Is het phishing? Check deze 5 tips

De meeste hackaanvallen starten met phishing. Wees aanvallers te snel af en leer phishing e-mail en -smsjes herkennen! Ontvang je een mailtje of sms-je, check dan:

1. **De afzender**
   Oplichters proberen de e-mailadressen vaak zo betrouwbaar mogelijk te laten lijken. Kijk naar het afzendadres, en let op de tekst na de @: komt dat overeen met de afzender? Check eventueel in een andere bron (internet) welk afzendadres de afzender gebruikt. **Let op!** Een goed uitziend e-mailadres geeft geen garanties, een beetje slimme oplichter kan elk e-mailadres als afzender gebruiken, zelfs je eigen e-mailadres. Dit heet spoofing.

2. **De link**
   Links in e-mails of smsjes kunnen leiden naar een website waar malware op je computer wordt geïnstalleerd. Beweeg met je muis over de link, dan komt de url tevoorschijn. Afhankelijk van het type url, kun je vaststellen of deze legitiem is (hiervoor dien je wel te weten wat de legitieme domeinnamen van de afzender zijn. Dat kun je doen door op internet te kijken of te bellen met de afzender. Stel vast wat de domeinnaam is en kijk goed naar de spelling: door één letter te veranderen, kan een kwaadaardige url griezelig veel op een legitieme url lijken. Meer informatie over het herkennen van urls vindt je op de volgende pagina

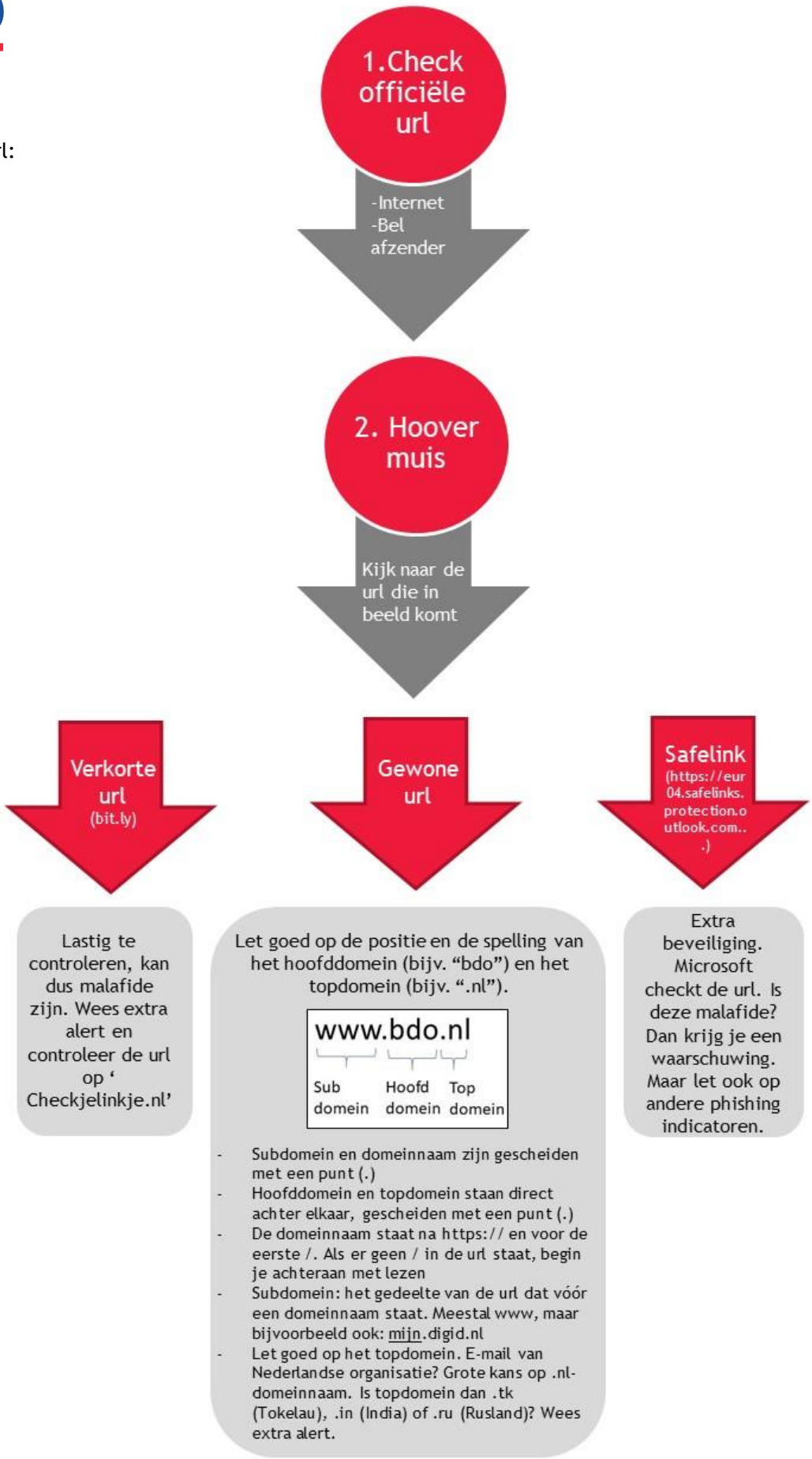
3. **De bijlagen**
   Bijlagen kunnen malware, zoals ransomware, bevatten. Open alleen bestanden die je 100% vertrouwt en waarvan je verwachtte ze toegestuurd te krijgen. Twijfel je? Let dan goed op het type bestand dat in de bijlage zit ingesloten. De volgende bestandstypen zijn extra verdacht:
   - .bat – Batch
   - .com - command file
   - .cpl - Control Panel
   - .docm - Microsoft Word met macro's
   - .exe - Windows Executable bestand
   - .jar - Java
   - .js - JavaScript
   - .pif - Programma Informatie bestand
   - .pptm - Microsoft PowerPoint met macro's
   - .ps1 - Windows PowerShell
   - .scr - Screensaver-bestand
   - .vbs - Visual Basic Script
   - .wsf - Windows Script File
   - .xlsm - Microsoft Excel met macro's
   - .zip – gecomprimeerd

4. **Het verzoek**
   In veel nepmails of -smsjes staat het verzoek om urgente actie, anders zouden er (hogere) kosten of sancties volgen. Vaak gebruikte onderwerpen zijn bankzaken, incasso's, boetes, facturen en gemiste pakketleveringen. Of men vraagt om te klikken om je persoonsgegevens 'te controleren'. Doe dit nooit, want een crimineel kan je dan naar een valse website leiden en je persoonlijke gegevens in handen krijgen. Je bank, verzekeringsmaatschappij en overheidsinstanties vragen nooit via een e-mail naar persoonsgegevens. Je kunt het bedrijf of de instantie natuurlijk wel even bellen om te controleren of ze de e-mail hebben verstuurd. Gebruik hiervoor nooit de contactgegevens in de e-mail, maar zoek deze zelf op.

5. **Het taalgebruik**
   Phishing e-mails staan tegenwoordig allang niet meer bol van de taal- en spelfouten. Ook de gebruikte logo's en foto's worden steeds professioneler. Kijk toch goed of je onregelmatigheden tegenkomt. Je kunt ook een eerdere mail van een bedrijf of instantie ernaast leggen ter vergelijking.

-

Check de url:



Hoe is het gesteld met de phishing awareness in jouw organisatie? Mocht je hulp of ondersteuning kunnen gebruiken, neem dan contact op met Marijke Stokkel van BDO: Marijke.Stokkel@bdo.nl