Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Goede bulkmail lijkt niet op phishingmail

Factsheet FS-2015-05
versie 1.0 | 28 oktober 2015

Bulkmail is e-mail die bedoeld is voor ontvangst door een breed publiek. Bulkmail is voor velen lastig te onderscheiden van phishingmail. Het herkenbaar maken van authentieke e-mails zal het ontvangers gemakkelijker maken phishingmail te herkennen.

Doelgroep
Marketeers en marketingmanagers

Aan deze factsheet hebben bijgedragen:
- Belastingdienst
- DDMA
- Forum Standaardisatie
- Measuremail
- NLnet Labs
- SNS Bank N.V.
- UWV

Achtergrond

Bulkmail is e-mail die bedoeld is voor ontvangst door een breed publiek. De bekendste vorm van bulkmail is de nieuwsbrief. Bulkmail wordt vaak gebruikt voor marketingdoeleinden.

Phishing is een vorm van social engineering waarbij mensen verleid worden tot het overhandigen van gevoelige gegevens. De meestgebruikte phishingmethode is het versturen van vervalste e-mails die afkomstig lijken van betrouwbare organisaties. Veelal bevatten de e-mails een link naar een nagemaakte internetpagina, waarop een besmet bestand aangeboden wordt of de ontvanger gevraagd wordt persoonlijke gegevens in te vullen. Op deze manier verschaffen kwaadwillenden zich toegang, bijvoorbeeld tot bankrekeningen of bedrijfsnetwerken.

Het komt regelmatig voor dat bulkmails erg op phishingmail lijken. Voorbeelden hiervan zijn verzending via domeinen die niet van de organisatie zijn, links naar derde partijen en slechte spelling. Een gebruiker die moet bepalen of een e-mail authentiek is, heeft daarom maar weinig houvast. Ook de groeiende kwaliteit van phishingmails draagt hieraan bij. Het gevolg is dat ontvangers eerder op kwaadaardige links klikken of een kwaadaardig bestand openen. Het herkenbaar maken van authentieke e-mails zal het ontvangers gemakkelijker maken phishingmail te herkennen. Zij kunnen er dan immers van uitgaan dat alle e-mail die op phishingmail lijkt, ook phishingmail is.

Naast verzenders hebben ook mailserverbeheerders de taak om authentieke e-mail herkenbaar te maken. Daarover gaat het NCSC-factsheet ‘Bescherm domeinnamen tegen phishing’.

Let op deze zaken bij het opstellen van bulkmail:

1. **Domein.** Gebruik altijd een emailadres van uw eigen domein in de 'From'-header van het bericht. Zelfs als een externe partij e-mail verzendt kunnen zij een domein van uw organisatie gebruiken. Als het nodig is, kan een subdomein aangemaakt worden ('mail.example.nl' voor 'example.nl').
2. **Links.** Laat alle links in bulkmail verwijzen naar uw eigen verzenddomein en maak gebruik van redirects. Bijvoorbeeld, als u mailt van '@bulkmail.example.nl', dan verwijzen alle links naar 'bulkmail.example.nl'.
3. **NAW.** Neem een link op naar een webpagina met NAW-gegevens van uw organisatie.
4. **Spelling en grammatica.** Voorkom spel- en grammaticafouten. Deze verlagen de betrouwbaarheid van een e-mail sterk.
5. **Opmaak.** Gebruik een opmaak die overeenkomt met de huisstijl van uw organisatie en voorkom inconsistenties. Phishingmails zijn te herkennen aan stijlinconsistenties en gebreken zoals het ontbreken van een logo.
6. **Inhoud.** Vraag ontvangers nooit in een e-mail om gevoelige gegevens.
7. **Bijlagen.** Beperk het toevoegen van bijlagen. Bijlagen worden vaak door phishers gebruikt als methode om een computer te besmetten.
8. **HTML.** Zorg dat de e-mail opgemaakt is door middel van correcte en gevalideerde HTML en laad geen externe scipts in.
9. **Reden van ontvangst.** Geef duidelijk aan waarom de ontvanger het bericht ontvangt.
10. **Aanhef.** Gebruik de naam van de ontvanger in de aanhef van de e-mail als deze bekend is. Phishingmails beginnen veelal met generieke begroetingen ('Dear customer') of met de gebruikersnaam ('Dear gebruiker123').
11. **Informatie.** Geef op uw website aan hoe de ontvanger phishingmail zou kunnen herkennen en hoe hij melding kan maken van een verdachte e-mail. Zorg dat de klantenservice over genoeg kennis beschikt om een melding te beoordelen. Geef op uw website aan welke e-mails klanten kunnen verwachten en communiceer als phishingmails namens uw organisatie verstuurd worden.

Uitgave van **Nationaal Cyber Security Centrum**
Turfmarkt 147 | 2511 DP Den Haag
Postbus 117 | 2501 CC Den Haag
www.ncsc.nl | info@ncsc.nl | T 070-751 55 55
Publicatienr: FS-2015-05 1.0 | Aan deze informatie kunnen geen rechten worden ontleend.