Phishing


PHISHING
PATROUILLE
PHISHING
PATROUILLE
VERSTUUR NOOIT
UW BETAALPAS!
VEILIGBANKIEREN.NL

Betekenis woord phishing

- Het woord 'phishing' is een samentrekking van de eerste letters van 'password harvesting', oftewel wachtwoorden oogsten, en 'fishing', wat vissen betekent.

- Het heeft niets met water en dieren met vinnen te maken; de paswoordenoogst vindt online plaats.

- Daar hengelen oplichters naar jouw (bank)gegevens: inlogcodes, creditcardnummer en meer van dat soort geheime informatie.

Wat is Phishing

- Verzamelnaam voor digitale activiteiten die tot doel hebben persoonlijke informatie aan mensen te ontfutselen.

- De criminelen maken hierbij misbruik van menselijke eigenschappen zoals nieuwsgierigheid, vertrouwen, hebzucht, angst en onwetendheid.

- Door hierop in te spelen met voorbeeld valse websites, telefoongesprekken en persoonlijk contact ontfutselen criminelen vertrouwelijke informatie.

Phishing via telefoon en/of email

- Telefoon: wees voorzichtig bij informele vragen om informatie per telefoon.

- Mail: per e-mail.

Phishing via software

- Speciaal ontworpen programma (malware - trojan horse) die de gevraagde informatie vastlegt.

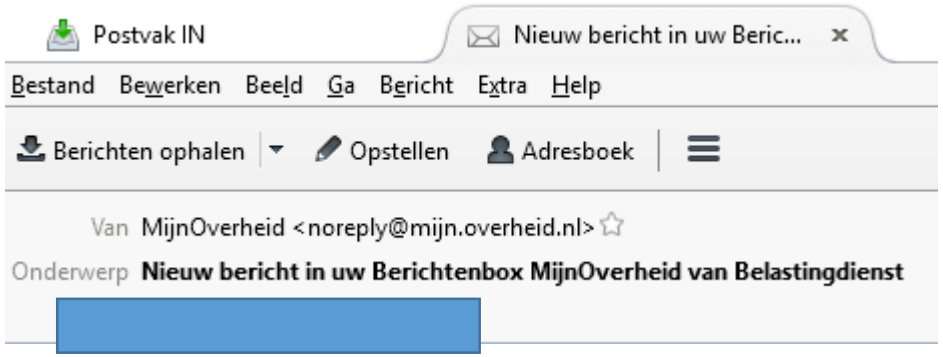
- Software die de route die u op internet aflegt zo aanpast dat u ongemerkt op een andere (criminele) nepwebsite komt. U geeft dan alle privé informatie aan criminelen.

- Software die toetsaanslagen vastlegt.

Phishing om bankgegevens

- In de financiële wereld zijn phishing e-mails er vaak op gericht om geheime kredietkaart- of e-banking - authenticatie gegevens (gebruikersnamen en paswoorden, …) te verkrijgen.

Voorbeeld van een perfecte email



Dit bericht is belangrijk voor u en u wordt verzocht (binnenkort) actie te ondernemen.
Meer informatie hierover kunt u vinden in uw Berichtenbox op MijnOverheid.

Ga naar MijnOverheid om dit bericht te lezen.

MijnOverheid stuurt geen notificaties met een link naar de website.
Dit is om te voorkomen dat u met valse e-mailnotificaties naar een namaak-website wordt geleid (zogenaamde phishing).

Neem daarom het webadres van MijnOverheid op in uw Favorieten en ga altijd van daaruit naar de website.

Ontvangt u toch een e-mailnotificatie met daarin een link, dan is deze dus nooit van MijnOverheid.

Voorbeeld van een phishing-mail

Van: "ING"<ingupdateservice@klantmail.nl>
Datum: 4 november 2015 14:04:46 CET
Onderwerp: Veiligheidscontrole
Antwoord aan: <ingupdateservice@klantmail.nl>

ING

Beste klant,

Onze systeem heeft opgemerkt dat er op uw account onlangs is ingelogd vanaf een ander IP-adres. Dit kan zijn geweest door dat u bent ingelogd vanaf een andere internetverbinding of door het herstarten van uw huidige internet modem.
De veiligheid van u bankomgeving gaat bij ons voorop en daarom zijn wij genoodzaakt om na te gaan of de toegang tot de rekening door u zelf is geautoriseerd.
Wij verzoeken u de autorisatie van de rekening via onderstaande link te bevestigen.

