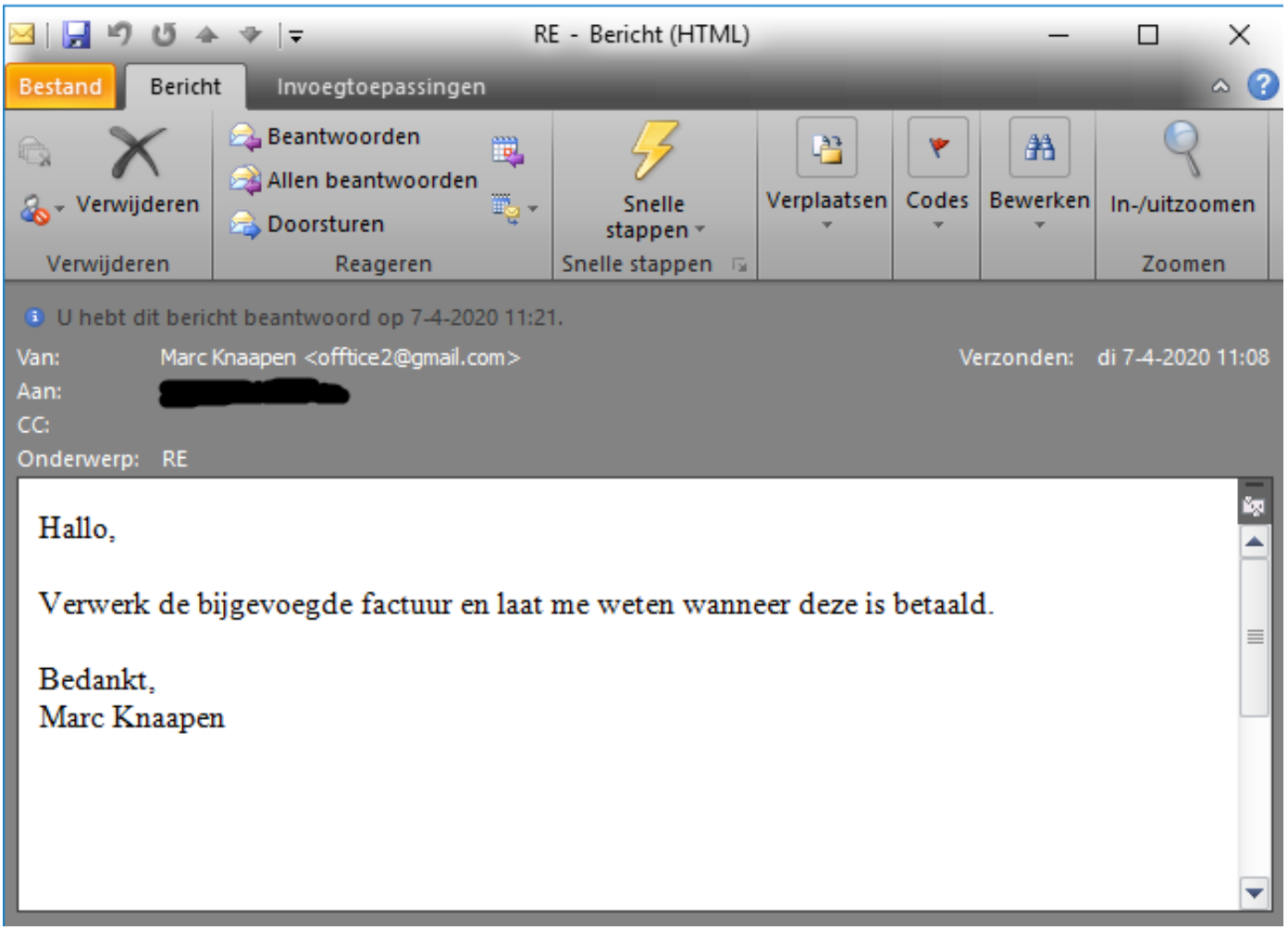
Phishing bij Gemeente Overbetuwe!

