Wees Alert Voor Phishingmails!

Lees voor
Gepubliceerd op:
12
maart
2019

Doelgerichte phishingmails zijn een wereldwijd probleem. Niet enkel banken en grote bedrijven, maar ook steden en gemeenten zijn steeds vaker slachtoffer van dit soort digitale aanvallen.

Sinds lange tijd merken we een verhoogd aantal kwaadaardige berichten die verstuurd worden vanaf herkenbare email adressen. In deze mails vraagt de afzender je, al dan niet expliciet, een bijlage of link te openen. Als je deze link opent, krijgt de afzender toegang tot je account en je paswoord. Vervolgens kan de afzender uit jouw naam nieuwe phisingmails versturen naar je contactenlijst.

Wees alert!

- **Klik enkel op deze bijlagen of links indien je de afzender kent en/of je weet waarom het document/de url naar jou werd gezonden.** Als je twijfelt kan je best even telefonisch of via een andere methode dan e-mail navraag doen bij de afzender. Een antwoord op de oorspronkelijke mail met de vraag voor meer info kan immers ook door de phisher beantwoord worden.
- **Wat verwacht de afzender van jou?** Moet je iets ‘verifiëren’, ‘bevestigen’, ‘documenten bekijken/downloaden’, ‘Beoordelen’. Is het 'dringend', 'belangrijk' of 'vertrouwelijk'? Let dan zeker goed op. Deze woorden worden bewust gebruikt om je nieuwsgierig te maken.
- **Let op het taalgebruik. Taalfouten** of een **vreemde taal** kunnen wijzen op een verdacht bericht. Maar phishingmails worden steeds beter en beter. Dus ook mails zonder taalfouten kunnen verdacht zijn.
- Naar waar leidt de link waar je op moet klikken? **Zweef met je muis over de link, zonder erop te klikken. Zo kan je de domeinnaam controleren.** Is de domeinnaam, het 'woord' voor .be, .com, .eu, .org, … en voor de allereerste slash “/”, ook echt de naam van de organisatie? (Vb: www.mechelen.be is betrouwbaar, www.mechelen.infosite.be is verdacht)
- Twijfel je over de echtheid van een bericht, dan kan je het steeds doorsturen naar verdacht@safeonweb.be

Heb je toch geklikt op een phishingmail?

- Verander onmiddellijk zelf je paswoord.
- Verander al je paswoorden die hetzelfde zijn als die van je account.
- Verwittig het contact van wie je de phisingmail ontving om hen te laten weten dat hun account gehackt werd.
- Verwittig ook je eigen contacten dat ze phisingmails vanuit jouw account kunnen ontvangen.

Zit je met verdere vragen over online veiligheid, dan kan je steeds terecht bij www.safeonweb.be

Stadsbestuur Mechelen
Huis van de Mechelaar
Reuzenstraat 1, 2800 Mechelen
T 0800 20 800, onthaal@mechelen.be

Correspondentieadres
Grote Markt 21, 2800 Mechelen
stadsbestuur@mechelen.be