Internetfraude

Prof. Em. Walter Leirman

SENIORNET VLAANDEREN vzw

VZW opgericht in juni 2000

Guido Willekens, lesgever Seniornet Vlaanderen

Veilig werken met een PC of Smartphone

Agenda

waar schuilt het gevaar?
wat maakt het Internet onveilig?
waar moet ik zelf voor opletten?
de topper is nog altijd Phishing!
wat moet ik doen als ik opgelicht ben?

Beveiligen: Waartegen? Hoe?

Alleen op een eiland:

- Geen beveiligingsrisico

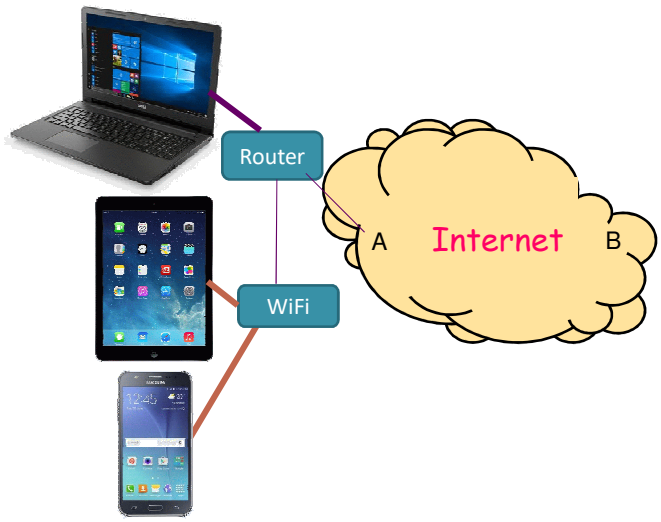
Beveiligen: Waartegen?

Meerderen op een eiland:

- Risico van diefstal van toestel
- Risico van frauduleus inloggen en diefstal van gegevens
- Begrip: ACCOUNT =

  GEBRUIKERSNAAM + PASWOORD

Verbinden met INTERNET: met Router



Beveiligen: Waartegen?

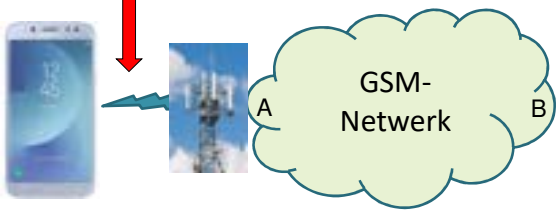
De verbinding met Internet:

- Met kabel: geen probleem
- Met WiFi: aftappen mogelijk

- Oplossing tegen aftappen: VPN: een tunnel van begin- tot eindpunt
- Virtual Private Network (Betalend)

Verbinden met INTERNET: via 3G of 4G GSM Netwerk

- Aftappen mogelijk



Beveiligen: Waartegen?

Bij gebruik van internet…

In volgorde van schade risico

- Spam(ware): vervelend
- Malware: echt storend
- Virussen: gevaarlijk
- Phishing: bedreigend
- Hackers: nemen over
- RansomeWare: fataal

Inbreuken op mijn Privacy

- Voor iedereen anders…

Spam is vervelend

- Ongewenste mail die je allerlei zaken aanbiedt (bv. Medicijnen, uurwerken, bitcoins, beleggen in vastgoed, enz.)
- NOOIT op deze mails antwoorden en niet op webadressen die er in vermeld staan klikken

SENIORNET VLAANDEREN

Waarom ontvang ik Spam en Phishing?

Op het internet is de account GEBRUIKER = E-MAIL adres

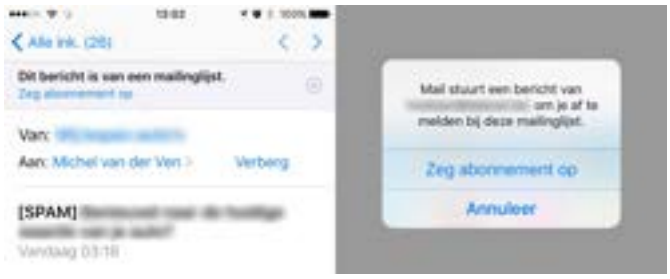
Op het 3G, 4G netwerk is de GEBRUIKER = GSM nummer

- De kans is groot dat je e-mailadres terecht is gekomen op een lijst die door verschillende spammers wordt gebruikt
- Daarom blijf je deze berichten krijgen, ook al heb je een aantal afzenders geblokkeerd. Andere spammers kunnen de lijsten nog steeds gebruikten.

SENIORNET VLAANDEREN

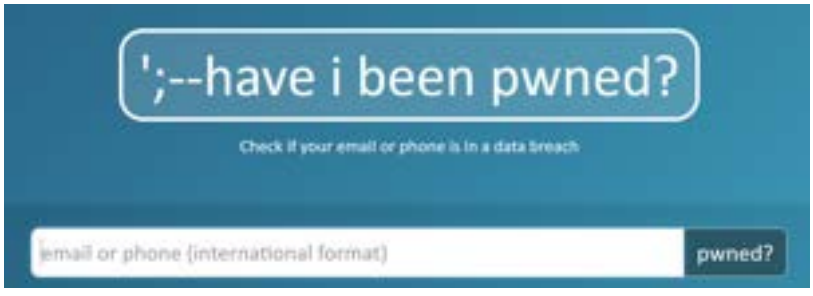
Klik nooit op ‘afmelden’ in een spammail

- Onderaan spamberichten is regelmatig een link te zien waar je op kunt klikken om je af te melden
- Dit is vaak een valse link: de afzender ziet dat je mailadres bestaat en wordt gebruikt
- Gevolg: je zal meer spam ontvangen!



Komt mijn mailadres en telefoonnummer voor in datalekken?

https://haveibeenpwned.com



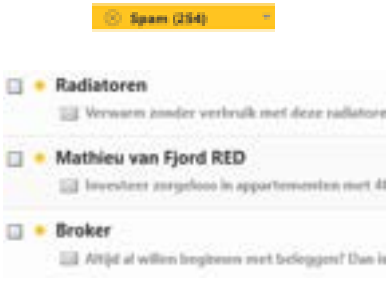
Hoe vermijd ik dat mijn mailadres op een lijst komt die cybercriminelen gebruiken?

- Hou je mailadres privé
- Denk 2 keer na voor je je mailadres opgeeft voor nieuwsbrieven en marketingacties
- Stuur kettingbrieven niet door
- Gebruik een wegwerp mail adres voor bepaalde zaken

Spam bestrijden

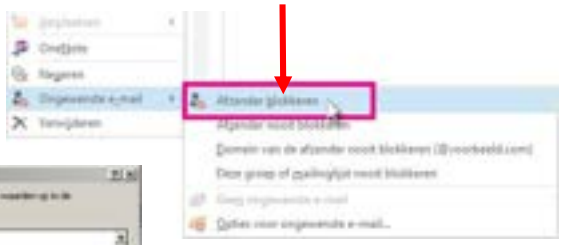
- Vermijdt een leeg onderwerp of eentje met woorden als gratis, gewonnen, bom, etc.
- De meeste providers (Telenet, Proximus…) filteren zelf op spam en sturen die niet meer door
- Zo kan een mail al eens verloren gaan: ga af en toe kijken via de webmail in de map voor spam

https://mail.telenet.be/



Spam vermijden

- Best de afzenders van deze mails blokkeren en de mails verwijderen.



