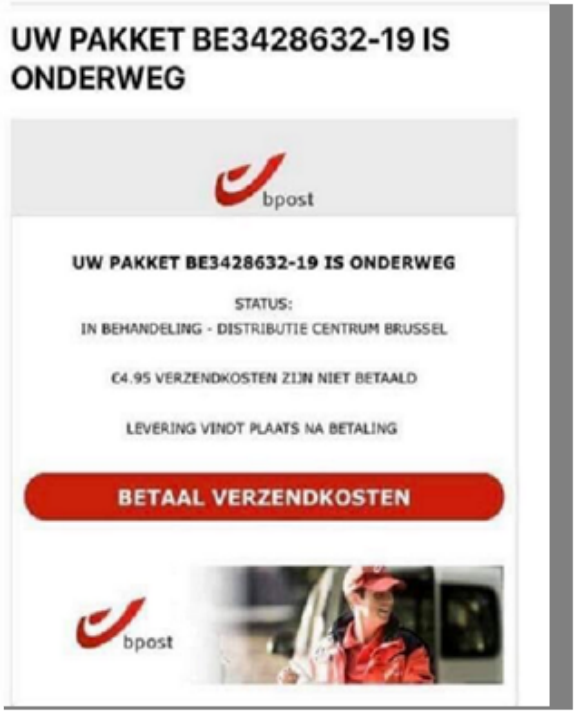
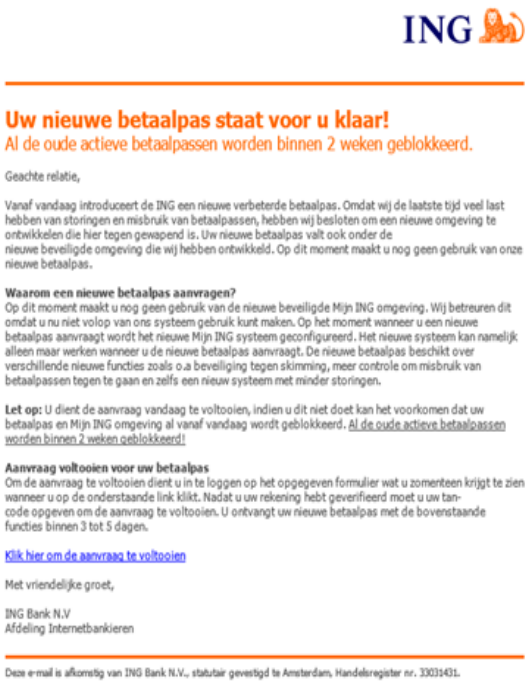
Phishing: het nieuwe inbreken anno 2021?

34.000.000 euro.[1] Dat is het totale bedrag dat phishers in het jaar 2020 konden stelen. Wat is phishing en hoe gaan deze cybercriminelen te werk? Krijg ik mijn geld terug als ik word opgelicht en hoe herken ik valse e-mails? Wij zochten het voor u uit.

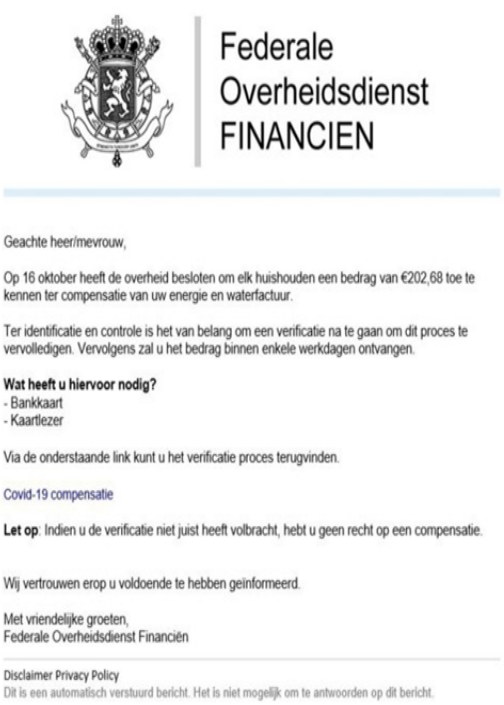
Phishing?

