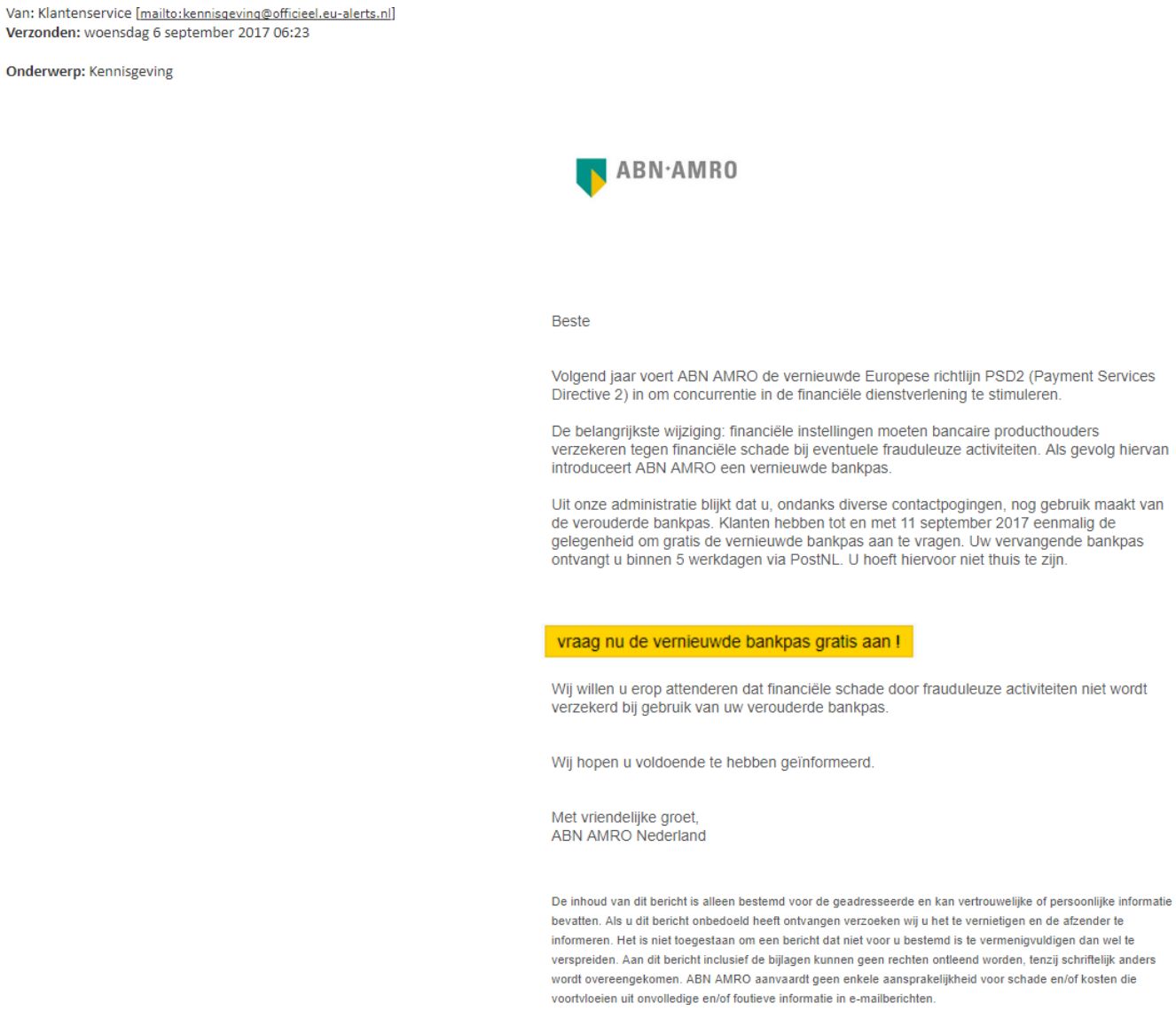
In een phishing-bericht zijn vaak de volgende elementen te vinden:

- De mail is niet aan de klant persoonlijk gericht, maar begint met een algemene opening als "geachte klant".
- De mail bevat taal- en stijlfouten.
- Er wordt gesuggereerd dat het account "geverifieerd" (op juistheid onderzocht en bevestigd) moet worden met de inloggegevens van de klant.
- Er wordt gedreigd met gevolgen als niet onmiddellijk gehoor gegeven wordt aan de mail.
- De link waarnaar wordt verwezen bevat subtiele verschillen met de originele link, zoals een andere extensie of andere schrijfwijze.

Een veelgebruikte methode is dat de fraudeur een e-mail stuurt met een bijlage waarin een keylogger of andere malware zit verborgen. De mail functioneert dan als een Trojaans paard. Zodra de gebruiker de bijlage heeft geopend, wordt – op de achtergrond – de keylogger geactiveerd. Hierdoor kan de fraudeur via internet zien welke wachtwoorden de gebruiker gebruikt bij het inloggen bij zijn of haar bank.

Voorbeeld e-mail

Middels deze e-mail willen ze op de URL-snelkoppeling laten klikken dat uw browser naar een malafide website zal laten doorsturen.