Schrijf zelf filter regels

Malware is echt storend

- Malware is de naam voor computerprogramma's (of delen daarvan) die informatie vergaren over een computergebruiker en deze doorsturen naar een externe partij. Het doel van malware is meestal om geld te verdienen
- Je wordt bedolven onder popups, ongewenste werkbalken verschijnen in je browser. Je startpagina en zoekmachine worden gekaapt zodat je terecht komt op sites die je helemaal niet wil zien.
- Onbekende programma's die plotseling op je computer geïnstalleerd zijn.
- Je surfgedrag wordt gecontroleerd: elke stap die je doet op het World Wide Web wordt gevolgd....
- Sommige freewareprogramma's die aangeboden worden op het internet, kunnen Malware bevatten.

Oplossingen

- Adblockplus

- Hitman Pro (suite)

(Computer) Virussen

- *Bijna even oud als de computer*
- *Lijken in veel opzichten op echte virussen*
- ze *verspreiden* zichzelf
- ze *tasten de systemen aan* waarin ze zich nestelen
- Ze bestaan in *vele varianten*: van griepje tot ebola
- Meeste *leveranciers* (Telenet, Proximus, Scarlet) bieden een *bescherming*
- Zitten vaak in *de bijlagen* bij een E-mail

1987 Eerste zware aanval

(Computer) Virussen Oplossingen

Basisregel: verdachte e-mails direct verwijderen !!!!

open **nooit** vreemde e-mails maar **verwijder ze direct**
bijlagen **niet** automatisch openen
downloaden alleen van **betrouwbare sites**

Bescherming: gebruik een antivirusprogramma

Betalend: McAfee, Norton, G-Data…

Antivirusprogramma geregeld laten bijwerken

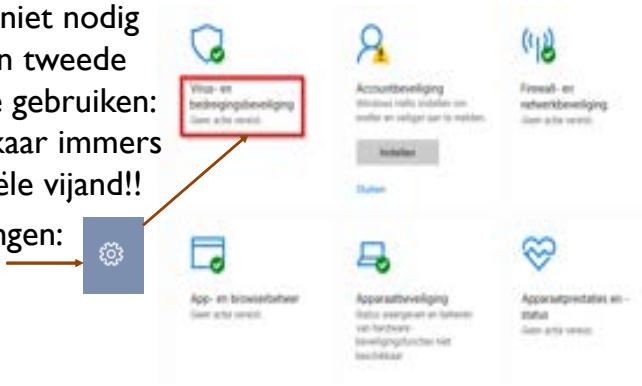
Updaten! Liefst automatisch

Hou uw besturingssysteem en toepassingen up to date

Doe dat regelmatig

Gratis: Windows 10 Defender

- De recentste versies van Windows 10 hebben een ingebouwde antivirus die vrij goed is.
- Het is dan niet nodig om nog een tweede antivirus te gebruiken: die zien elkaar immers als potentiële vijand!!
- Via Instellingen:



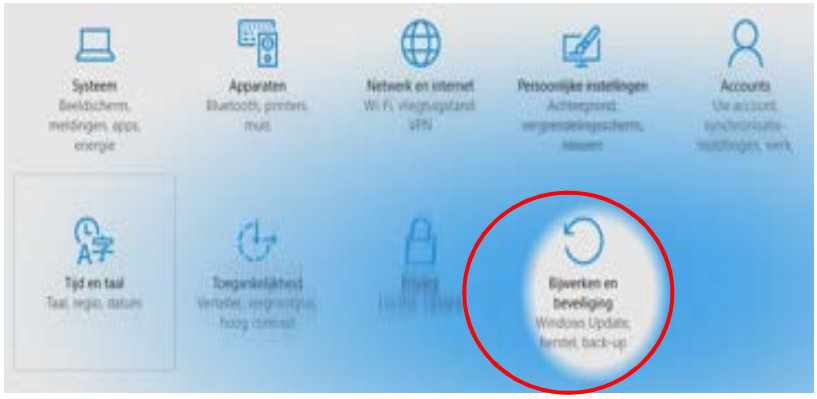
Gratis: Avast

- https://www.avast.com/nl
- Elk jaar registreren, blijft daarna gratis
- Vertraagt opstarten
- Soms vervelende boodschappen om te doen kopen

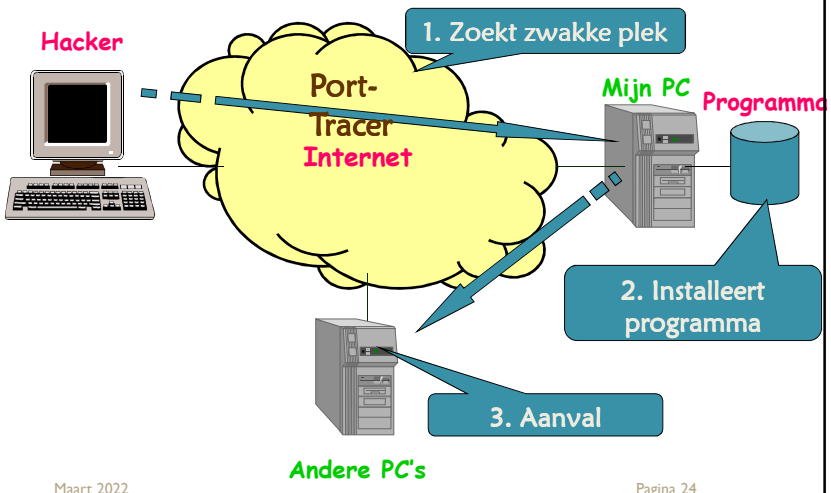
Gratis: Kaspersky

- → https://www.kaspersky.com/free-antivirus
- Nog recent en daarom minder vervelende boodschappen om te doen kopen…
- Wordt nu afgeraden: Russische oorsprong

Hou uw Windows up to date



Hackers: nemen over.



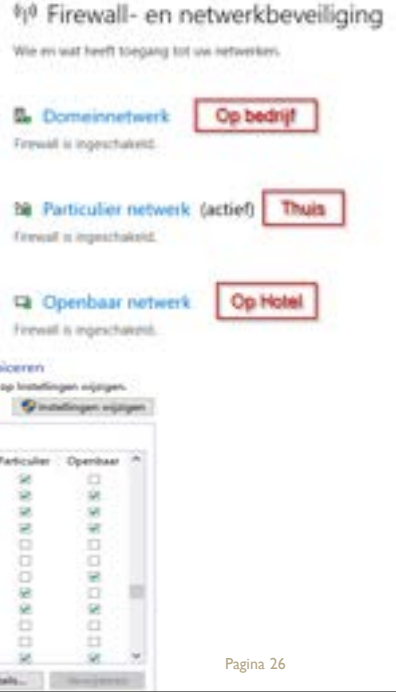
Bescherming: de FireWall

- Elke Toepassing of App gebruikt een Protocol
- Elk Protocol heeft een Poort Nummer…
  Vb.: HTTP is poort 8080
- Sluit alle onnodige poorten

FireWall in Windows 10

- Via de instellingen:

Firewall- en netwerkbeveiliging



Ransomware: fataal

- Hackers vergrendelen al je harde schijven en vragen losgeld (Ransom) om deze vergrendeling op te heffen.
- Regel : NOOIT BETALEN!!!
- Preventie: maak altijd een backup van je systeemschijf en gegevensschijf op een externe drager of in de Cloud.
- Laat je externe schijf niet aan je PC hangen als je ze niet nodig hebt: ze wordt ook immers versleuteld!
- Maar één oplossing: ga met toestel en back-up naar een specialist.

Phishing
Geef oplichters geen kans!

