Eerste hulp bij Phishing

Wat is phishing?

Phishing is een vorm van computercriminaliteit waarbij de oplichter nietsvermoedende personen probeert te misleiden. Computercriminelen proberen daarbij om misbruik te maken van de goedgelovigheid van hun doelwit.

Hoe werkt het?

- Ontfutselen van vertrouwelijke informatie.

Oplichters sturen vandaag meestal een e-mail met een link naar een vervalste website. Via die website proberen ze dan op listige wijze aan persoonlijke(bank) gegevens te komen.

- Malware.

Computercriminelen versturen e-mails met bijlagen waarin schadelijke software verborgen zit of met hyperlinks die naar een website verwijzen die geïnfecteerd is met schadelijke software.
De schadelijke software kan dan aan de oplichter wachtwoorden doorgeven die de gebruiker hanteert. Via deze wachtwoorden krijgt men toegang tot persoonlijke of vertrouwelijke informatie.
Malware kan zich via het netwerk verspreiden en zo via het netwerk enorm veel schade aanrichten.

- Cryptoware.

Sommige kwaadaardige software kan de gegevens die op de computer staan blokkeren; De oplichters eisen vervolgens geld van het slachtoffer om de blokkade op te heffen. Niets garandeert dat na betaling de blokkade wordt gedeblokkeerd.
Net als bij malware kan ook cryptoware zich verder via het computernetwerk verspreiden en enorme schade aanrichten.

Phishing herkennen

Hoe phishing herkennen?

- Men kan phishing berichten vaak herkennen aan de onpersoonlijke toon, taal -en stijlfouten.
- E-mail is niet aan een specifieke geadresseerde gericht, maar begint met de aanspreking "*Geachte klant*".
  Criminelen gaan echter steeds professioneler te werk en hanteren meer en meer persoonlijke aansprekingen.
- De oplichter tracht de ontvangers van een phishing-mail te verleiden om een bijlage te openen of op een meegestuurde hyperlink te klikken.
  Deze hyperlink brengt je naar een vervalste website waar om je persoonlijke gegevens gevraagd wordt.
- Phishing berichten proberen vaak om een gevoel van angst of dringendheid op te wekken.
  Dergelijke berichten verwijzen vb. naar een veiligheidsprobleem of wedstrijd die bijna afloopt.
  Er wordt aangedrongen om snel actie te ondernemen.
  Soms wordt er gedreigd met kwalijke gevolgen als geen gehoor wordt gegeven aan de oproep.

Mogelijke phishing schade

- Vertrouwelijke informatie uit je persoonlijke mailbox of uit een gemeenschappelijke mailbox kan in verkeerde handen vallen of publiek worden gemaakt.
- Betalingen of transacties kunnen worden uitgevoerd uit jouw naam met jouw bankrekening.
- Er kunnen boodschappen worden verspreid op sociale media vanuit jouw naam, waardoor je reputatie of die van je organisatie besmeurd wordt.

Aanbevolen acties

Hoe risico's van phishing verkleinen

- Wees altijd wantrouwig ten opzichte van e-mails die om persoonlijke informatie, wachtwoorden en financiële gegevens vragen.
  Deel bovenstaande informatie nooit via telefoon of email.
- Klik niet op hyperlinks die worden meegestuurd in verdachte e-mails.
  Ga met de aanwijzer boven de link staan, onderaan verschijnt de URL die verwijst naar de (malafide) website.
- Open geen bijlagen die worden meegestuurd met verdachte mails.
- Gebruik alleen computers waarop een up-to-date antivirus en antimalware programma draait.

Wat te doen bij vermoedelijke phishing

- Vraag advies aan bevoegde experten binnen de organisatie, zoals IT-helpdesk of de veiligheidsconsulent.
  Zij kunnen eventueel via de eigenschappen van de mail proberen na te gaan waar die werkelijk vandaan komt.
- Neem via een andere manier contact op met de vermeende afzender.
- Verander onmiddellijk eventueel vrijgegeven wachtwoorden, op alle websites of toepassingen waar datzelfde wachtwoord wordt gebruikt.
  Kies dit wachtwoord in de toekomst niet meer.
- Raadpleeg het laatste nieuws en de tips over online veiligheid op de site van de Vlaamse overheid
  [https://overheid.vlaanderen.be/klikgevaar]
  [https://www.safeonweb.be]

Veiligheidsconsulent: Yvan Gielens