Laat je niet phishen

Ontvang je een e-mail met daarin een link? Kijk uit, want het kan om phishing gaan. Aan de hand van vier actuele voorbeelden geven we tips hoe je phishing kunt herkennen.

1 De bankmail

De betaalpas of de scanner van je bank is aan vervanging toe. Je moet snel handelen, want anders wordt je rekening geblokkeerd of heb je extra kosten. Of de bank wil dat je je (opnieuw) identificeert. En snel ook. Je herkent deze phishingmails aan het gevoel van urgentie dat ze uitstralen ('binnen 2 werkdagen') en een link die leidt naar een andere website. Het verwarrende is dat banken dat soort mails soms ook sturen, met urgentie en een linkje erin. Dat maakt het nóg lastiger om echt van nep te onderscheiden.

Een voorbeeld van een echte mail van de bank Knab: 'Om de blokkade van je rekening op te heffen, wil ik je verzoeken om een kopie van je identiteitsdocument naar ons toe te sturen, zodat we aan de hand hiervan je gegevens kunnen verifiëren en indien nodig aanpassen.' Het simpelweg negeren van zo'n mail kan leiden tot een permanente rekeningblokkade.

Twijfel je of de mail echt is?

- Klik nergens op.
- Neem op een andere manier contact op met de bank. Dus krijg je een mail die je niet vertrouwt, bel de bank.
- Wacht op een herinnering. Als het echt is en de bank het belangrijk vindt, stuurt die herinneringen. Daarbij zal de urgentie in elke volgende mail toenemen. Bij phishing is dat anders. Daar spreekt uit de eerste mail al veel urgentie, door het woord 'herinnering' en/of hoofdlettergebruik.
- Stuur nooit je betaalpas op en vul nooit je pincode in.

ABN·AMRO

Geachte heer/mevrouw,

Uw huidige betaalpas voldoet niet meer aan de standaard eisen van de ABN AMRO en komt hierdoor binnenkort te vervallen.
We adviseren u om uw nieuwe betaalpas **binnen** 2 werkdagen op te vragen om een blokkade te voorkomen.

Is uw betaalpas al geblokkeerd?
Dan kunt u in de tussentijd op verschillende manieren betalen.
- Betalen met een creditcard
- Geld opnemen in een ABN AMRO vestiging
- Betalen met Apple en/of Google Pay

Kosten nieuwe betaalpas
Om uw nieuwe betaalpas geheel kosteloos te ontvangen heeft u uiterst **2 dagen** de tijd om de aanvraag in te dienen.
Dit kunt u doen door ___ te klikken.
Na de genoemde datum brengen we 24,95 euro in rekening per betaalpas.

Uw mening
Wat kunnen wij volgens u verbeteren? Geef ___ uw mening.

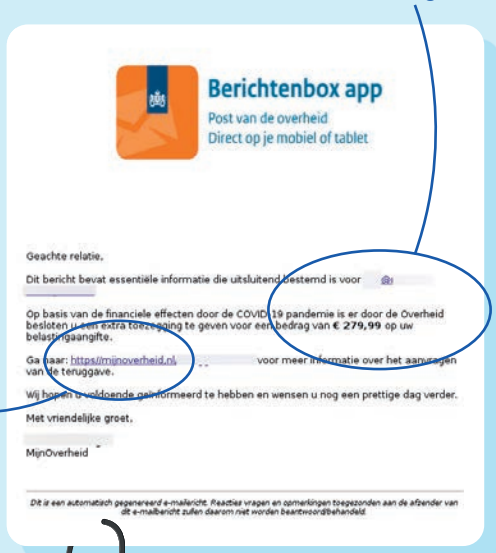
Heeft u nog vragen? Neem gerust contact met ons op.

Met vriendelijke groet,
Afdeling bankzaken
ABN AMRO

gevoel van urgentie

deze link leidt niet naar abnamro.nl maar een nagemaakte banksite

criminelen spelen in op actualiteit (corona) en financieel gewin



Berichtenbox app
Post van de overheid
Direct op je mobiel of tablet

Geachte relatie,

Dit bericht bevat essentiële informatie die uitsluitend bestemd is voor

Op basis van de financiele effecten door de COVID-19 pandemie is er door de Overheid besloten u een extra toezegging te geven voor een bedrag van **€ 279,99** op uw belastingaangifte.

Ga naar: https://mijnoverheid.nl voor meer informatie over het aanvragen van de teruggave.

Wij hopen u voldoende geinformeerd te hebben en wensen u nog een prettige dag verder.

Met vriendelijke groet,

MijnOverheid

Dit is een automatisch gegenereerd e-mailbericht. Reacties vragen en opmerkingen toegezonden aan de afzender van dit e-mailbericht zullen daarom niet worden beantwoord/behandeld.

deze link lijkt op de echte website, maar de punt tussen mijn en overheid ontbreekt

2 De overheidsmail

'U krijgt geld terug', 'U ontvangt een teruggave', 'Uw terugbetaling staat klaar'. Zulke mails en talloze variaties hierop komen zogenaamd van Mijn overheid. Doorgaans beloven de mails geld, zoals een belastingteruggave of een 'corona-compensatie'. Vaak spelen ze ook in op de actualiteit (zoals corona). Doel van de criminelen is daarbij om je te laten inloggen, zogenaamd bij je bank. In werkelijkheid log je in bij de crimineel. Net als bij bankmails geldt dat het om bonafide mails kan gaan. Alleen zet de overheid nooit linkjes in haar mails.

