PHISHING

- Verantwoordelijkheid van de overkoepelende vzw naar feitelijke verenigingen

De feitelijke vereniging is conform het Wetboek Vennootschappen en Verenigingen een vereniging zonder rechtspersoonlijkheid beheerst door de overeenkomst tussen partijen.

Omwille van het zonder rechtspersoonlijkheid functioneren, kan de feitelijke vereniging geen verbintenissen aangaan, geen eigendommen bezitten, geen schenkingen of legaten aanvaarden en zijn het de individuele leden die zich persoonlijk verbinden tot de verplichtingen van de vereniging.

Een vzw is niet verantwoordelijk voor de activiteiten van de onderliggende autonome feitelijke verenigingen.

Indien de activiteiten in eigen beheer van de feitelijke verenigingen worden gevoerd en indien de feitelijke verenigingen beschikken over eigen inkomsten en uitgaven, die niet in de jaarrekening van de koepel zijn opgenomen, dan wijst dit alvast op een autonoom beheer van de feitelijke verenigingen.

Het feit op zich dat de vzw overkoepelend werkt, brengt geen verantwoordelijk mee voor de onderliggende, autonome feitelijke verenigingen.

Wat betreft beveiliging tegen phishing, is er de mogelijkheid om (naar de toekomst toe) een cyberverzekering af te sluiten.

(bronnen: WVV en VSDC)

- Ter info

Phishing is een vorm van internetfraude waarbij criminelen via e-mail, sms, WhatsApp of telefoon proberen persoonlijke gegevens of geld te stelen.

Ze doen zich voor als een betrouwbaar bedrijf of instelling (zoals een bank of een webshop) en proberen je via valse links of telefoontjes te verleiden je inloggegevens, wachtwoorden of bankgegevens te geven.

Hoe werkt het?

- **E-mails en berichten:** Je ontvangt een bericht dat er verdacht uitziet, bijvoorbeeld omdat er wordt gedreigd met een geblokkeerde rekening, of omdat je geld terugkrijgt.
- **Valse websites:** De link in het bericht brengt je naar een nepwebsite die sterk op de echte site lijkt. Hier wordt je gevraagd in te loggen met je gegevens.

- **Telefoontjes (vishing):** Een oplichter belt je op en doet zich voor als iemand van je bank of een andere instantie. Ze vragen naar je pincode of andere gevoelige informatie.
- **Software installeren:** Soms proberen ze je via een link of bijlage schadelijke software te laten installeren, waarmee ze op afstand toegang krijgen tot je computer.

Hoe kun je phishing herkennen?

- **Algemene aanhef:** De e-mail of het bericht is niet persoonlijk aan jou gericht, maar gebruikt algemene aanhef zoals 'Geachte klant'.
- **Taal- en spelfouten:** Veel phishingberichten bevatten taal- of spelfouten.
- **Dringendheid of dreiging:** Er wordt druk uitgeoefend, met bijvoorbeeld een dreigement dat je account wordt gesloten als je niet meteen reageert.
- **Vreemde links:** Als je met je muis over de link gaat (zonder te klikken), zie je een ander webadres verschijnen dan het officiële adres.
- **Vragen om persoonlijke gegevens:** Banken en officiële instanties zullen nooit via e-mail, sms of telefoon naar je pincode, wachtwoord of andere gevoelige gegevens vragen.

Wat te doen bij phishing?

- **Klik nooit op links:** Klik niet zomaar op links in verdachte e-mails, sms'jes of WhatsApp-berichten.
- **Open bijlagen niet:** Open geen bijlagen van onbekende afzenders, want dit kan een virus installeren.
- **Neem nooit contact op via het nummer in het bericht:** Als je twijfelt, neem dan zelf contact op met de instantie via de officiële kanalen, bijvoorbeeld via de website of een telefoonnummer dat je zelf opzoekt.
- **Negeer of verwijder het bericht:** Sluit de pagina en verwijder het bericht. Verwijder het ook uit je prullenbak.
- **Meld het:** Meld het verdachte bericht bij de politie of andere relevante instanties, zoals Politie.be en Safeonweb.be.

(bron: AI-modus van www.google.com)