Phishing is bedreigend

- Oplichters "vissen" naar je gegevens.
- Ze sturen een e-mail die lijkt op die van een vertrouwd bedrijf, zoals bv. een bank, telefoonmaatschappij, enz..
- Ze vervalsen ook de website van de afzender. Hap je toe, kunnen je geld en zelfs je identiteit in gevaar zijn.

- **NOOIT** vertrouwelijke gegevens zoals rekeningnummer en pincode doorgeven.
- Best de mails ongelezen verwijderen.

SENIORNET VLAANDEREN vzw

1. De media

pano.

Phishers gingen vorig jaar aan de haal met 34 miljoen euro: "Hoe kan je zo stom zijn, dacht ik, en ik trapte er zelf in"

Oplichters hebben vorig jaar 34 miljoen euro gestolen via phishing. Fraudeurs sturen slachtoffers een mail of sms waarin ze zich voordoen als iemand anders, bijvoorbeeld je bank, om zo codes te stelen. Ons reportagemagazine "Pano" kon via onlinechatgroepen honderden gesprekken voeren met phishers en daaruit blijkt dat online oplichting kinderspel is.

SENIORNET VLAANDEREN vzw

Mail vol taalfouten kost bol.com 750.000 euro

De Nederlandse webwinkel bol.com heeft zich in de luren laten leggen door een phishingmail. Eigen schuld, dikke bult; oordeelt een Nederlandse rechter.

Eind 2019 kreeg webwinkel Bol.com een mail, zogezegd van een medewerker van het bedrijf Brabantia. Daarin stond dat betalingen voortaan op een ander rekeningnummer moesten gebeuren. De mail stond vol taalfouten. "*Houd he rekening mee dat we vanaf vandaag een wijziging in onze bankrekeninggegevens hebben voor incaende betalingen. Voortaan moten all incoming betalingen have been overgemaakt naar onze filiaalrekening in Spanje. We het op prijs as u uw gegevens kunt bijwerken*", stond er letterlijk in.

Zonder te controleren of het wel om een echte mail ging, werkte Bol de betaalgegevens bij, en werden betalingen uitgevoerd op dat nieuwe bankrekeningnummer. In januari 2020 vroeg het échte Brabantia aan Bol.com waarom de rekeningen niet betaald werden. Toen werd duidelijk dat de webwinkel het slachtoffer geworden was van fraude. In totaal had Bol.com ruim 750.000 euro aan de oplichters betaald.

bol.com

Categorieën Cadeaus & Inspiratie Aanb

Klantenservice › Nepmails

Nepmails

Phishing mails herkennen & wat te doen

Herken een nepmail

- de mail is slordig opgesteld.
- de mail bevat taalfouten.
- je naam staat niet in de aanhef (wij spreken je altijd aan).
- je moet iets doen om te voorkomen dat er een groot bedrag van je rekening wordt afgeschreven. Zoals klikken op een link of informatie geven.
- je moet klikken op een link om de verzending van een artikel dat je niet hebt besteld te volgen.
- je wordt uitgenodigd voor een prijsvraag en kunt winnen door alleen maar op de link te klikken en je gegevens achter te laten.

Maart 2022 33

Radio 2-Inspecteur Sven Pichal liet zich phishen: "Denk bij elk bericht dat je opent anderhalve seconde langer na"

Maart 2022 34

> **„Het was zo'n typisch" zinnetje: Hey Sven, ik moet je dit nog vertellen over jouw studiogast van vandaag...**
>
> — Sven Pichal, De Inspecteur

"Ik heb een mail gekregen waarvan ik **niet doorhad dat het een valse mail was.** In die mail stond een link waar ik niet op had moeten klikken. Maar waarop ik dus wel heb geklikt ... Toen ik het doorhad, heb ik heel hard 'Kraki!' en **'Smeerlappen!'** geroepen. De link opende en ik kreeg een video te zien waarin me verteld werd dat ik dat niet had mogen doen. Maar wie was die smeerlap?", lacht onze Inspecteur Sven Pichal.

Het was **David Van Ooteghem** van 'Spits' zijn idee om eens te proberen of we de [illegible] dat we ons niet mogen laten vangen, zelf te phishen. David kreeg de hulp van Frederik [illegible] een ethische phisher. Hij wordt ingehuurd door bedrijven om hun werknemers bewust te maken van de gevaren van internet, zonder dat hij écht kwaad wil doen.

SENIORNET VLAANDEREN vzw

Inspelen op het gevoel

Frederik twijfelde er niet aan dat het zou lukken. Hij had drie strategieën: "Als ik hem wil te pakken krijgen, moet ik **inspelen op zijn emoties**. Ik ga hem proberen boos te maken of **zijn nieuwsgierigheid op te wekken.** Door in te spelen op zijn emoties [illegible] dat hij niet nadenkt, maar **gewoon doorklikt.**"

Het tijdstip is belangrijk

"Het is ook belangrijk dat ik **goed nadenk over het tijdstip** dat ik mijn phishingmail verstuur", gaat Frederik verder. "Door een beetje op te zoeken op het internet weet ik wanneer hij zijn programma heeft. Dat is ook het tijdstip dat hij iets minder attent is. Dat is misschien wel het goede tijdstip voor mij om toe te slaan."

En het **tijdstip was goed gekozen, vertelt Sven** [illegible] gestuurd tijdens het programma 'De inspecteur'. Ik heb dan meestal geen tijd om mails te lezen, maar meteen na de uitzending staan er dan een stuk of 12 mails klaar. Daarbij stond dus ook een mailtje dat **me inderdaad wel nieuwsgierig maakte.**"

SENIORNET VLAANDEREN vzw

Het Nieuwsblad

Vrijdag 14 mei 2021

Al 10.000 slachtoffers van valse app Bpost

In amper 48 uur tijd zijn bijna 10.000 Belgen het slachtoffer geworden van een oplichtingstruc via sms. Hackers stuurden massaal berichten uit, zogezegd van Bpost, waarin gevraagd wordt op een link te klikken om na te gaan waar je pakket zich bevindt. Wie ingaat op de vraag om ook de (valse) app van Bpost te downloaden, is gehackt. De oplichters kunnen op die manier bankkaartgegevens en paswoorden stelen.

"De omvang, snelheid en professionaliteit van deze aanval zijn ongezien", zegt Miguel De Bruycker, de baas van het Centrum voor Cybersecurity. (phu) ▶3

SENIORNET VLAANDEREN.nav

SENIORNET VLAANDEREN.nav


3
Er werd gevraagd de 'officiële applicatie' van Bpost te installeren op je Android-toestel. Wie een iPhone gebruikt loopt minder gevaar, want enkel via Android kan je applicaties downloaden die niet standaard in de Playstore of Appstore zitten.
4
Eens de valse app geïnstalleerd, is het kalf verdronken. Er is helemaal geen postpakket onderweg, wel steelt een hacker intussen al je persoonlijke gegevens, van je bankkaartgegevens tot je adres, je locatie, je paswoorden, noem maar op.
5
Je nummer wordt nadien hergebruikt om in het buitenland, dezer dagen veelal in Spanje, nieuwe slachtoffers te maken. Vaak stuurt de hacker tot tienduizend sms'en in jouw naam.
6
De app zelf verwijderen lukt niet. Je kan wel opnieuw de fabrieksinstellingen herstellen en hopen dat je intussen niet digitaal bestolen werd.
SENIORNET VLAANDEREN vzw
Maart 2022
39