Verifieer uw huidige IP-adres

Als de verificatie van u rekening binnen 24 uur na ontvangst van deze email niet is voldaan, dan is het aan de ING om het betaalverkeer veilig te houden. De ING zal daarom ook een preventiefe blokkade instellen op uw MIJN ING en uw ING betaalpas.
Meer informatie

Daarnaast vragen wij u ook de bankafschrift te controleren op onregelmatige activiteiten. Merkt u een onbekende af/bijschrijving op uw rekening dient u zo snel mogelijk contact op te nemen met uw lokale bank.

Met vriendelijke groet,

ING Bank N.V Nederland.

Voorbeeld van een phishing-mail

Van: ABN-AMRO Bankieren
Datum: donderdag 17 november 2011 15:17
Aan: [redacted]
Onderwerp: Betreft: beveiligingsprocedure ABN-Bankieren

ABN·AMRO

Rotterdam, 17 november 2011

0027852

Betreft: beveiligingprocedure Mijn ABN-AMRO

Geachte heer/mevrouw,

Afgelopen donderdag is onze server ABN-bankieren aangevallen door internet-criminelen. Wij zijn bezig met ons onderzoek dat onlangs is ingesteld en hopen binnenkort deze internet-criminelen te achter halen. Tijdelijk is het noodzakelijk dat alle klanten die gebruik maken van ABN-bankieren nu momenteel op de onderstaande website inloggen en hun opnieuw verifiëren. Om uw ABN-bankieren te beveiligen dient u éénmalig uw gegevens te verifiëren op de onderstaande website. Als u éénmaal bent ingelogd word u binnen 1-5 werkdagen automatisch gebeld door onze automatische spraakmachine met verdere instructies. De spraakmachine zal u vragen of het u gelegen belt. Zo niet, kunt u de spraakmachine aangeven hoelaat/wanneer het u moet terug bellen.
Opgelet! Deze beveiliging kan alleen gestart worden door de onder staande website volledig in te vullen.
Opgelet! Het verifiëren moet binnen 48 uur gedaan worden, anders verdenken wij dat er een internet-crimineel achter uw ABN-bankieren zit.
Opgelet! Deze beveiliging kan alleen voltooid worden nadat u bent gebeld door de automatische spraakmachine en de instructies heeft gevolgd.

Klik hier! Voor de beveiligde website!
(Het kan zijn dat sommige computers het moeilijk hebben met de capaciteit van de en niet alles meer zichtbaar is)

Opgelet!
Bewaar deze brief/e-mail bij uw andere belangrijke documenten.

Hoogachtend,

Martin Westerland
Afdeling ICT & Physics

Voorbeeld van een phishing-mail

Van: ING [mailto:iban-nieuwsbrief@iban.nl]
Verzonden: maandag 2 december 2013 13:50
Onderwerp: Betreft: Over op IBAN. Wat betekent dit voor u ?

Geachte heer / mevrouw,

Vanaf 1 december krijgt iedereen in Nederland een IBAN Card. Vanaf 1 februari 2014 worden alle eurobetalingen in Europa gestandaardiseerd, als gevolg van SEPA (Single Euro Payments Area).
Hierdoor wordt het mogelijk om makkelijker internationale betalingen te doen.
Alle banken hebben zich hier op voorbereid en zullen de richtlijnen van SEPA al invoeren per 1 december 2013.

Wat merkt u van de overstap?
IBAN regelt de uitbreiding van uw bankrekeningnummer(s) automatisch voor u.
U hoeft daar dus niets voor te doen. Uw bankvertegenwoordiger gebruikt uw IBAN vanaf 1 december 2013 als nieuw bankrekeningnummer.

Voordelen
Wij tonen uw IBAN op uw betaalpas. Dit doen wij op de plaats waar voorheen uw 9-cijferige kaartnummer stond.
U ontvangt een betaalpas met IBAN gratis als u nu een nieuwe betaalpas aanvraagt.
Na 1 december betaalt u 17,50 EUR als u pas kwijt raakt of toe is aan een vervanging bij uw eigen bank.

Bestel nu gratis uw IBAN betaalpas.