Phishing is een vorm van cybercriminaliteit waarbij het potentiële slachtoffer wordt benaderd via e-mail, sms, sociale media of telefoon. De oplichter doet zich daarbij voor als iemand anders in een poging toegang te krijgen tot de vertrouwelijke gegevens van slachtoffers. Het lijkt op internetfraude, met dit verschil dat de dader geen gegevens manipuleert, maar wel personen. Het is een vorm van psychologie om op die manier het vertrouwen te winnen van het slachtoffer. Phishers gaan hierbij zeer ingenieus te werk en spelen handig in op de actualiteit. Berichtjes van een bank, een technologiebedrijf of een postbedrijf dat zegt dat er een pakje op je wacht, de kans dat u één van deze berichtjes heeft ontvangen, is bijzonder groot.





[1] https://www.febelfin.be/nl/press-room/phishing-2020-de-cijfers



Federale Overheidsdienst FINANCIEN

Geachte heer/mevrouw,

Op 16 oktober heeft de overheid besloten om elk huishouden een bedrag van €202,68 toe te kennen ter compensatie van uw energie en waterfactuur.

Ter identificatie en controle is het van belang om een verificatie na te gaan om dit proces te vervolledigen. Vervolgens zal u het bedrag binnen enkele werkdagen ontvangen.

Wat heeft u hiervoor nodig?
- Bankkaart
- Kaartlezer

Via de onderstaande link kunt u het verificatie proces terugvinden.

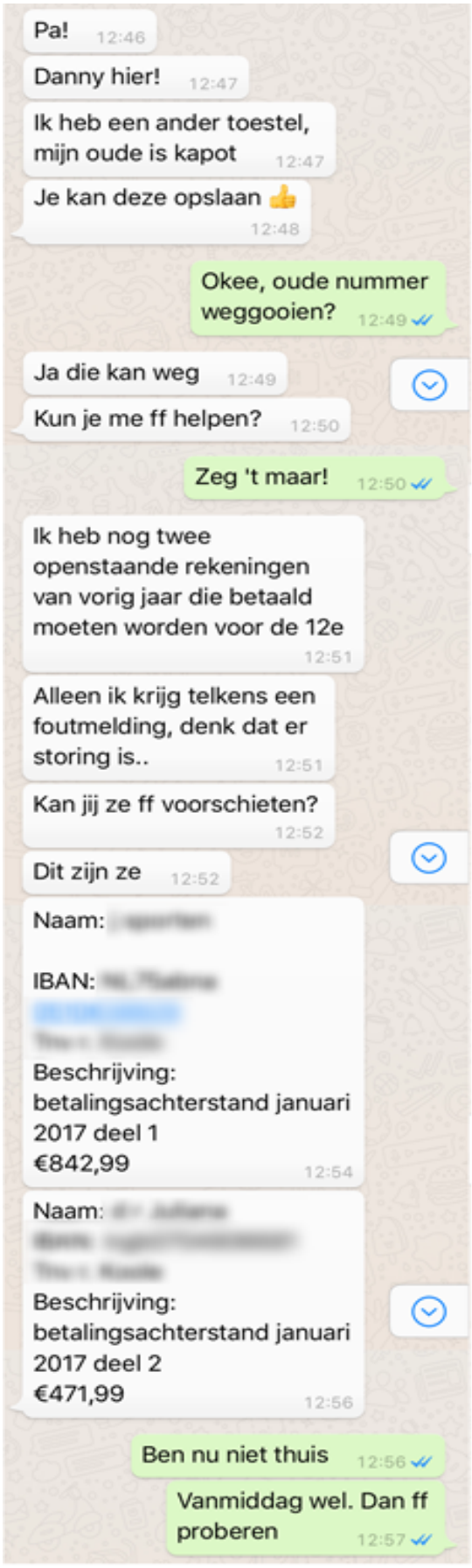
Covid-19 compensatie

Let op: Indien u de verificatie niet juist heeft volbracht, hebt u geen recht op een compensatie.

Wij vertrouwen erop u voldoende te hebben geinformeerd.

Met vriendelijke groeten,
Federale Overheidsdienst Financiën

Disclaimer Privacy Policy
Dit is een automatisch verstuurd bericht. Het is niet mogelijk om te antwoorden op dit bericht.