Belgisch cybersecuritycentrum analyseerde in 2020 3,2 miljoen phishingmails
Het Centre for Cyber Security in België kreeg het afgelopen jaar bijna twee keer zoveel phishingmeldingen binnen als het jaar ervoor. Op een speciaal daarvoor bedoeld e-mailadres kwamen in 2020 3,2 miljoen berichten binnen.
In totaal kwamen er in heel 2020 3.225.234 berichten binnen op het e-mailadres verdacht@safeonweb.be. Dat is een initiatief van het Centre for Cyber Security Belgium waar burgers een mogelijk phishingbericht naar kunnen doorsturen als ze die hebben ontvangen. In heel 2019 kwamen er nog maar half zoveel berichten binnen: 1,7 miljoen.
De instantie analyseert die berichten geautomatiseerd. Vervolgens worden verdachte links doorgestuurd naar bijvoorbeeld Google en Microsoft, die ze kunnen blokkeren in e-mailclients en zoekmachines. Uit alle binnengekomen berichten werden 667.356 frauduleuze url's gehaald die zijn doorgestuurd. Ook werden er 26.109 bijlages gedetecteerd, waarvan er 4370 een virus zouden bevatten.
Volgens het CCB was het merendeel van de berichten traditionele phishing. Het ging om onderwerpen zoals nepwaarschuwingen van banken en overheidsinstellingen, pakketdiensten en diensten als PayPal of Microsoft. In zo'n 45.000 gevallen ging het om corona-gerelateerde phishing. Het CCB zegt dat het niet zeker kan weten of er ook meer berichten zijn verstuurd, maar in ieder geval wel dat die op het e-mailadres zijn binnengekomen.
SENIORNET VLAANDEREN vzw
Maart 2022
40

2. Phishing voorbeelden: E-mails


ING

Uw nieuwe betaalpas staat voor u klaar!

Al de oude actieve betaalpassen worden binnen 2 weken geblokkeerd.


ARGENTA

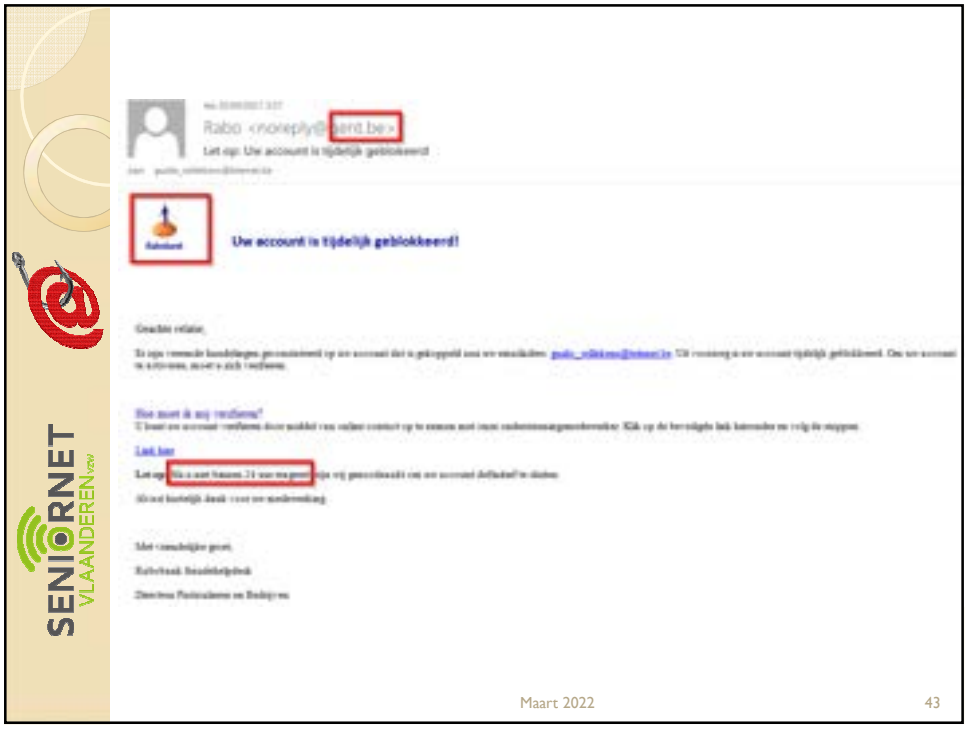
Geachte klant,

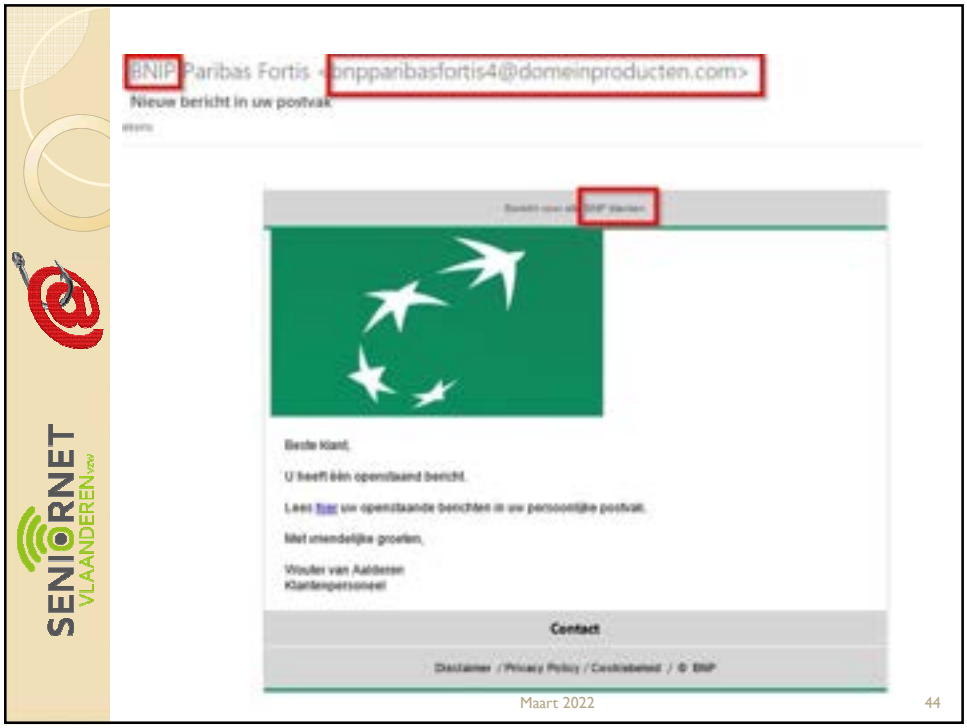
Bevestig op tijd uw gegevens, zo weten wij dat uw gegevens nog up-to-date zijn. U heeft tot 5 juli om deze bevestiging te voltooien. Volgens onze voorschriften is dit verplicht voor al onze klanten.