Hoogachtend,

Over op IBAN

Voorbeeld van een phishing-mail

Geachte Klant,
Uit onze gegevens blijkt dat er recentelijk een derde abonnement op uw KPN rekening is gedetecteerd.
Nederland is het enige land in Europa waar je als consument een telefoonwinkel uit kan lopen met de nieuwste en duurste mobiele telefoon, zonder dat je de verkoopprijs betaalt.
Dat komt door de constructie die de telefoonmaatschappijen gebruiken: aan de afgifte van de mobiele telefoon zit een duur abonnement gekoppeld.
In de maandelijkse abonnementskosten zit de waarde van de mobiele telefoon verdisconteerd.
Deze constructie werkt fraude in de hand. Jaarlijks worden er honderden jongeren gedwongen of overgehaald om voor eigen rekening mobiele telefoonabonnementen af te sluiten.
Zij treden op als "katvanger" voor de daders. De mobiele telefoons die de slachtoffers "gratis" krijgen bij de aanvraag van de abonnementen moeten zij bij de daders inleveren.
Vervolgens blijven de slachtoffers zitten met torenhoge telefoonrekeningen.
Als de slachtoffers de telefoonrekeningen niet betalen, worden zij na enige tijd voor de kantonrechter gedaagd.
Daarom hebben wij besloten om de actieve toegang tot uw account te beperken.
Om deze vervelende omstandigheden te voorkomen en om uw nieuwe account te kunnen bevestigen hebben wij het volgende nodig:
- Een kopie van uw paspoort, ID of rijbewijs (voor en achterkant)
- Een kopie van uw betaalpas (voor en achterkant)

Om de kopieën te sturen moet u reageren op dit mail adres en dan de kopieën invoegen.
Na de bevestiging van uw gegevens zal er een automatische update plaatsvinden in ons systeem.

Met vriendelijke groet,
KPN Nederland

Robert Hoogwaard

KPN Nederland,
Afdeling fraude.

Voorbeeld van een phishing-mail

Van: Ziggo <ziggo@hus.nl>
Verzonden: zo 31-5-2015 20:26
Aan:
CC:
Onderwerp: Betaalherinnering

Ziggo

Klantnummer: 2110927-2

Geachte heer/mevrouw,

U ontvangt deze e-mail omdat uit onze administratie gebleken is dat het door u te betalen bedrag voor de geleverde Ziggo diensten niet automatisch van uw rekening kan worden geincasseerd. Wij verzoeken u vriendelijk het openstaande bedrag van **€ 79,69** alsnog aan ons over te maken. Door onderstaande stappen te volgen kunt u dit bedrag eenvoudig voldoen.

Vraag uw betaalgegevens op

Als u niet zelf betaalt, dan kunt u deze e-mail doorsturen naar de persoon of instantie die het openstaande bedrag dient te betalen.

Heeft u vragen?
Kijk op ziggo.nl/klantenservice voor meer informatie, wij staan hier dag en nacht voor u klaar. Of bel 0900-1884 (normaal tarief) of gratis 1200 met een vaste Ziggo lijn. Bereikbaar 7 dagen per week van 7.00 tot 23.00 uur.

Met vriendelijke groet,

Hans Blom
Directeur Consumentenmarkt

Ziggo Services B.V., mede handelend onder de naam Ziggo, statutair gevestigd te Utrecht. KvK 62393944. BTW nr NL 854800748B01. De betreffende Algemene Voorwaarden voor de geleverde diensten, gedeponeerd bij de KvK Amsterdam, zijn van toepassing.

Phishing-mail herkennen

- Afzender:
  kijk niet alleen naar de afzendernaam, maar ook naar het precieze afzendadres.

- Is dit een vaag adres, of een afgeleide versie van de echte naam van een bestaand bedrijf?
  Dan is het waarschijnlijk foute boel.

Phishing-mail herkennen

- Aanhef:
  Beste klant'. 'Geachte heer / mevrouw'. 'Dear Madam / Sir'.
  'Dear Google client'.

- Word je in zulke algemene bewoordingen aangesproken in plaats van met je naam?

- Of staat er helemaal geen aanhef? Pas dan op.

Phishing-mail herkennen

- Inhoud:
  In phishingmail staat vaak een verzoek om persoonsgegevens.
  Die moeten om de één of andere reden zogenaamd 'bijgewerkt' of 'geverifieerd' worden.

