KDV De Hoeksteen
Beerststraat 36 | 8600 Diksmuide - Vladslo | Tel 051 43 29 00 |
algdirectie@de-hoeksteen.be |

Informatiedocument phishing en smishing

1. Algemene info

Phishing is een vorm van internetfraude waarbij een cybercrimineel probeert gevoelige info (bvb. een gebruikersnaam, wachtwoord, …) van jou probeert te ontrafelen om later te misbruiken. Dit gebeurt vaak via valse e-mails, websites of berichten, maar de cybercrimineel kan je ook opbellen.

SMS wordt ook vaker gebruikt om berichten te versturen met valse links met de bedoeling om mensen op te lichten. Deze vorm heet: *smishing* of ook *SMS-phishing*.

Vaak maken cybercriminelen misbruik van iets waar je in gelooft of van iemand die je vertrouwt. Valse berichten lijken daarom vaak afkomstig van betrouwbare personen of instanties, zoals een collega, overheid, een bank of een koerierdienst. Ze spelen vaak in op je emoties en misbruiken de actualiteit om je nieuwsgierig te maken.

2. Tips om een verdacht bericht te herkennen

- Is het onverwacht?
  Krijg je zonder reden een bericht van deze afzender? Is het te mooi om waar te zijn? Je nam bijvoorbeeld niet deel aan een wedstrijd, je kocht niets, …

- Is het dringend?
  Hou je hoofd koel wanneer het bericht dwingend of dringend aanvoelt. Je kreeg bijvoorbeeld een eerste aanmaning tot betaling? Een collega die in nood zit?

- Ken je de afzender?
  Controleer het emailadres, ook op spellingsfouten. Fraudeurs gebruiken vaak een emailadres die goed lijkt op het officiële adres. Maar let op, ook een legitiem e-mailadres is geen garantie!

- Vind je de vraag vreemd?
  Het vragen van bepaalde gegevens zoals wachtwoord, bankgegevens of andere persoonlijke en gevoelige gegevens worden niet via mail gevraagd.

- Naar waar leidt de link waar je moet op klikken?
  Klik nooit zomaar op een URL in een verdacht bericht! Een mail van een persoon waar je geen mail van verwachtte met een link? Of twijfel je of de link betrouwbaar is? Contacteer dan de IT dienst.
  Toch (per ongeluk) geklikt? Vul geen velden in en breek elke interactie af. Contacteer dan zo snel mogelijk de IT dienst.

- Word je persoonlijk aangesproken?
  Berichten met algemene en vage aanspreektitels, of je e-mailadres als aanspreking, die wantrouw je beter. Ook taalfouten of een vreemde taal kunnen wijzen op een verdacht bericht.

- Probeert iemand je bang of nieuwsgierig te maken?

Laat je niet vangen! Iedereen is wel nieuwsgierig bij een bericht met een link als 'Kijk wat ik over jou las …' of 'Ben jij dit op deze foto?'. Cybercriminelen spelen vaak in op de actualiteit en weten welke thema's ons interesseren.

3. Wat indien een vals bericht?

Vermoedelijke valse berichten meld je best via e-mail aan de IT dienst of DPO. Daarna verwijder je ze onmiddellijk.

Toch op geklikt of gegevens doorgegeven? Neem dan zo snel mogelijk contact op met de IT dienst EN DPO. Sluit onmiddellijk uw emailaccount af en wacht met software te openen tot de IT dienst uw computer heeft gecontroleerd.

Contactgegevens bij problemen:
- hannes.rosseel@de-hoeksteen.be (tel 0484/ 02 64 41)
- DPO@de-hoeksteen.be (tel 0479/ 35 55 56)