Het fenomeen van phishing of "hengelen" naar gevoelige gegevens zoals wachtwoorden en bank- of kredietkaartgegevens is de laatste jaren exponentieel gegroeid. In 2020 werden er maar liefst 3.200.000 verdachte berichten doorgestuurd naar het Centrum voor Cybersecurity België (CCB). In de eerste helft van vorig jaar stelde de politiediensten 3.438 pv's rond phishing op. Een viervoudiging in vergelijking met het jaar ervoor. Maar dat is nog maar het topje van de ijsberg, weet het Parket.[2]

Verschillende redenen liggen hiervoor aan de basis. Ten eerste stijgt het aantal phisingberichten exponentieel waardoor Justitie de toevloed aan dossiers simpelweg niet meer kan verwerken. Het lijkt haast een onaangename bijwerking van de coronacrisis, nu contacten steeds vaker digitaal verlopen. Gezien de vele slachtoffers en beperkte mensen en middelen bij Justitie is de kans dat daders gepakt worden eerder klein.

Daarnaast is de anonimiteit waarin de dader vertoeft een belangrijke verklarende factor.

[2] https://www.vrt.be/vrtnu/a-z/pano/2021/pano-s2021a7/.

Veilig van achter zijn computerscherm kan een cybercrimineel onder de radar van Justitie duizenden mensen tegelijk bestelen, nu zij in veel gevallen niet in staat zijn de identiteit te achterhalen van de persoon die valse berichten stuurt of een valse website opzet. Daders wanen zich straffeloos.

Tot slot, phishing is kinderspel. Je hoeft helemaal geen computerwizard te zijn om aan phishing te kunnen doen. Het is een kwestie van het vertrouwen te winnen van slachtoffers om op die manier gevoelige informatie te ontfutselen en vervolgens geld te stelen.

Hoe gaan deze cybercriminelen te werk?

Heel eenvoudig. Phishing kent vaak een gestructureerde organisatie. Bovenaan de piramide staan de IT-experten die softwareprogramma's maken waarmee zij geloofwaardige phishingsites en -mails kunnen maken. Door websites te hacken waarop personen zich hebben aangemeld, komen de oplichters aan data die via online marktplaatsen aangeboden worden in gesloten chatgroepen. Phishers kopen de data die voortkomen uit de softwareprogramma's en kiezen uit deze lijst hun slachtoffers. Op die manier kunnen phishers vaak duizenden mensen tegelijkertijd mailen. Onderaan staan de geldezels. Op hun rekeningen komt het geld van de slachtoffers terecht dat de phishers stelen. Met andere woorden een soort van afleidingsmanoeuvre voor Justitie, want zo blijven niet enkel de bendeleiders vaak buiten beeld bij de speurders, maar zijn ook de phishers amper te traceren.

Krijg ik mijn geld terug?

Misschien wel de belangrijkste vraag voor slachtoffers: krijg ik mijn geld terug? Essentieel hierbij is dat slachtoffers snel handelen. Heb je het gevoel dat een transactie bij nader inzien toch verdacht is, contacteer dan onmiddellijk uw bank. Zij kunnen de toegang tot jouw rekeningen laten blokkeren. De kans dat je op tijd bent, lijkt wel kleiner nu het geld definitief vertrekt vanaf het moment dat daartoe de opdracht werd gegeven. Vandaar dat banken samenwerken om zo snel mogelijk rekeningen te laten blokkeren. Zodra een bank op de hoogte wordt gesteld van een phishinggeval, zal de bank van het slachtoffer contact opnemen met de bank van de geldezel. Met andere woorden de bank naar waar het geld getransfereerd wordt. Zij proberen alsnog de gelden te blokkeren en achteraf te gaan recupereren.

Lukt dit niet en is er reeds geld verdwenen, dan staat er een mogelijkheid open tot schadevergoeding van uw bank. Deze laatste zal een belangenafweging maken omtrent de vraag of je als klant aansprakelijk kan gesteld worden of niet. Hiervoor gebruikt de bank de figuur van de 'grove nalatigheid'.[3] Men zal per situatie gaan kijken naar welke fraudetechniek gehanteerd werd en of klanten té onvoorzichtig geweest zijn door hun persoonsgegevens - weliswaar onder druk en te goeder trouw - te delen met een cybercrimineel. In elk geval is het zo dat de bewijslast rust bij de bank en het dus niet aan u is om te bewijzen dat je niet nalatig bent geweest.

