DUTCHWYSE®

CREATIVE ICT SOLUTIONS

FIRST RESPONSE GUIDE

Voor Phishing mails

Een handeiding van **DUTCHWYSE**

HELP!! Ik heb een phishing-mail ontvangen!

Je hebt een email gekregen met een link of bijlage die niet legitiem bleek te zijn. Heb je de email verwijderd, is er meestal niets aan de hand. Heb je een bijlage geopend, een link gevolgd of zelfs je wachtwoord ingevoerd? Dan is er onmiddellijk actie nodig!

1 : Ik heb de mail meteen verwijderd.

Goed! Als je niets hebt aangeklikt of geopend kan je de mail verwijderen.

- Laat je manager en collega's weten dat er een phishing-mail in omloop is.
- Wil je dat wij de mail onderzoeken? Stuur deze dan door aan **servicedesk@dutchwyse.nl.**

2 : Ik heb de mail gelezen.

Niets aan de hand. Zo lang je geen links hebt aangeklikt of bijlages hebt geopend kan je de mail verwijderen.

- Laat je manager en collega's weten dat er een phishing-mail in omloop is
- Wil je dat wij de mail onderzoeken? Stuur deze dan door aan **servicedesk@dutchwyse.nl**

3 : Ik heb een link aangeklikt.

Meestal is het aanklikken van een web-link onvoldoende om direct schade toe te doen.

- Sluit je browser(s) onmiddellijk.
- Laat je manager en collega's weten dat er een phishing-mail in omloop is.
- Neem contact op met Dutchwyse op 088-506-4500.

4 : Ik heb de bijlage geopend.

- Zorg ervoor dat je computer meteen van het netwerk gaat. Verbreek de WiFi en/of netwerkverbinding en sluit de computer af.
- Laat je manager en collega's weten dat er een phishing-mail in omloop is.
- Neem contact op met Dutchwyse op 088-506-4500.

5 : Ik heb een link aangeklikt en een programma gedownload.

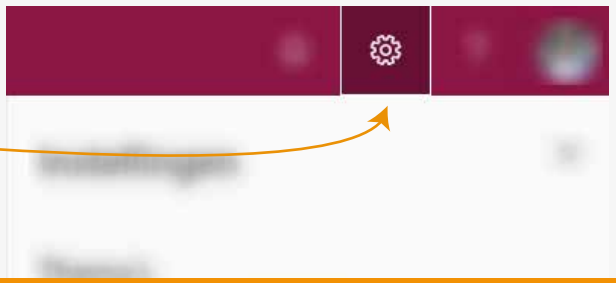
- Zorg ervoor dat je computer meteen van het netwerk gaat. Verbreek de WiFi en/of netwerkverbinding en sluit de computer af.
- Laat je manager en collega's weten dat er een phishing-mail in omloop is.
- Neem contact op met Dutchwyse op 088-506-4500.

6 : Ik heb mijn Microsoft 365 log-in gegevens ergens ingevoerd.

- Verander onmiddellijk je wachtwoord op **https://portal.office.com**. (Zie hieronder)
- Neem contact op met Dutchwyse op 088-506-4500.
- Vraag een collega om namens jou naar iedereen een mail te sturen met de waarschuwing om e-mails van jou te negeren.
- Informeer je manager of vraag een collega dit te doen.

Je wachtwoord veranderen bij Microsoft 365

- Open een browser en ga naar **https://portal.office.com**
- Log-in met je gebruikersnaam en wachtwoord (indien nodig)
- Klik op het tandwieltje rechts boven
- Selecteer "Wachtwoord wijzigen"
- Voer je oude en nieuwe wachtwoord in en zorg ervoor dat je nieuwe wacthwoord niet lijkt op je oude wachtwoord!!



Ons stappenplan.

Bij elke melding hanteren we een stappenplan om verdere verspreiding van de mail te voorkomen en de downtime van de medewerker zo veel mogelijk te beperken. In sommigge gevallen mag de computer niet meer op het netwerk worden aangesloten en moet deze voor controle naar onze technische dienst.

Bij onderzoek van een phishing-mail (1&2)

- Bij onderzoek naar een phishing-mail vragen we je deze door te sturen.
- Aan de hand van de afzender en het onderwerp gaan we door middel van een zogenaamde mail-trace kijken of en hoe de email is verspreid binnen het bedrijf.
- We controleren de aard van de mail en of de eventuele bijlagen veilig zijn.

Bij het aanklikken van een link (3)

- We loggen remote in op het systeem en kijken samen of er modificaties aan de browser gedaan zijn.
- We wissen de cookies en browser-geschiedenis.
- We voeren een handmatige virusscan uit.

Bij een geopende bijlage of gedownload programma (4 & 5)

Deze computer mag niet meer op het netwerk worden aangesloten.

- We maken een afspraak om het systeem te laten retourneren naar de technische dienst waar we in een offline omgeving een uitgebreide virus scan uitvoeren en indien nodig het systeem opnieuw installeren.

Bij het verkrijgen van Office login gegevens (6)

- Als de gebruiker dit (nog) niet zelf gedaan heeft maken wij onmiddellijk een nieuw wachtwoord aan.
- Aan de hand van de afzender en het onderwerp gaan we door middel van een zogenaamde mail-trace kijken hoe de email is verspreid binnen het bedrijf en aan welke contactpersonen (intern & extern) de mail is doorgestuurd.
- De resultaten worden verstuurd naar de gebruiker zodat hij/zij weet wie email van hem/haar heeft ontvangen en de contactpersonen op de hoogte kan brengen.
- We controleren of er regels zijn aangemaakt in de mailbox van de gebruiker en verwijderen deze.
- We controleren wanneer en vanaf waar* er is ingelogd op het account van de gebruiker.
- We deblokkeren de gebruiker indien deze bij Microsoft is geblokkeerd vanwege het versturen van spam.
- We verzenden een rapportage naar de manager.

* Op basis van IP adres. Dit is doorgaans niet nauwkeurig en kan door een aanvaller vervalst worden.

Melding van een datalek is verplicht!:

Wanneer een aanvaller toegang heeft tot het Office365 account van een gebruiker, heeft deze ook toegang tot Sharepoint/OneDrive en alle bestanden waartoe de gebruiker toegang heeft. Dit is een datalek waarbij een bedrijf **verplicht** is deze te melden.
Zie https://datalekken.autoriteitpersoonsgegevens.nl

Disclaimer:

De wijze waarop mails worden opgesteld en verstuurd en de wijze waarop aanvallers te werk gaan veranderd dagelijks. Aan het advies in deze handleiding kunnen dan ook geen rechten worden ontleend. Ook zijn wij niet aansprakelijk voor data-verlies of schade, op welke manier dan ook, die voortvloeit uit het volgen van hetgeen omgeschreven in deze handleiding.

Kijk op de website voor het voorkomen van ongeoorloofde toegang en meer informatie en tips over digitale veiligheid!