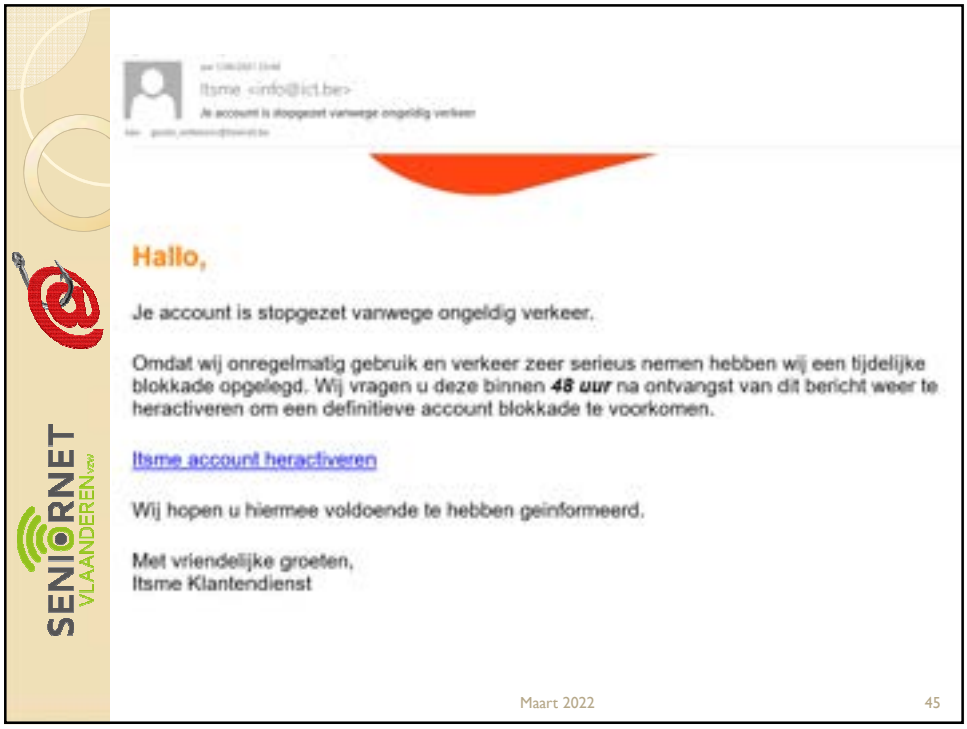
Als u nog vragen heeft dan kunt u contact opnemen met onze klantenservice.

Met vriendelijke groet,

Frank Rooijs
Klantendienst


Rabo <noreply@kbc.be>
Uw account is tijdelijk geblokkeerd!
SENIORNET VLAANDEREN vzw
Maart 2022
43


BNP Paribas Fortis <bnpparibasfortis4@domeinproducten.com>
Nieuw bericht in uw postvak
Beste klant,
U heeft één openstaand bericht.
Met vriendelijke groeten,
Contact
SENIORNET VLAANDEREN vzw
Maart 2022
44

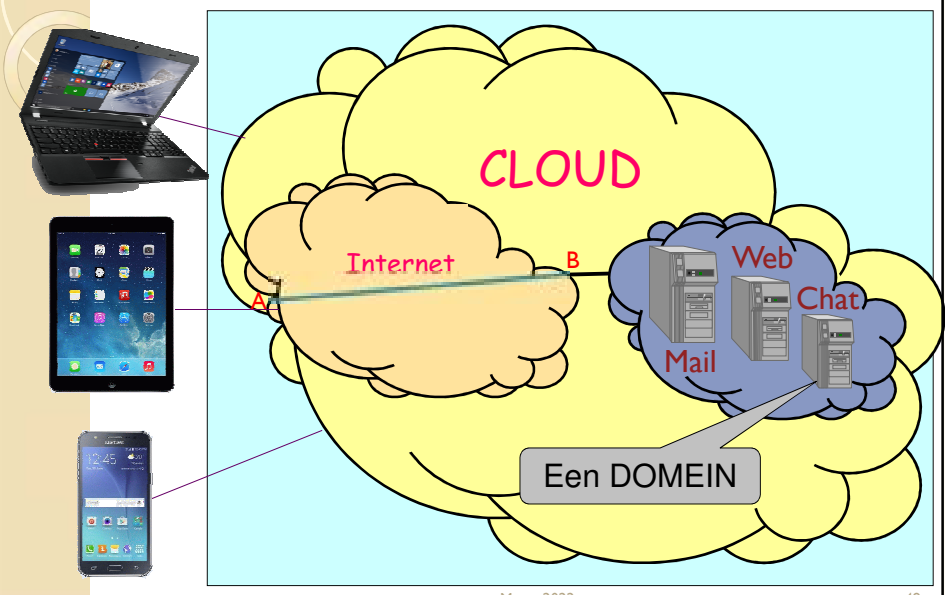

Itsme <info@ict.be>
Je account is stopgezet vanwege ongeldig verkeer
Hallo,
Je account is stopgezet vanwege ongeldig verkeer.
Omdat wij onregelmatig gebruik en verkeer zeer serieus nemen hebben wij een tijdelijke blokkade opgelegd. Wij vragen u deze binnen 48 uur na ontvangst van dit bericht weer te heractiveren om een definitieve account blokkade te voorkomen.
Itsme account heractiveren
Wij hopen u hiermee voldoende te hebben geinformeerd.
Met vriendelijke groeten,
Itsme Klantendienst
SENIORNET VLAANDEREN vzw
Maart 2022
45


My e-box <mailsysteem@myebox.be>
Nieuwe bericht in uw online brievenbus
Ongelezen bericht in uw beveiligde elektronische brievenbus
Geachte heer/mevrouw,
U heeft een nog ongelezen bericht van in uw eBox.
Belangrijke info betreft uw COVID-19 Vaccin.
U kan dit bericht inkijken tot 28/05/2024.
Bekijk dit bericht via my e-box :
mycitizenebox.belgium.be/myebox/
Het eBox team
.be
SENIORNET VLAANDEREN vzw
Maart 2022
46


my e-Box <myebox@inmna.email>
[BSSPAM-LOW] Actie vereist, betaal uw verkeersboete direct!
Nieuw bericht in uw beveiligde elektronische brievenbus
U heeft een nieuw bericht ontvangen van FOD Justitie in uw eBox.
Verkeersboete van FOD Justitie
U kan dit bericht inkijken tot 22/08/2021.
Bekijk dit bericht via My eBox :
Ga naar My eBox
Het eBox team
SENIORNET VLAANDEREN
Maart 2022
47


Federale
Overheidsdienst
FINANCIEN
Hoe herkent u een poging tot fraude?
1. Het e-mailadres van de afzender is geen officieel adres van de FOD Financiën.
● Officiële extensie: @minfin.fed.be of @mailing.minfin.fed.be
● Andere extensie. Opgelet! Fraudeurs gebruiken soms een e-mailadres dat goed op het officiële adres lijkt (bv.: @minfin.fgov.be, minfin.fed.be@europe.com; @minfin-fed.org ...).
2. ● Men vraagt u om via e-mail, sms of whatsapp vertrouwelijke bankgegevens of gegevens in verband met internetbankieren (digipass) mee te delen.
3. Het verhaal is te mooi om waar te zijn of komt totaal onverwacht:
● U krijgt plotseling een bericht dat men u een bepaald bedrag gaat terugbetalen.
● U wordt verzocht om een schuld te vereffenen, maar u hebt geen idee waarover het gaat.
4. Men vraagt u om een betaling te doen naar de bankrekening waarop u dat moet doen, is geen bankrekening van de FOD Financiën. Er zijn maar een beperkt aantal manieren om een betaling te doen aan de FOD Financiën:
● U gebruikt MyMinfin.
● U stort het bedrag op een officiële rekening. Die heeft altijd de volgende structuur: BEXX 6792 XXXX XXXX.
● U gaat naar een van onze kantoren en u doet daar de betaling.
5. ● Er staan veel spel- en/of taalfouten in het bericht.
6. ● De persoon die u opbelt, is opdringerig en gebruikt dreigementen om u aan te sporen snel een betaling te doen.
7. ● U krijgt een e-mail, sms of whatsapp van een gerechtsdeurwaarderskantoor waarin die u in onze opdracht vraagt om een schuld te vereffenen. We werken wel samen met gerechtsdeurwaarders, maar die sturen geen officiële documenten per e-mail, sms of whatsapp. Meer tips over fraudepogingen door valse deurwaarders.
SENIORNET VLAANDEREN
Maart 2022
48

Wat is een DOMEIN?