- Of je hebt iets gewonnen, en je hoeft alleen nog maar een paar privégegevens te verstrekken...

Phishing-mail herkennen

- In de mail word je aangemoedigd om op een link te klikken. Als het goed is gaat er nu al een alarmbel bij je af: zeer waarschijnlijk heb je met een phishingmail te maken.

- De e-mail bevat vaak taal- en schrijffouten. Het gaat om een slecht stuk vertaalde tekst

Phishing-mail herkennen

- Er wordt vaak gesuggereerd dat het account "geverifieerd" of te wel gecontroleerd moet worden. Dit controleren moet dan door ergens in te loggen met uw (bank)gegevens.

- Er wordt gedreigd dat als men niet inlogt er geen gebruik meer van uw bankrekening kan worden gemaakt of dat er een veiligheidsrisico is.

- Het afzender e-mailadres is niet altijd dat van uw bank. Vaak word wel een deel van de naam van uw bank genoemd.

Phishing-mail herkennen

- Taalgebruik:
  Kijk kritisch naar het taalgebruik.
  Phishingmail bevat vaak tekst die door een vertaalcomputer is gehaald.

- Dat levert vaak vreemde zinsconstructies en taalfouten op.
  Inconsequent hoofdlettergebruik en rare interpunctie zijn ook geen goed teken.

- E-mails van echte bedrijven en officiële instanties zijn doorgaans een stuk verzorgder geschreven.

Phishing-mail herkennen

- Weblinks:
  Klik nooit zomaar op een link in een e-mail waarover je twijfelt. Controleer eerst of het wel een legitieme link is.

  Dat doe je zo: ga met je muis op de link staan, zonder erop te klikken. Doorgaans verschijnt dan het adres in beeld waar de link daadwerkelijk naartoe gaat. Komt dit niet overeen met de tekst? Staat er geen officieel bedrijfsadres? Dan is het oppassen geblazen!

- Een andere manier is: klik erop met je rechtermuisknop, kopieer de koppeling en plak hem in een tekstbestand om te kunnen zien waar je precies heen gaat.

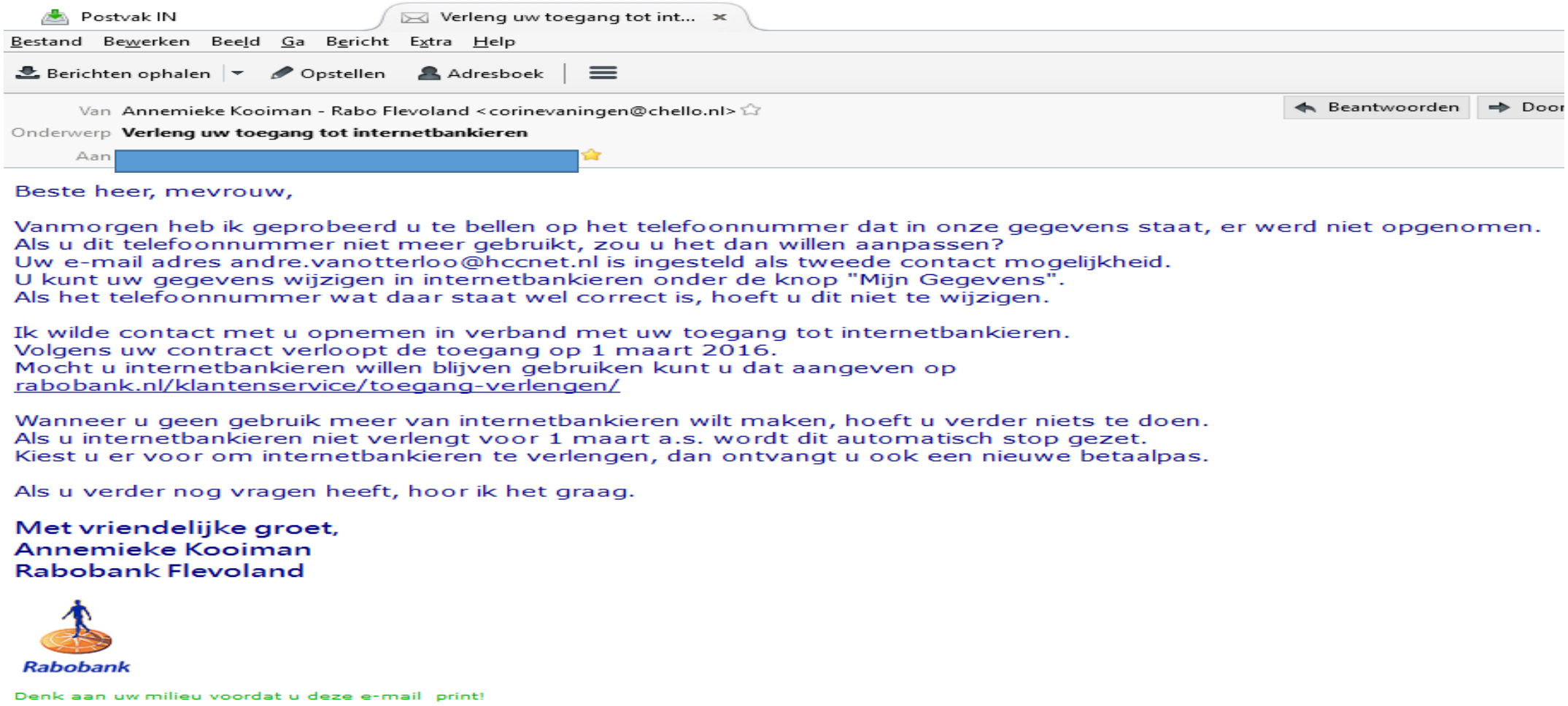
Praktijk voorbeeld weblink tonen in mail