Twijfel je of de mail echt is?

- Klik nergens op.
- Ga naar mijn.overheid.nl of kijk in de Berichtenbox-app om te zien of je een bericht hebt.

TIPS

- Controleer altijd of het webadres achter de link leidt naar de echte (bank)site.
- Je ziet het échte webadres door er met de muis boven te zweven of (op de mobiel) door de link ingedrukt te houden.
- Klopt het internetadres niet (bv. abn-amro.nl.login.ru en niet abnamro.nl), verlaat de website dan meteen.
- Pas extra goed op bij mails afkomstig van banken, overheidsinstanties en bezorgdiensten.
- Bij twijfel: log zelf in op de website van de afzender, of bel de afzender
- Check of de mail bekend is bij Fraudehelpdesk.nl

3 De pakketmail

'Kennisgeving van uw pakje', 'Je pakket is onderweg', 'Levering van het opgeschorte pakket'. Als je online iets koopt, krijg je mails met informatie over de status, van zowel de verkoper als van de pakketdienst. Wie koopt er niet regelmatig iets online? Criminelen spelen daarop in met mails waarin ze zogenaamd een paar euro vragen voor 'verzendkosten' of 'douanekosten'. Je laat dan je bankgegevens achter op de nagemaakte banksite. Zie het kader bovenin pagina 17. In juni was er een variant in omloop (niet het voorbeeld onder) waar je via de echte banksite betaalde. Je betaalde dan geen €2 aan DHL, maar sloot ongemerkt een peperduur abonnement af via je creditcard. We vroegen creditcarduitgever ICS, die dit faciliteerde, om opheldering. 'Het is ons bekend dat er uit naam van DHL frauduleuze berichtgeving rondgaat. We kunnen echter bij voorbaat geen verkopende partijen blokkeren', aldus ICS. ICS erkende de misleiding, maar vindt dat klanten moeten opletten. 'Aangezien klanten zelf de gegevens invullen, goedkeuring geven voor de €2 en akkoord gaan met de algemene voorwaarden, kan ICS helaas weinig betekenen op voorhand.'

Twijfel je of de mail echt is?

- Klik nergens op.
- Download de app van de bewuste bezorgdienst. Vul het zendingsnummer, huisnummer en postcode in. Dan zie je of de zending werkelijk bestaat.
- Of neem contact op met de verkoper of bezorgdienst en vraag of de kosten kloppen.

deze link leidt naar nepvariant van de DHL-site

Toch je bankgegevens ingevuld?

Kom je er na het invullen van je bankgegevens achter dat je dat op een nagemaakte site deed, dan kan het kwaad al zijn geschied. De criminele websitemaker kan de webpagina zo instellen dat hij je gegevens ziet zodra je die intypt, dus nog voordat je op de verzendknop hebt gedrukt. Vermoed je dat je gegevens in verkeerde handen zijn gevallen?

1. Wijzig meteen je bankwachtwoorden.
2. Zet limieten voor betalen, overmaken, geldopnames op 0.
3. Betaalpassen blokkeren kan ook, maar bij loos alarm is dat onnodig onhandig. De bank moet nieuwe maken en het duurt even voor je ze in huis hebt.
4. Neem contact op met je bank en houd je rekening scherp in de gaten

Voorkomen is beter dan genezen. Doe je zelden grote betalingen, stel je limieten dan laag in. Helaas kunnen criminelen bij sommige banken (zoals ABN Amro) je limiet direct verhogen.

VERDER LEZEN?

In ons boek **De online fraude Survivalgids** geven we tips om je te wapenen tegen de trucs van internetcriminelen.

€23 (niet-leden €28,50)
Als e-book €16
(niet-leden €20)

consumentenbond.nl/fraude-survivalgids

4 Mails over winacties

'Bedankt voor uw deelname!' (AH), 'Bevestiging van jouw deelname!' (Bol): willekeurige mails aan mensen die nooit deelnamen. Maar ze hebben zogenaamd wel een leuke geldprijs gewonnen, als tegoed of aan boodschappen. Wie wil dat nu niet? Ook hier wordt urgentie ingezet: je moet snel zijn, anders loop je je geld mis.

Twijfel je of de mail echt is?

- Klik nergens op.
- Doe geen betaling.
- Neem contact op met de genoemde partij om erachter te komen of die daadwerkelijk een winactie organiseert. Zoek het adres op op de website van het bedrijf.

Achter de schermen bij de crimineel

Wat kan er nou misgaan als je een enkele cent betaalt als controle van je identiteit? Of €2 voor bijvoorbeeld douanekosten? Veel, zeker als je ter bevestiging van een betaling ook nog iets extra's moet doen. Zoals het invullen van een code die een apparaatje van de bank, een e-dentifier, genereert. Het probleem is dat criminelen de website van de bank exact namaken. Dan voer je je gegevens dus niet in op de banksite, maar op de site van de crimineel. Die zit klaar om je gegevens direct op de échte banksite in te typen. Vaak vraagt de bank om een extra controlestap bij het inloggen of om een betaling te bevestigen. De crimineel stuurt die vraag via de nepsite naar je door. Vul je de code in, dan kan de crimineel daarmee inloggen op de echte banksite en je rekening plunderen. Of het gaat zo: krijg je via de bankieren-app de vraag om het inloggen of een betaling te bevestigen? Grote kans dat je dan op de bevestigingsknop drukt. ■