Tip 1: controleer de afzender

De domeinnaam is het stukje van het adres achter het @ teken

- Is de domeinnaam van het e-mailadres raar?
  - @xyz123.be is een vreemde domeinnaam
  - federalepolitie@gmail.com: een officiële instantie of bedrijf gebruikt geen mailadres bij gmail, hotmail,…
- Ken je de afzender niet?
- Of verwacht je er helemaal geen bericht van?

Uitkijken dan!

Tip 2: lees de URL (adres van de site)

- Controleer altijd de URL en de domeinnaam van de links alvorens er op te klikken. Je kan dit eventueel eenvoudig controleren door je cursor er op te plaatsen zonder er op te klikken!
- **delhaize-be.site** is geen domein van Delhaize. Achteraan zou je **delhaize.be** moeten zien.
- Controle domeinnaam: tik in Google bv. Delhaize in en kijk welke domeinnaam er gebruikt wordt.

Tip 3: let op de taal en de stijl

- Bevat de tekst schrijffouten? Dan is het bijna zeker Phishing
- Is het taalgebruik opdringerig en dwingend?
  - Het taalgebruik van een professionele partij, zeker van een financiële instelling, zal nooit opdringerig zijn.
  - Berichten naar klanten krijgen nooit de vermelding 'importance: high'. Dit doen criminelen om je onder druk te zetten.
- Maakt het bericht je echt nieuwsgierig?
  Denk dan geen 2 maar 5 keer na voor je klikt.

Tip 4: kijk uit met onverwachte berichten/mails

Is de communicatie onverwacht? Wees dan op je hoede.

- Heb je geen pakketje besteld? Dan is de kans heel klein dat je een trackingcode of andere informatie rond een pakket toegestuurd krijgt.
- Idem voor een bericht dat je krijgt van een bank of een leverancier waarvan je geen klant bent.

Even oefenen


Herinnering: Uw betaalde belastingen ontvangen
Van: "Vlaamse Overheid" <contacting@beschikkingsaffiniteit.nl>
Aan: "Willy Messiaen" <willy.messiaen@telenet.be>
Vlaamse overheid
Belastingen terugbetaling
Maart 2022
55


Wij hebben een verrassing voor Bol.com-klanten!
Van: "Bol.com" <km9zks0@quadranet.com>
Aan: "Willy Messiaen" <willy.messi en@telenet.be>
bol.com
Hartelijke Dank Geachte!
Vul onze in om in aanmerking te komen voor deze speciale aanbieding 30 seconden marketingonderzoek over je ervaringen met en kies je beloning
Klik op OK om te Beginnen!
Om te Beginnen
Maart 2022
56


Nieuwe Mededeling
Van: "Bnpparibasfortisnv" <hoofdkantoor1@mynargenadienste.com>
Aan: "Willy Messiaen" <willy.messiaen@telenet.be>
BNP PARIBAS
FORTIS
Beste klant,
U heeft een belangrijke mededeling in uw postvak. Lees hieronder uw ongelezen bericht voor 1 mei.
Bericht Lezen
Hoogachtend,
Melissa Jacobs
Afdeling personeelszaken
SENIORNET VLAANDEREN.nav
Maart 2022
57


GEFELICITEERD Willy Messiaen!
Van: "NMBS" <[info@telenet.be.willy.messiaen@telenet.be>>
Aan: "Willy Messiaen" <willy.messiaen@telenet.be>
10X
onbeperkt reizen
Beste Willy Messiaen,
Maak nu kans ›
SENIORNET VLAANDEREN.nav
Maart 2022
58


willy.messiaen, UW PAKKET BE3428632-21 IS ONDERWEG
Van: "bpost Bezorgdienst BE" <tM1CEiBAx2bzFNYHlv7willy.messiaen@apathhy.xyz>
Aan: "Willy Messiaen" <willy.messiaen@telenet.be>
Antwoorden aan: reply@apathhy.xyz
Uw pakket is onderweg:
BE3428632-21
STATUS: WACHTEND IN HET DISTRIBUTIECENTRUM
HUIDIGE BEHANDELING BIJ SORTEERCENTRUM BRUSSEL
ONTBREKENDE BETALING VAN €1,50,-
UW PAKKET WORDT VERZONDEN WANNEER HET BEDRAG IS BETAALD
VERZENDKOSTEN BETALEN
SENIORNET VLAANDEREN.nav
Maart 2022
59


Kom nu binnen en ontvang je cadeau
Van: "eClickx" <eclickx@bluepixlmedia.info>
Aan: "Willy Messiaen" <willy.messia n@telenet.be>
Antwoorden aan: reply@cli-nique.com
PAASPAKKET!
Hallo willy.messiaen
JA, wil ik! ›
SENIORNET VLAANDEREN.nav
Maart 2022
60

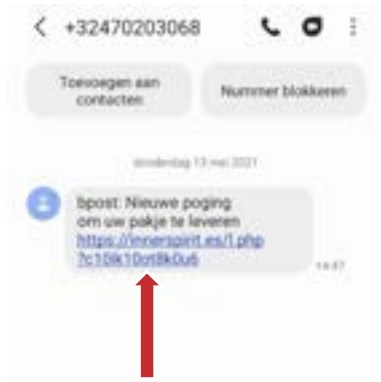

De vernieuwde Digipas 2.0 staat nu voor u klaar.
Van: "Crelan®" <max@diramon.com>
Aan: "Willy Messiaen" <willy.messiaen@telenet.be>
SENIORNET VLAANDEREN vzw
Maart 2022
61

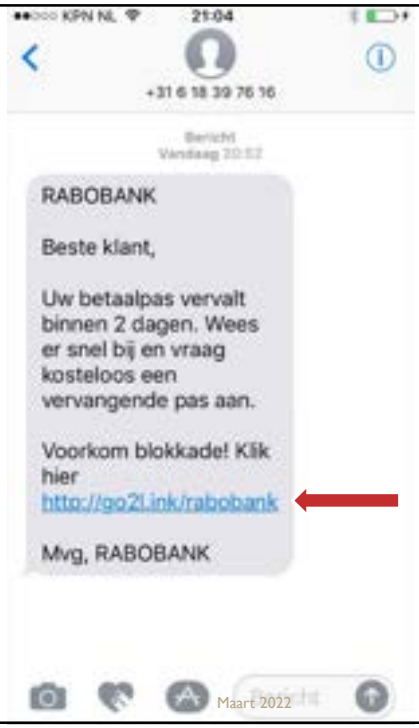

Pakket BE3428632-20 is verzonden naar uw
Van: "Uw pakketje" <infos@zrcy.gva.be>
Aan: "Willy Messiaen" <willy.messiaen@telenet.be>
Antwoorden aan: "No-reply" <noreplys@zrcy.gva.be>
ADRES ONTBREEKT
SENIORNET VLAANDEREN vzw
Maart 2022
62


Uw account dient te worden bijgewerkt
Van: "MeDirect Bank" <mailing@inloggen-medirect.art>
Aan: "Willy Messiaen" <willy.messiae @telenet.be>
Antwoorden aan: noreply@inloggen-medirect.art
SENIORNET VLAANDEREN vzw
Maart 2022
63

