Phishing Campagne

Januari 2024

DIGITAAL VLAANDEREN

Vlaamse overheid

WAT ?

Wat houdt deze ‘IT Security’ phishing mail juist in?

Uitvoeren van phishingsimulaties naar medewerkers van VO-entiteiten met als doel:

- Phishing kunnen herkennen;
- URL’s leren lezen;
- Meldingsprocedure kennen,

Het gewenste resultaat:

- Alertheid en vaardigheden van medewerkers verhogen;
- Beveiligingsincidenten vermijden;
- Inzicht in gedragingen van medewerkers;
- Opleiding- en awareness behoeften in kaart brengen.

WAT ?

Hoe ziet deze “IT Security” phishing mail eruit?

- Datum: 10-12/01/2024
- Afzender: “IT Security” – e-mail: itsecurity@communicatie.vlaanderen
- Onderwerp: [ACTIE VEREIST] – Verdachte activiteit op je account gedetecteerd
- Body:

  Beste medewerker,

  We hebben onlangs verdachte activiteit gedetecteerd op jouw account en willen ervoor zorgen dat je account veilig blijft. Er is een poging tot ongeautoriseerde toegang geweest vanaf een onbekend apparaat.

  Om je account te beveiligen, vragen we je om onmiddellijk activiteit te bevestigen. Indien er binnen 24 uur geen actie wordt ondernomen, zal je account geblokkeerd worden. Klik op de onderstaande link om naar de beveiligingspagina te gaan:

  [LINK]

  Dank je wel voor je medewerking.

  Met vriendelijke groeten,

  IT Security

WAT ?

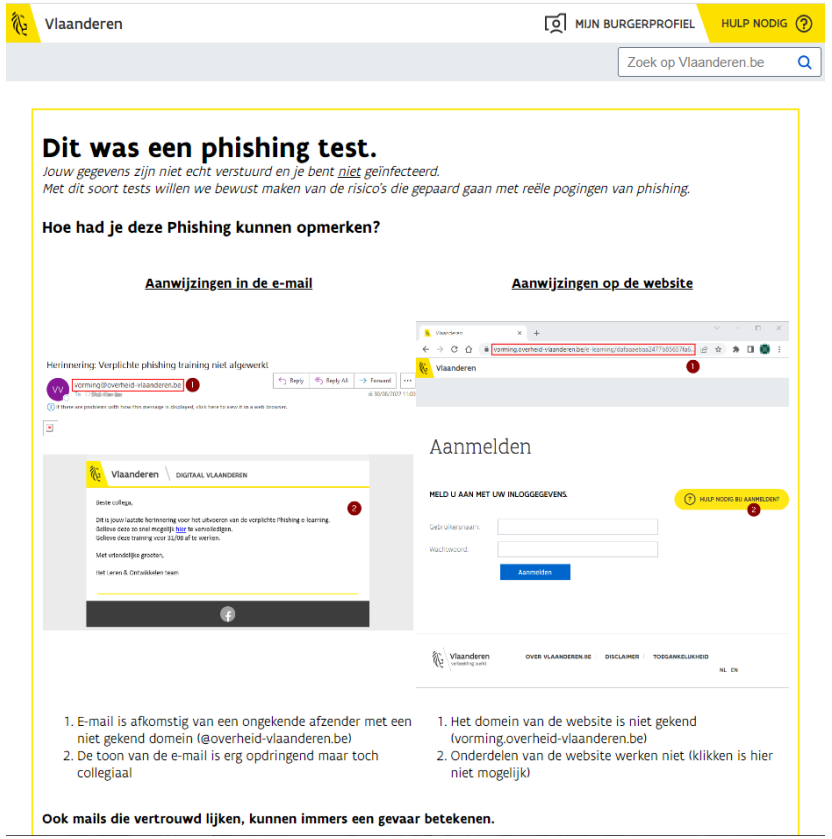
Hoe ziet de phishing website er juist uit?

URL: https://authenticatie.communicatie.vlaanderen/activiteit/*

Opzet: Gebaseerd op Microsoft inlogpagina om login-gegevens te verzamelen

Lay-out: In opmaak

Learningpagina (na aanmelden):



Opmerking!

Er worden niet effectief login-gegevens bijgehouden of doorgestuurd, deze invoervelden worden leeggemaakt voor de data naar de phishing server gestuurd wordt.

WAT ?