Van: Klantenservice [mailto:kennisgeving@officieel.eu-alerts.nl]
Verzonden: woensdag 6 september 2017 06:23

Onderwerp: Kennisgeving

ABN·AMRO

Beste

Volgend jaar voert ABN AMRO de vernieuwde Europese richtlijn PSD2 (Payment Services Directive 2) in om concurrentie in de financiële dienstverlening te stimuleren.

De belangrijkste wijziging: financiële instellingen moeten bancaire producthouders verzekeren tegen financiële schade bij eventuele frauduleuze activiteiten. Als gevolg hiervan introduceert ABN AMRO een vernieuwde bankpas.

Uit onze administratie blijkt dat u, ondanks diverse contactpogingen, nog gebruik maakt van de verouderde bankpas. Klanten hebben tot en met 11 september 2017 eenmalig de gelegenheid om gratis de vernieuwde bankpas aan te vragen. Uw vervangende bankpas ontvangt u binnen 5 werkdagen via PostNL. U hoeft hiervoor niet thuis te zijn.

vraag nu de vernieuwde bankpas gratis aan !

Wij willen u erop attenderen dat financiële schade door frauduleuze activiteiten niet wordt verzekerd bij gebruik van uw verouderde bankpas.

Wij hopen u voldoende te hebben geïnformeerd.

Met vriendelijke groet,
ABN AMRO Nederland

De inhoud van dit bericht is alleen bestemd voor de geadresseerde en kan vertrouwelijke of persoonlijke informatie bevatten. Als u dit bericht onbedoeld heeft ontvangen verzoeken wij u het te vernietigen en de afzender te informeren. Het is niet toegestaan om een bericht dat niet voor u bestemd is te vermenigvuldigen dan wel te verspreiden. Aan dit bericht inclusief de bijlagen kunnen geen rechten ontleend worden, tenzij schriftelijk anders wordt overeengekomen. ABN AMRO aanvaardt geen enkele aansprakelijkheid voor schade en/of kosten die voortvloeien uit onvolledige en/of foutieve informatie in e-mailberichten.

Voorkomen beter dan genezen

Wellicht is dit iets waarvan u denkt dat dit voor de hand ligt. Maar toch is het eerste **Gebruik uw gezond verstand.**

- Verwacht u e-mail van deze partij?
- Is deze manier van communicatie gebruikelijk voor de partij waarmee u zaken doet?
- Komt de mail vanuit de quarantaine, behandel deze dan ook als 'verdacht'. Ga hier extra voorzichtig te werk.

Als er een link in een bestand zit controleer deze dan eerst voor hier gelijk op te klikken.

Een link bestaat uit 2 delen.

- De display tekst. Dit is de naam die u ziet staan. In ons voorbeeld is dit http://www.google.nl
- De link. Dit is de daadwerkelijke website waar je naartoe gaat wanneer je hier op klikt

Deze kan dus verschillen.

Hoe kun je dit zien?

- Ga met uw muis op de link staan en klik hier dus **NIET**
- Vervolgens zal de daadwerkelijke link zichtbaar worden
- Wat je zult zien is dat deze verwijst naar een compleet andere website als de tekst welke zichtbaar is

Wanneer u nu op deze link zou klikken wordt u dus daadwerkelijk naar de site van Centralpoint gestuurd in plaats van de te verwachten google.nl

Bij twijfel vraag uw collega om mee te kijken, vraag de versturende partij of het correct is of neem contact op met de servicedesk van Centralpoint.

Preventieve maatregelen

Indien u ondanks dit alles toch wordt getroffen is eigenlijk de enige juiste methode om uw data terug te krijgen een restore vanuit de back-up. Dus het eerste punt:

Zorg voor een goed werkende back-up

De overige punten kunnen helpen om het buiten de deur te houden:

- Spamfilter, deze scant uw e-mail voordat dat deze bij u aankomt en verwijderd de op dat moment bekende Spam / Ransomware mails
- Firewall, op verschillende lagen wordt het verkeer geïnspecteerd en waar nodig geblokkeerd
- Anti-virus, zorg voor een goedwerkende anti-virus.
- Updates, zorg er voor dat u altijd bij bent met de beveiligings updates van Microsoft.

Dit alles samen zorgt voor een zo optimaal mogelijke beveiliging. Hou hierbij in gedachten dat 100% tegengaan een illusie is. De preventie loopt altijd achter de maker aan.

Toch besmet?

Als u onverhoopt toch besmet raakt, twijfel geen seconde en neem contact op met de Servicedesk van Centralpoint.

Hoe eerder dit gedaan is, hoe kleiner de schade zal zijn.

Wie slachtoffer is van phishing, wordt aanbevolen:

- Om de bank op de hoogte te brengen van het ontvangen bericht en van de phishingactie;
- Om codes van de online bankaccount te veranderen of deze te blokkeren;
- Om alle gegevens die bewijs kunnen leveren van de feiten en de geleden schade te verzamelen;
- Om onmiddellijk aangifte te doen bij de politie.

Revision #4
Created 26 September 2019 08:40:14 by Servicedesk
Updated 11 October 2019 10:55:05 by Servicedesk