Phishing Campagne

November 2023

DIGITAAL VLAANDEREN

Vlaamse overheid

WAT ?

Wat houdt deze 'Black Friday' 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 'Black Friday' phishing mail eruit?

Datum: 22-27/11/2023

Afzender: “Cadeaubon” – e-mail: “no-reply@cadeaubon-vlaanderen.be”

Subject: “BEDANKT! Black Friday Voucher”

Body:

Beste medewerkers,

We naderen één van de meest opwindende winkeldagen van het jaar: Black Friday! Om onze waardering te tonen voor jullie harde werk en toewijding gedurende het jaar, willen we jullie een speciale traktatie aanbieden.

Elke medewerker binnen de Vlaamse Overheid heeft recht op een exclusieve Black Friday-voucher ter waarde van €50! Dit is onze manier om je te bedanken voor je inzet. Deze aanbieding is slechts 2 dagen geldig dus zorg ervoor dat je de link tijdig gebruikt om je korting te activeren.

Om je voucher te ontvangen, klik eenvoudigweg op de onderstaande link: [LINK]

Geniet van je Black Friday shopping en veel plezier!

Met vriendelijke groeten,

Cadeaubon-Vlaanderen

WAT ?

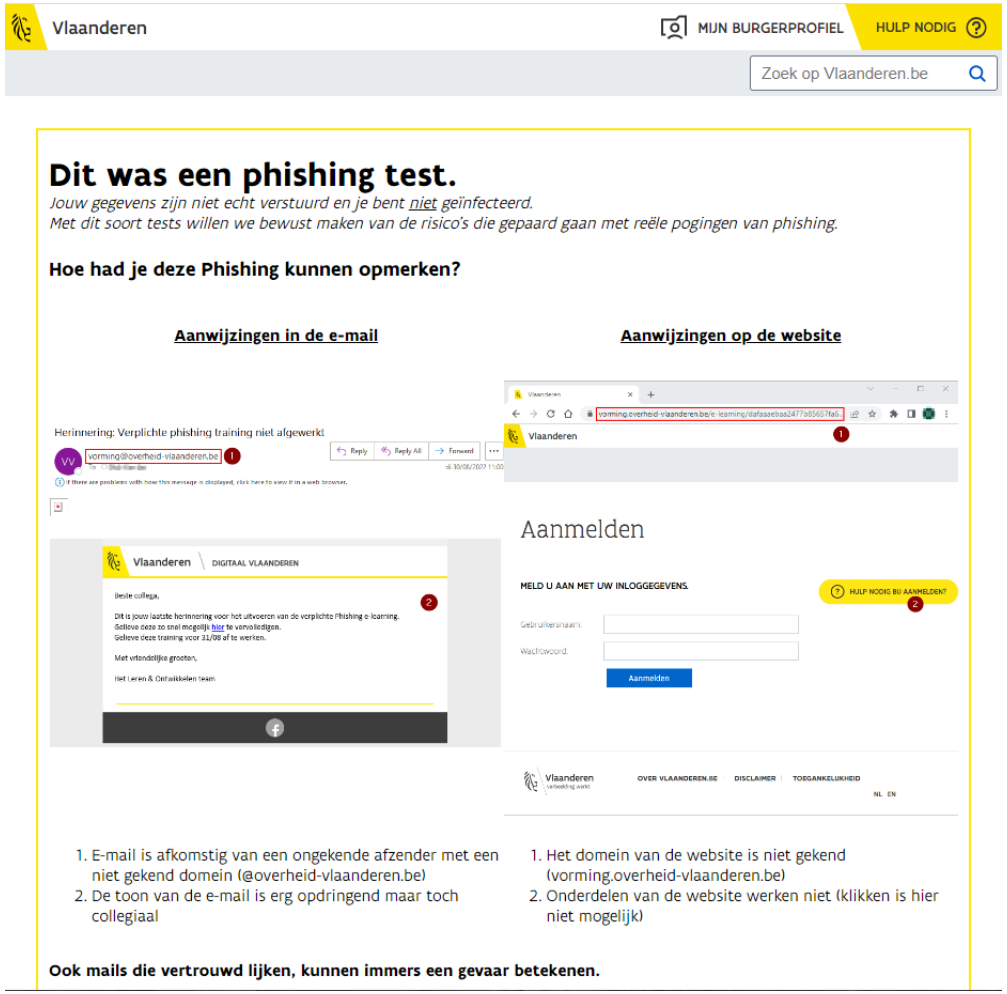
Hoe ziet de phishing website er juist uit?

URL: https://cadeaubon-vlaanderen/black-friday/voucher/eaz5e4c1qd84

Opzet: Op 'maat gemaakt geschenken portaal' om persoonsgegevens te verzamelen (adres gegevens, etc.)

Lay-out: in opmaak

Learningpagina (na aanmelden):



OPMERKING

Er worden geen persoonsgegevens bijgehouden of doorgestuurd, deze invoervelden worden leeggemaakt voor de data naar de phishing server gestuurd wordt.

HOE ?

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 (BvB. senior management, communicatieteam, helpdesk, …)

Start phishing campagne

- ✓ Deloitte voert test uit binnen afgesproken timing

RAPPORTERING

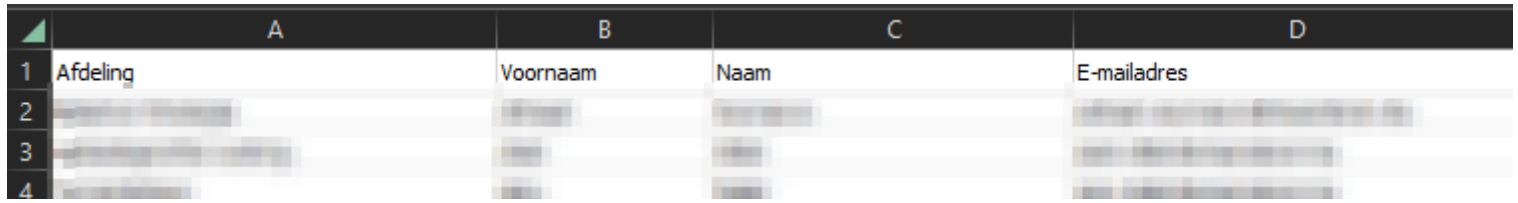
Dashboard

- ✓ 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)

HOE ?

Targetlijst

Gelieve de targetlijsten te uploaden in Excel-formaat, en indien van toepassing, te voorzien van de gewenste onderverdeling (bv. functie, categorie, afdeling, etc.);
Sharepoint: phishing-as-a-service (map: Entiteit → Campagne 8 – 20-11-2023)



	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.

HOE ?

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.)
- Safe links voor de URL moeten uitgeschakeld worden (door dit toe te passen worden valse clicks vermeden)
- 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 V0-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

Classificatie: Klasse 2