Phishing? Fraude?
Loopt u een beetje verloren?

Een woordje uitleg...

Phishing, afgeleid van het Engelse woord 'fishing', betekent 'vissen naar persoonlijke gegevens'. Een vorm van internetfraude om persoonsgegevens te bemachtigen. Waarna deze gegevens worden gebruikt om toegang te krijgen tot de onlinetools van de klant (bankapps bijvoorbeeld of sociale kanalen/media).

Bij phishing probeert de fraudeur het doelwit te verleiden tot het uitvoeren van een bepaalde actie (persoonlijke info doorgeven, een transactie uitvoeren…). Phishingberichten (vaak e-mails, valse webpagina's, sms'en, telefonische oproepen) lijken van een officiële instantie te komen (bv. de bank die een verdachte transactie heeft opgemerkt of Microsoft dat een probleem met de computer van het doelwit meldt), of van iemand die u kent om zo vertrouwen te winnen. Die sms, webpagina of e-mail bevat een link waarop de fraudeur uitnodigt te klikken om gegevens in te vullen of malware te installeren waarmee hij de controle over het systeem kan overnemen. Als het slachtoffer persoonsgegevens doorgeeft, belt de oplichter hem/haar op om hem/haar een betaling te doen uitvoeren.

Fraude is de algemene term/verzamelnaam voor oplichting waaronder phishing. Doel: het slachtoffer psychologisch manipuleren en beïnvloeden om handelingen te verrichten die hij of zij normaal niet zou doen. Voorbeelden? Fraude via de website 2dehands.be, WhatsApp, hulpvraagfraude, vriendschapsfraude, boilerroom, factuurfraude, CEO-fraude, overschrijvingsfraude, e-ID-fraude…

op deze pagina

Hoe herkent u een verdacht bericht?

- **Link**
  Klik nooit zomaar op een link in een verdacht bericht.
  Zweef met uw muis over de link, dan verschijnt de URL van de link.
  Is de domeinnaam (het woord vóór .be, .com, .eu, .org, … en voor de allereerste slash "/") ook echt de naam van de organisatie? Een voorbeeld:
  - Bij de link www.safeonweb.be/tips is het domein safeonweb.
  - Bij de link www.safeonweb.tips.be/safeonweb is 'tips' het domein en wordt u naar een andere website geleid.
    Twijfelt u of de link betrouwbaar is? Zoek de website dan eerst even op via een zoekmachine.
    Toch (per ongeluk) geklikt? Vul geen velden in en breek elke interactie af.
- **Onverwacht**

Krijgt u zonder enige reden een bericht van deze afzender: u hebt niets gekocht, het gaat over een wedstrijd waar u niet aan deelgenomen hebt, iemand met wie u geen contact hebt gehad, … Wees op uw hoede.

- **Dringend**
  Hou het hoofd koel als het bericht dwingend of dringend aanvoelt. Kreeg u echt een eerste aanmaning tot betaling? Kent u die 'vriend in nood' wel?
- **Afzender**
  Controleer het e-mailadres, ook op spelfouten. Fraudeurs gebruiken vaak een e-mailadres dat goed op het officiële adres lijkt. Maar let op, ook een legitiem e-mailadres biedt geen garantie.
- **Vreemde vraag**
  Een officiële instantie zal u nooit via e-mail, sms, Whatsapp of telefoon vragen naar uw wachtwoord, uw bankgegevens of andere persoonlijke en gevoelige gegevens.
- **Vraag tot betaling of bankverificatie**
  Wordt er u gevraagd om te betalen, terwijl het u onduidelijk is waarom? Of wordt er gevraag om uw rekeningnummer te verifiëren? Wees dan extra waakzaam. Er circuleren ook frauduleuze apps om een QR-code te scannen. Als u na het scannen van de QR-code op een site terechtkomt die u vraagt om te betalen of persoonlijke informatie door te geven zoals een rekeningnummer, rijksregisternummer of een bankcode, wees dan op uw hoede.
- **Persoonlijke aanspreking**
  Berichten met algemene en vage aanspreektitels, of alleen uw e-mailadres als aanspreking, kunt u beter wantrouwen. Ook taalfouten of een vreemde taal kunnen wijzen op een verdacht bericht.
- **Spamfolder**
  U kunt zelf verdachte berichten markeren als Spam of Junk en zo anderen waarschuwen.
- **Angst of nieuwsgierigheid**
  Iedereen zou nieuwsgierig worden bij berichten met een link als "Kijk wat ik over jou las ..." of "Ben jij dat op deze foto?". Maar laat u niet vangen: cybercriminelen spelen in op de actualiteit en weten welke thema's ons interesseren.

- **Safeonweb App**

Als u op uw smartphone de app van Safeonweb installeert, kunt u 2 soorten waarschuwingen krijgen:

- 'Nieuws' geeft informatie over actuele cyberdreigingen in België. Deze berichten gaan over actuele kwetsbaarheden, nieuwe phishingpraktijken en tips om u online nog beter te beveiligen.
- 'Bedreigingen' zijn waarschuwingen die specifiek zijn voor uw geregistreerde wifinetwerk.

Phishing-berichten over Vlaamse premies en teruggave van belastingen

Er circuleren frauduleuze berichten (mails en sms'en) over premies of teruggave van belastingen. Het gaat zowel om verzonnen premies (bv. aanmoedigingspremie voor alle sectoren werkend in België) als om bestaande premies (bv. renovatiepremie of groeipakket).

- De berichten **lijken afkomstig van de overheid** maar zijn dat niet. In de mails/berichten zitten links naar valse webpagina's, google-docs, …
- **Een officiële instantie zal u nooit via e-mail, sms, Whatsapp of telefoon vragen naar uw wachtwoord, uw bankgegevens of andere persoonlijke en gevoelige gegevens.**

Wat doet u met een verdacht bericht?

Klik niet op een link of bijlage in het bericht dat u niet vertrouwt. Surf beter rechtstreeks naar de aanmeldpagina van de website die u vertrouwt en meldt u daar aan om rechtstreeks in de beveiligde omgeving te bekijken of er een nieuw bericht of document voor u klaar staat.

- Stuur een (vermoedelijk) vals bericht via e-mail door naar verdacht@safeonweb.be .
    - U loopt geen gevaar als u een verdacht bericht doorstuurt.
    - Safeonweb.be scant het bericht automatisch op kwaadaardige inhoud (bv. poging tot fraude of een virus). Als de links of bijlagen schadelijk zijn, worden die doorgegeven aan de leveranciers van internetbrowsers, die de schadelijke inhoud kunnen blokkeren.
- Verwijder daarna de mail of het bericht.
- Als u een verdacht bericht **op het werk** ontvangt, moet u de procedures opvolgen die daar gelden voor phishing, bijv. doorsturen naar de ICT-dienst.

Hebt u toch op een link geklikt? Hebt u toch uw gegevens doorgegeven?

- Voer een virusscan uit.
- Als u een wachtwoord hebt doorgegeven dat u ook op andere plaatsen gebruikt, verander het dan onmiddellijk.
- Als u uw creditcardgegevens hebt doorgegeven, verwittig dan onmiddellijk Cardstop (www.cardstop.be of **078 170 170**).
  IN DIT GEVAL OOK UW BANK TENEINDE UW REKENINGEN TE LATEN BLOKKEREN .

Hebt u schade geleden door phishing?

Dien dan altijd klacht in bij de plaatselijke politie . Stuur het bericht zeker ook naar verdacht@safeonweb.be