Over de figuur van de 'grove nalatigheid' woeden de hevigste discussies, nu de wet niet duidelijk omschrijft wat wel en wat niet onder 'grove nalatigheid' dient te worden verstaan. Testaankoop[4] vindt dan ook dat banken te pas en te onpas dit

[3] https://www.standaard.be/cnt/dmf20210507_97478909

begrip inroepen om niet of minder te moeten terugbetalen. Voorbeelden van 'grove nalatigheid' zijn onder andere het nalaten van je bankkaart te laten blokkeren of de kaart samen met de code te bewaren of aan iemand toe te vertrouwen. Maar het is heel moeilijk om daar een algemene lijn in te trekken. In de praktijk is het immers wel zo dat heel wat banken, in heel wat gevallen, de klant terugbetalen.[5]

Schuift de bank de volledige aansprakelijkheid in uw schoenen en denk je als slachtoffer in uw recht te staan, aarzel dan niet om je conflict aan te kaarten bij Ombudsfin[6], de ombudsdienst voor financiële geschillen. Dat is een onafhankelijke instelling die kan bemiddelen omtrent betwistingen over frauduleuze verrichtingen en terugbetalingen tussen slachtoffer en bank.

Hoe herken ik valse berichten?

Phishers blijken zeer vindingrijk en bedenken geregeld nieuwe kunstgrepen om mensen geld of gegevens afhandig te maken. Daarnaast zijn de oplichtingsmethodes ook steeds moeilijker te herkennen. Het onderscheid maken tussen valse e-mails en betrouwbare berichten, het lijkt haast een onmogelijke opdracht. Hieronder zetten we een aantal tips op een rijtje om te beoordelen of je een bericht kan vertrouwen.

Twijfel je of een bericht verdacht is? Beantwoord dan kort voor jezelf deze vragen:[7]

1. Is het onverwacht?
2. Is het dringend?
3. Ken je de afzender?
4. Vind je de vraag vreemd?
5. Naar waar leidt de link waar je moet op klikken? Tip: beweeg over de link en kijk waar deze u naartoe stuurt. Een verdachte link doet u best niet open.
6. Word je persoonlijk aangesproken?
7. Bevat het bericht veel taalfouten?
8. Zit het bericht in je Spam?
9. Probeert iemand je nieuwsgierig te maken?

Zit er een reukje aan een bepaalde transactie die je hebt verricht? Contacteer zo snel mogelijk Card Stop om je kaart te laten blokkeren. Dit kan op het nummer 070

---

[4] https://www.test-aankoop.be/geld/betalen/dossier/betaalkaarten-hoe-krijgt-u-uw-geld-terug/dief-heeft-uw-kaart-of-gegevens.
[5] https://www.vrt.be/vrtnu/a-z/pano/2021/pano-s2021a7/
[6] https://www.ombudsfin.be/
[7] https://www.safeonweb.be/nl/leer-valse-mails-herkennen

344 344. Weet dat Card Stop nooit mensen zal opbellen. Geeft iemand zich aan de telefoon uit als een medewerker van Card Stop, dan is dit 100% een oplichter.

Daarnaast is het belangrijk om zo veel mogelijk bewijzen te verzamelen. Noteer steeds alle gegevens die je van de oplichters kreeg, zoals telefoonnummers en namen. Neem eventueel screenshots van de vervalste mails, links en website. Met deze bewijzen op zak kan je eenvoudig een aangifte doen bij de politie en een proces-verbaal laten opstellen.

Tot slot, geef nooit persoonlijke codes door zoals je pincode of responscode. De bank zal deze codes immers nooit vragen via welk kanaal dan ook. Wees in het algemeen niet te naïef. Een bericht dat te mooi is om waar te zijn, zal dit meestal ook zijn. Daarnaast spelen phishers vaak in op het gevoel dat het snel moet gaan. Wees dus alert voor berichten waar een zekere urgentie achter zit. Geloof niet blindelings in elke mail of sms, maar geloof ook niet dat het jou nooit zou overkomen. Wees op je hoede en dubbelcheck!

Komt u tijdens het surfen op het internet een verdacht bericht tegen, aarzel dan zeker niet om dit bericht door te sturen naar verdacht@safeonweb.be. Zij controleren de links en bijlages van deze doorgestuurde berichten waarbij ze in staat zijn om verdachte links te laten blokkeren. Op die manier zijn minder oplettende internetgebruikers die op de link geklikt hebben, ook beschermd. Door snel te ageren, verkleint de kans dat cybercriminelen slachtoffers maken. Een gewaarschuwd man is er twee waard.

Indien u na het lezen van dit artikel nog vragen hebt omtrent phishing, aarzel dan niet om ons te contacteren via joost.peeters@studio-legale.be, simon.geens@studio-legale.be of 03 216 70 70.