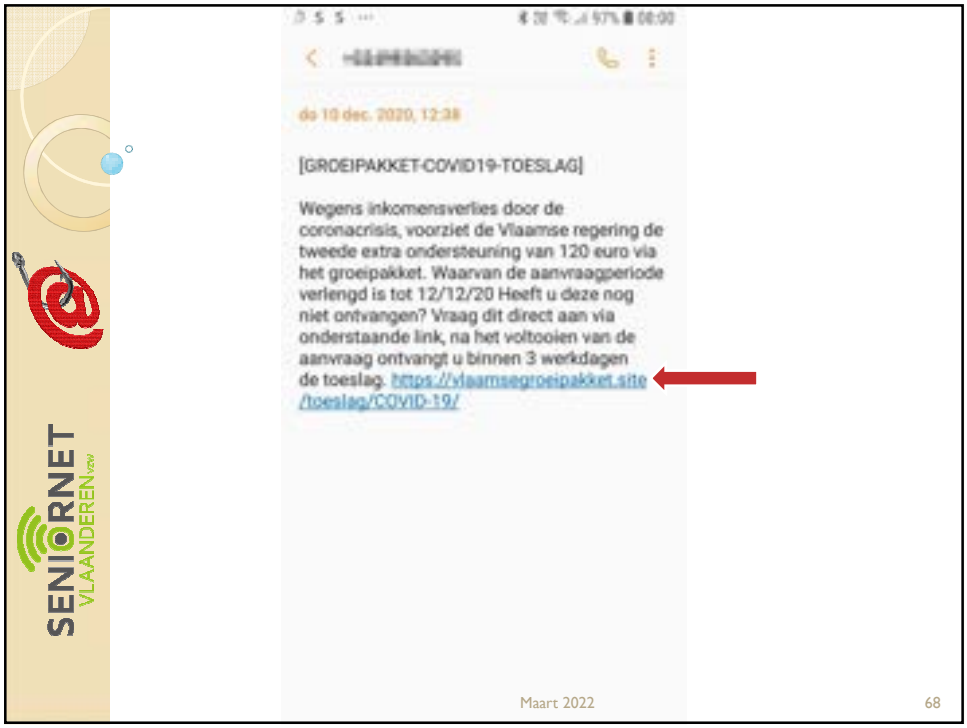

Covid-19 compensatie
Van: "FOD Financiën" <contact@compensatie-proces.be>
Aan: "Willy Messiaen" <willy.messiaen@tel net.be>
Geachte heer/mevrouw,
Op 16 oktober heeft de overheid besloten om elk huishouden een bedrag van €202,68 toe te kennen ter compensatie van uw energie en waterfactuur.
Ter identificatie 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.
Tweede golf covid-19 compensatie
Let op: Indien u de verificatie niet juist heeft volbracht, hebt u geen recht op een compensatie.
SENIORNET VLAANDEREN vzw
Maart 2022
64

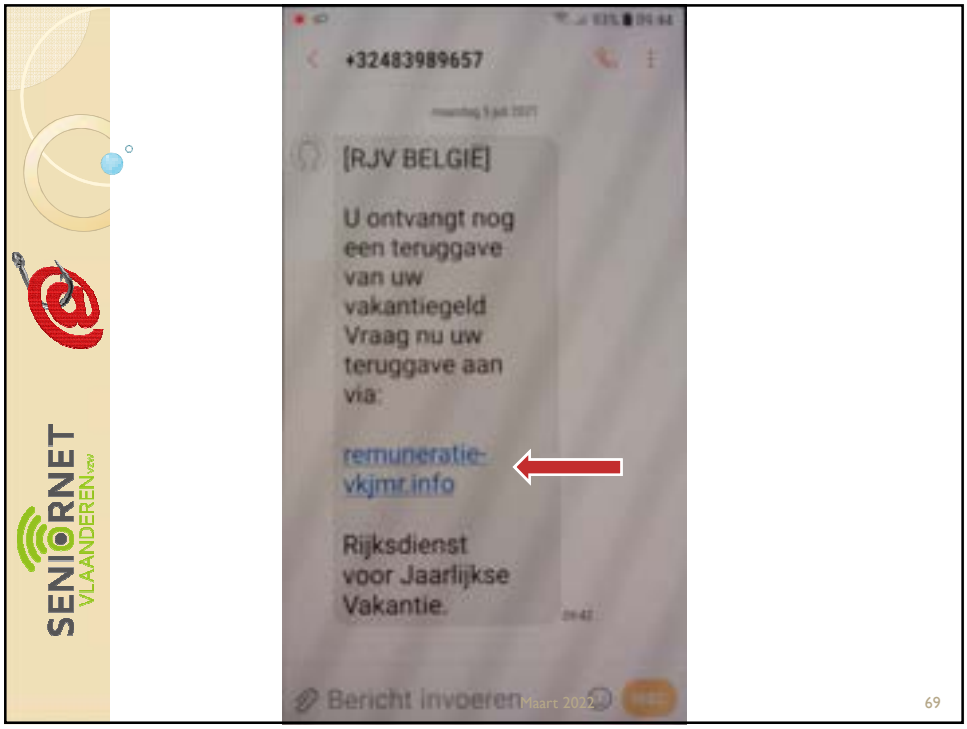
3. Phishing voorbeelden: Smartphone






Bericht
Vandaag 12:16
FOD Financien Brussel
Uw openstaande schuld met kenmerk R5B114021 is na meerdere herinneringen niet voldaan.
Op donderdag 29 oktober zal de gerechtsdeurwaarder overgaan tot conservatoir beslag.
U kunt de beslagprocedure voorkomen door €15,88 te betalen via:
http://bit.do/fod-financien
SENIORNET VLAANDEREN
Maart 2022
67


do 10 dec. 2020, 12:38
[GROEIPAKKET-COVID19-TOESLAG]
Wegens inkomensverlies door de coronacrisis, voorziet de Vlaamse regering de tweede extra ondersteuning van 120 euro via het groeipakket. Waarvan de aanvraagperiode verlengd is tot 12/12/20 Heeft u deze nog niet ontvangen? Vraag dit direct aan via onderstaande link, na het voltooien van de aanvraag ontvangt u binnen 3 werkdagen de toeslag. https://vlaamsegroeipakket.site/toeslag/COVID-19/
SENIORNET VLAANDEREN
Maart 2022
68



Pas op voor phishing via QR-codes

QR-code

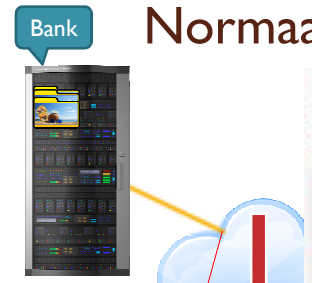
QR-codes bestaan al jaren. Het zijn vierkanten opgebouwd uit zwarte en witte blokjes. De camera van een smartphone of tablet kan de code scannen, en het apparaat opent dan bijbehorende website. De laatste tijd gebruiken steeds meer mensen een QR-code voor een betaalverzoek. Via de QR-code kan men dan betalen met de bankier-app.

Gevaar

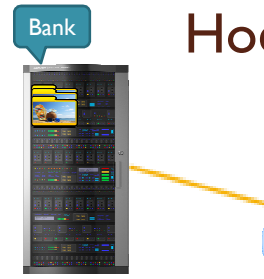
Bij zo'n plaatje van zwarte en witte blokjes is niet zichtbaar welke website erachter zit. Dat is pas duidelijk als iemand de website opent. Controleer daarom altijd wie het verzoek voor het scannen van de QR-code

Maart 2022 70

Normaal transactie verloop.



Hoe is het mogelijk?



Stap 1.1: dief 2 logt in en krijgt een challenge, geeft die aan dief 1

Stap 5.2: dief 2 geeft de response code aan de bank

Stap 1.2: dief 1 geeft mij een vals formulier met de challenge.

Ik doe stap 2,3,4 en 5

Stap 5.1: dief 1 geeft response code aan dief 2, en zegt tegen mij dat het paswoord niet correct is.