Proces

VOORBEREIDING

Draft scenario

- ✓ Digitaal Vlaanderen stuurt 2 weken op voorhand voorstel van scenario door
- ✓ Entiteit bevestigt deelname aan phishing campagne

Targetlijsten

- ✓ Opladen targetlijst →zie volgende slide

Whitelisting

- ✓ Entiteit brengt whitelisting in orde (bij gebruik van eigen IT infrastructuur) → zie volgende slide

Test

- ✓ Deloitte stuurt enkele dagen op voorhand een test naar de contactpersonen
- ✓ Entiteit reviewt binnen 1 werkdag

START CAMPAGNE

Aankondigingsmail

- ✓ Deloitte stuurt 2 werkdagen op voorhand een bericht naar de contactpersonen om start van phishing campagne aan te kondigen
- ✓ Dit geeft de contactpersoon de mogelijkheid om nog een beperkt aantal personen in te lichten (Bv.. senior management, communicatieteam, helpdesk, …)

Start phishing campagne

- ✓ Deloitte voert test uit binnen afgesproken timing

RAPPORTERING

Dashboard

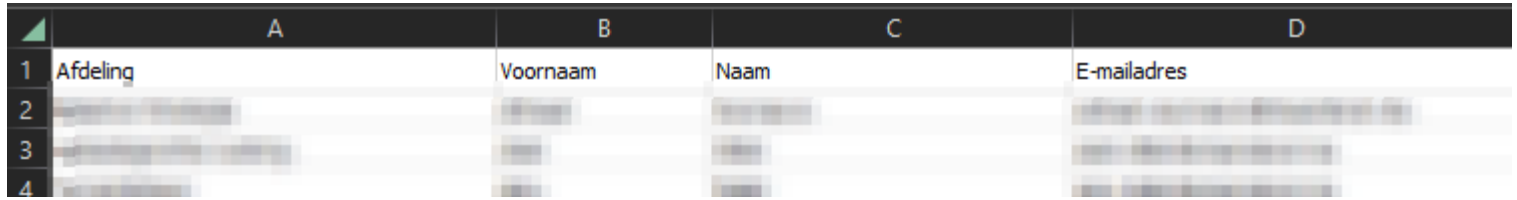
- ✓ Resultaten worden opgeladen in dashboard
- ✓ Resultaten en lessons learned worden gedeeld met de contactpersonen van de deelnemende entiteiten (= geanonimiseerde resultaten van de entiteit + gemiddelde van de deelnemende entiteiten)

WAT ?

Targetlijst

Gelieve de targetlijsten te uploaden in Excel-formaat, en indien toepassing, te voorzien van de gewenste onderverdeling (bv. functie, categorie, afdeling, etc.)

SharePoint-site: phishing-as-a-service (map: entiteit → Campagne 2024-01)



	A	B	C	D
1	Afdeling	Voornaam	Naam	E-mailadres
2				
3				
4				

Het is belangrijk om op te merken dat elke onderverdeling minimaal 5 gebruikers moet bevatten om de anonimiteit van individuen te waarborgen. Daarnaast bestaat de mogelijkheid om het aantal gebruikers te verminderen mits de campagne meer dan 15.000 doelwitten bevat.

WAT ?

Whitelisting

Voor de entiteiten die hun IT infrastructuur autonoom beheren, vragen we de whitelisting door te voeren op de volgende security controles/oplossingen:

- E-mail/domain van de afzender moet toegelaten worden op de mailserver (O365, Exchange Server, etc.): communicatie.vlaanderen
- Safe links voor de URL moeten uitgeschakeld worden (door dit toe te passen worden valse clicks vermeden): https://authenticatie.communicatie.vlaanderen/activiteit/*
- Netwerk trafiek naar het domein moet toegelaten worden op de netwerk oplossingen (Proxy, Firewalls, etc.).

Bij technische of praktische vragen, neem contact op via dit e-mailadres

Opmerking: Voorafgaand aan de lancering van de phishing campagne stuurt Deloitte eerst een test mail uit. Hiermee kunnen de deelnemende VO-entiteiten nakijken of:

- *De e-mail correct werd ontvangen;*
- *De webpagina probleemloos geopend kan worden;*
- *Ze de learningpagina kunnen raadplegen.*

Het is de bedoeling dat de deelnemers aan Deloitte bevestigen dat ze de test mail succesvol hebben ontvangen.

Contact

Nog Vragen?

U kan bij ons terecht via deze e-mail