Iedereen heeft er wel eens van gehoord en veel collega's hebben het ook zelf ervaren: phishing (“vissen” naar), oftewel valse e-mails (of vals smsje/andere digitale berichten). Je wordt dan verleid om op een valse link of een valse bijlage te klikken. Er vinden veel pogingen plaats. Sommige zijn makkelijk te herkennen, anderen niet. Succesvolle phishing acties kunnen tot grote schade leiden. Ook de beruchte ransomware kan beginnen met phishing. Dat gebeurde zo eind 2019 bij Universiteit Maastricht.

Ook al helpt de techniek (zoals een spamfilter) in het voorkomen van veel problemen, toch blijf jij zelf de belangrijkste schakel in het omgaan met veel potentiële dreigingen. De meeste phishing pogingen worden afgevangen, maar sommige komen toch in jouw mailbox terecht. We willen je aan de hand van een praktijkvoorbeeld graag kort meenemen in hoe ook jij hiermee geconfronteerd kunt worden en wat je dan moet doen.

Een bijzondere vorm van phishing is 'spearphishing' (op een speciale groep of persoon gericht). Iemand doet zich dan bijvoorbeeld voor als een leidinggevende en probeert een nep-factuur te innen of vertrouwelijke informatie te ontfutselen. Ook bij gemeente Overbetuwe maken we dit helaas mee. Zie als voorbeeld het e-mailtje hieronder.



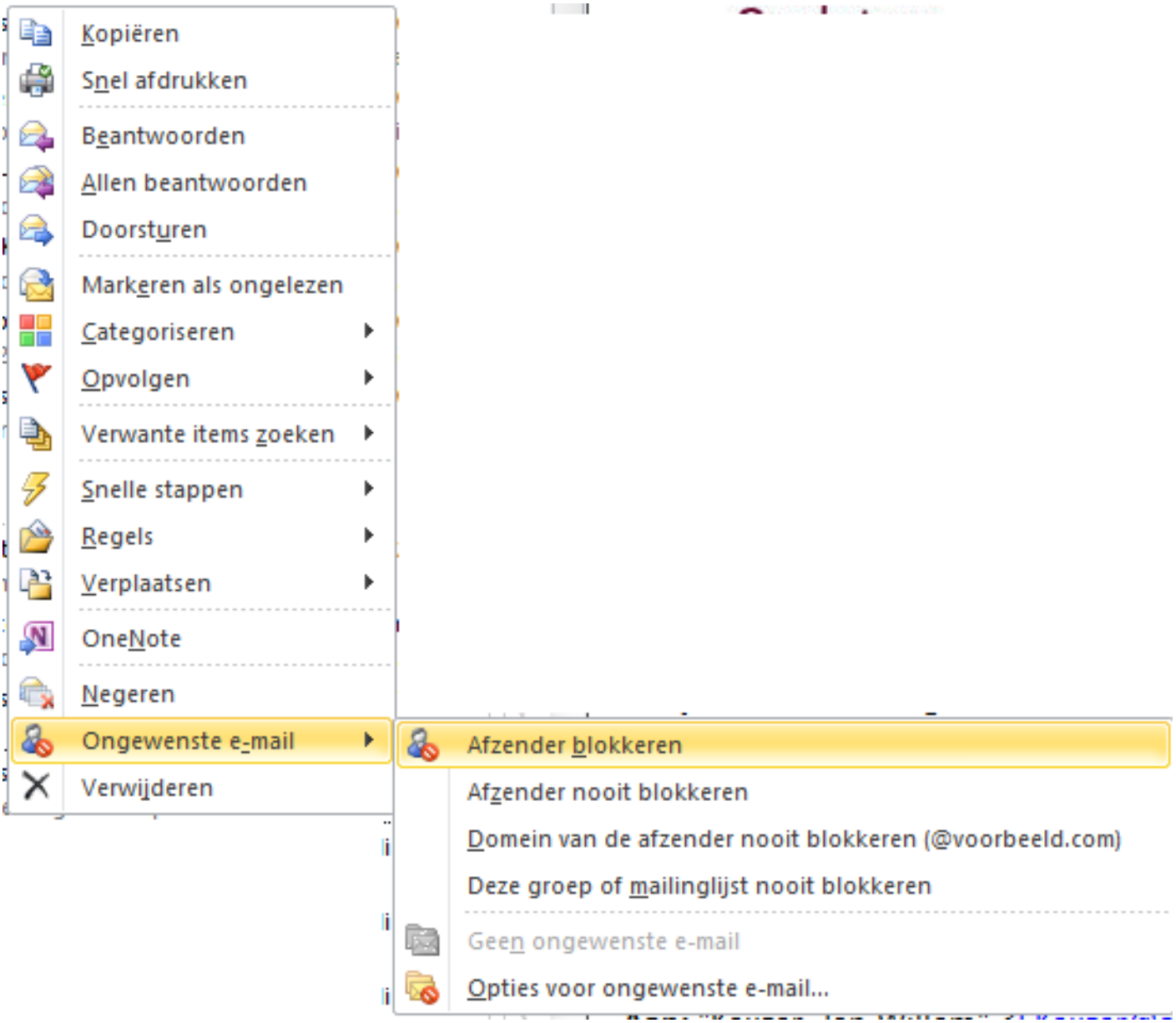
Dit voorbeeld is nog relatief opzichtig. Iemand heeft zich voorgedaan als ‘Marc Knaapen’, maar bij controle kan je meteen zien dat er gemaild is vanuit een vreemd e-mailadres. Foute boel dus, maar gelukkig is dit snel door de oplettende collega’s als nep herkend. Top!