http://td35.tripolis.com/public/r/y78qhZwrrWEWfjXOpcaMWQ/uI6Tfs8LREXJxD4lGIq7RA/rUnnkoHX6E1ufJeYzO8fAg

Praktijk voorbeeld weblink tonen in mail

http://pic.reshift.nl/4628/5f0992e9b0088787cc16d55b7ddeb639/55097

Praktijk voorbeeld weblink tonen in mail



Postvak IN | Verleng uw toegang tot int...

Bestand Bewerken Beeld Ga Bericht Extra Help

Berichten ophalen | Opstellen | Adresboek

Van Annemieke Kooiman - Rabo Flevoland <corinevaningen@chello.nl>

Beantwoorden | Door

Onderwerp **Verleng uw toegang tot internetbankieren**

Aan [redacted]

Beste heer, mevrouw,

Vanmorgen heb ik geprobeerd u te bellen op het telefoonnummer dat in onze gegevens staat, er werd niet opgenomen.
Als u dit telefoonnummer niet meer gebruikt, zou u het dan willen aanpassen?
Uw e-mail adres andre.vanotterloo@hccnet.nl is ingesteld als tweede contact mogelijkheid.
U kunt uw gegevens wijzigen in internetbankieren onder de knop "Mijn Gegevens".
Als het telefoonnummer wat daar staat wel correct is, hoeft u dit niet te wijzigen.

Ik wilde contact met u opnemen in verband met uw toegang tot internetbankieren.
Volgens uw contract verloopt de toegang op 1 maart 2016.
Mocht u internetbankieren willen blijven gebruiken kunt u dat aangeven op
rabobank.nl/klantenservice/toegang-verlengen/

Wanneer u geen gebruik meer van internetbankieren wilt maken, hoeft u verder niets te doen.
Als u internetbankieren niet verlengt voor 1 maart a.s. wordt dit automatisch stop gezet.
Kiest u er voor om internetbankieren te verlengen, dan ontvangt u ook een nieuwe betaalpas.

Als u verder nog vragen heeft, hoor ik het graag.

Met vriendelijke groet,
Annemieke Kooiman
Rabobank Flevoland

Rabobank

Denk aan uw milieu voordat u deze e-mail print!

http://bit.ly/1KktnHP

Bescherming

- Deze doelstelling is nog belangrijker geworden door het groeiende aantal nieuwe elektronische bedreigingen in de afgelopen jaren, zoals virussen, spam, spyware en phishing.

- Zorg sowieso dat je computer beschermd is door middel van up to date antivirussoftware.

- Betaalde versie !!!

Denk heel goed na voor je hapt !!!

[m.a.w. je privé gegevens uitdeelt]