Phishing as a Service

AANBOD

Uitvoeren van phishingsimulaties naar medewerkers met als doel :

- Phishing, smishing en vishing (leren) herkennen
- URL leren lezen
- Meldingsprocedure kennen

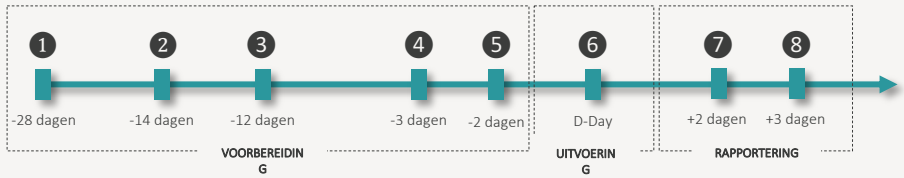
Beoogd resultaat:

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

WAT

- 9 campagnes per jaar (7 phishing / 1 smishing / 1 vishing)
- Deelname aan iedere campagne is vrijblijvend
- Entiteit bepaalt zelf de doelgroep
- Rapportering (per entiteit)
  - Resultaten campagne
  - Evolutie
  - Benchmarking tov andere entiteiten

HOE GAAN WE TE WERK



VOORBEREIDING

1. Intekenen kan tot 4 weken voor de start van de campagne.
2. Digitaal Vlaanderen stuurt 2 weken op voorhand het draft scenario door.
3. Afnemer geeft feedback op draft scenario.
   Indien gewenst kan afnemer nog afzien om deel te nemen aan de campagne.
4. Opsturen van testmail + verwerken finale feedback.
   Afnemer geeft e-mail, voornaam, GSM-nummer (afhankelijk van scenario) van doelgroep door.
5. Contactpersonen entiteit ontvangt aankondigingsmail
   = beperkt aantal personen ('need to know')

UITVOERING

6. Uitvoering scenario binnen de afgesproken timing.
   Digitaal Vlaanderen informeert contactpersoon tijdens het verloop van de campagne.

RAPPORTERING

7. Eenmaal campagne afgerond ontvangt contactpersoon rapport met de resultaten. (basis = anoniem // optioneel detail per persoon)
8. Digitaal Vlaanderen geeft een aantal aanbevelingen door aan contactpersoon (lessons learned)

DOELGROEP

Entiteiten Vlaamse overheid
Lokale besturen

KOST

Gratis

DIENSTVERLENER

Digitaal Vlaanderen
i.s.m. Deloitte

PROCEDURE

Mail naar
security@vlaanderen.be

DIGITAAL VLAANDEREN
Vlaamse overheid