Hoe kan ik phishing herkennen?

Phishing herkennen is makkelijker gezegd dan gedaan. Kijk in ieder geval goed naar het adres van de afzender. Wees altijd extra alert bij e-mail van iemand waarvan je geen e-mail verwacht. Maar ook e-mail van iemand waar je juist wél een e-mail van verwacht kan nep zijn. Want soms is daarin de domeinnaam in het adres anders dan je zou verwachten (zoals ook in het voorbeeld). De domeinnaam herken je aan wat achter het @-teken in het e-mailadres staat. Maar de domeinnaam kan ook weer juist verdacht veel op de legitieme domeinnaam lijken. Zo kan er in plaats van @Overbetuwe misschien wel @0verbetuwe staan. Door dit soort vernuftige ‘trucjes’ is phishing helaas nog vaak lonend. Kortom: wees alert!

Wat doe je als je een (mogelijk) phishing mailtje ontvangt?

Altijd: **melden bij de Servicedesk**! Ook bij twijfel of wanneer je al wel geklikt hebt.
Als je zeker weet dat de e-mail nep is kun je ook zelf de afzender blokkeren. Zie hieronder hoe je dat doet (rechts klikken op het bericht).



Wat doen we met de meldingen?

Doordat phishing incidenten door de Servicedesk worden geregistreerd kan analyse plaatsvinden. Hiermee kan de spamfilter eventueel worden aangepast en er meer phishing tegengehouden worden. Bij ernstige of nieuwe vormen van fraude pogingen door phishing, wordt dit bij officiële instanties gemeld en indien nodig wordt er aangifte bij de politie gedaan.
Dit alles doen we om jou en elkaar te helpen en ons ervoor te behoeden dat we slachtoffer worden van cybercrime.

Hoe verder?

Phishing is een fenomeen waar iedereen vroeg of laat mee te maken krijgt. Het kan zomaar gebeuren dat ook jij binnenkort een valse e-mail (of ander soort digitaal bericht) krijgt. Helaas zijn sommige valse e-mails tegenwoordig zo geraffineerd gemaakt dat ze lastig van echt te onderscheiden zijn. Dit maakt het moeilijk om ze door het spamfilter tegen te laten houden. Daarom zijn we mede op jouw oplettendheid aangewezen om onze systemen veilig te houden. Ben je toch in een phishing mail getrapt of heb je gegevens achter gelaten wat je niet vertrouwd? Ook dan is het belangrijk dit te melden bij de Servicedesk. Zo helpen we elkaar om onze werkomgeving veilig te houden!

Herken jij een phishing poging?
Doe hier de test !

Meer info?
Kijk op deze site van de Rijksoverheid.

Of stel je vraag in de groep Informatieveiligheid op NIVO.

Aangemaakt door:

Bernard Jansen
14 mei, 09:43

Laatst gewijzigd door:

Bernard Jansen
4 augustus, 16:32