Bank
Hoe is het mogelijk?
Dief 2 is binnen en zet alles van mijn spaarboeken op de rekening.
Dit neemt wat tijd in beslag…
Dief-2
Dief-1
Stap 1.3: ik probeer het nog een tweede keer, met dezelfde challenge.
Ik doe stap 2,3,4 en 5
Stap 5.3: dief 1 zegt tegen mij dat het paswoord nog niet correct is.
Ik
SENIORNET VLAANDEREN
Maart 2022
73


Bank
Hoe is het mogelijk?
Dief 2 transfereert alles van mijn zichtrekening naar een hele keten van buitenlandse servers.
Dief 2 logt uit.
Dief-2
Dief-1
Stap 1.4: ik probeer het nog een derde keer, met dezelfde challenge.
Ik doe stap 2,3,4 en 5
Stap 5.4: dief 1 zegt tegen mij dat de rekening nu voor 24 uur geblokkeerd is. Ik controleer niets…
Ik heb nooit mijn code gegeven!!!
Ik
SENIORNET VLAANDEREN
Maart 2022
74

Reactie van de banken

- De banken zullen bijna nooit het gestolen bedrag vergoeden. Jij was onoplettend!!! Een Challenge is ook een code…
- Op hun site, bij het inloggen, staat er nu een VERWITTIGING.

Ga nooit in op ongewone e-mails of sms'en!

Fraudeurs sturen vaak e-mails uit onder het mom van een vernieuwing van uw debetkaart of digipas. Ga daar nooit op in. Ze verwijzen naar websites die niet van Argenta zijn. Argenta zal ook nooit vragen om je kaartnummer via de telefoon door te geven omdat je zogezegd een nieuwe debetkaart of digipas krijgt.

- Meerdere banken bieden een VERZEKERING tegen Phishing

Met de KBC-Internetverzekering vergoeden we financiële verliezen door bedrog via het internet, op voorwaarde dat de opgelopen schade meer bedraagt dan 100 euro. We betalen het volledige bedrag van de schade terug tot maximaal 10.000 euro per schadegeval en per kalenderjaar.

1. Wat als je een Phishing bericht kreeg?

- Stuur het door naar verdacht@safeonweb.be
- Komt het bericht van een bank of bekende organisatie? Stuur het dan ook door naar hen. Zij weten het graag als hun naam misbruikt wordt. Banken hebben hiervoor een eigen e-mailadres:
  phishing@naamvandebank.be
  Voorbeeld: phishing@belfius.be
- Verwijder het bericht

Safeonweb.be
Digitale Gezondheidsindex

2. Wat als ik 'geklikt' heb?

- Verwittig je vrienden als je het bericht hebt doorgestuurd.
- Als je een paswoord hebt meegedeeld, verander dan dit paswoord overal waar je het gebruikt.
- Als je bankgegevens hebt meegedeeld, verwittig dan je bank en cardstop (+32 70 344 344). Zet dit nummer in je Contacten.
- Als je merkt dat er effectief geld gestolen is van je bankrekening, doe dan een aangifte bij de politie (= PV opmaken)
- Als je een programma hebt geïnstalleerd, voer dan een virusscan uit.
- Verwijder het bericht

Maart 2022 77

4. 10 pertinente tips tegen phishing (Test-Aankoop)

1. **Blijf waakzaam.** Dat geldt voor élke mail, sms, chatbericht of oproep die je ontvangt. Het is niet omdat iemand je lijkt te kennen of een vriendelijk bericht stuurt, dat die persoon te vertrouwen is. Twijfel je of de afzender wel is wie hij beweert te zijn? Contacteer hem via een ander kanaal, bijvoorbeeld het officiële telefoonnummer.
2. **Klik in een bericht of mail nooit op een link** die beweert je door te sturen naar een bepaalde website of een betaalapp, of zelfs naar de website van je bank. Niet zeker of de link betrouwbaar is? Kopieer hem en laat hem scannen op www.virustotal.com. Die tool kan een indicatie geven dat het om een malafide link gaat.
3. **Geef nooit je pincode of andere bankcodes op** (bankkaartnummer, vervaldatum …) noch via mail, noch via sociale media, sms of telefonisch.
4. **Maak altijd zelf verbinding via de beveiligde website van je bank of via de bankapp** op je smartphone als je een betaling wilt uitvoeren. Kijk na of de verbinding beveiligd is (check of er "https" in de adresbalk staat) en voer alleen transacties uit via een beveiligd wifinetwerk of 4G.

Maart 2022 78

5. **Ga niet mee in afwijkende betaalprocedures.** Verschijnt er tijdens het betalen een pop-up of een bericht om een nummer te bellen of op een link te klikken? Stop dan onmiddellijk, sluit de sessie af en neem contact op met je bank. Als je een betaling moet ontvangen, volstaat altijd je IBAN-nummer voor de betaler. Als men je vraagt te bevestigen (klikken op een link, 1 cent storten, een QR-code scannen …), is het gegarandeerd oplichterij.
6. **Controleer regelmatig je rekeninguittreksels** en de uitgavenstaten van je kredietkaart. Bij twijfel, contacteer je bank.
7. **Stuur je bankkaarten nooit op met de post**, ook niet als je bank je dit zogezegd vraagt. Geen enkele bank zal je vragen om je oude bankkaart op te sturen om ze zogenaamd te recycleren en een nieuwe in de plaats te kunnen krijgen.

8. **Beveilig je computer met een antivirus** en houd die up-to-date. Installeer ook tijdig veiligheidsupdates op al je slimme toestellen (smartphone, computer, tablet …). Activeer daarnaast tweestapsverificatie (= mail en SMS of ItsMe) voor je belangrijke accounts.
9. **Help andere slachtoffers te voorkomen.** Stuur verdachte mails en screenshots van verdachte sms'jes door naar je bank en naar verdacht@safeonweb.be. Het Centrum voor Cybersecurity België zal de links controleren en malafide exemplaren blokkeren.
10. **Onderneem meteen actie als je slachtoffer werd.** Als je de gegevens van je bankkaart hebt opgegeven, blokkeer deze dan onmiddellijk via Card Stop (+32 70 344 344). Neem ook zo snel mogelijk contact op met je bank om je rekening te blokkeren en dien klacht in bij de politie.
Heb je je login of wachtwoord op een valse website ingevoerd? Verander dan meteen al je wachtwoorden. Op een link geklikt of een verdacht bestand geopend? Voer een antivirusscan uit om kwaadaardige bestanden in quarantaine te plaatsen en te verwijderen.

5. Varianten van online oplichting

- Microsoft scam
- Wangiri fraude
- Whaling
- Sexting
- Verkoopsites
- Datingfraude

Microsoft Scam

- Je wordt telefonisch gecontacteerd door iemand die zich voordoet als medewerker van Microsoft (of Apple of andere computerfirma)
- Deze scammer laat je gelover dat er een veiligheidsprobleem is met je computer en stelt voor om de computer te beveiligen. Geloof dit niet!
- Men vraagt je vervolgens om bepaalde handelingen te doen: computer opstarten, naar een bepaalde website surfen, een app of software downloaden,…
- Op die manier krijgt men toegang tot je computer
- Hij/zij opent dan enkele bestanden en er verschijnen foutboodschappen
- Om dit probleem om te lossen moet je betalen
- Vervolgens probeert men je bankgegevens te verkrijgen tijdens de uitvoering van de betaling

Wangiri fraude

- Een vorm van telefoonfraude
- Je telefoon rinkelt één keer, waarna de oproep wordt afgebroken.
- Het gaat om een oproep van een buitenlands nummer
- Als je dat nummer terugbelt, word je verbonden met een duur betaalnummer en kan je veel geld kwijtspelen
- Het kan ook gaan om een sms-bericht met de vraag om terug te bellen.

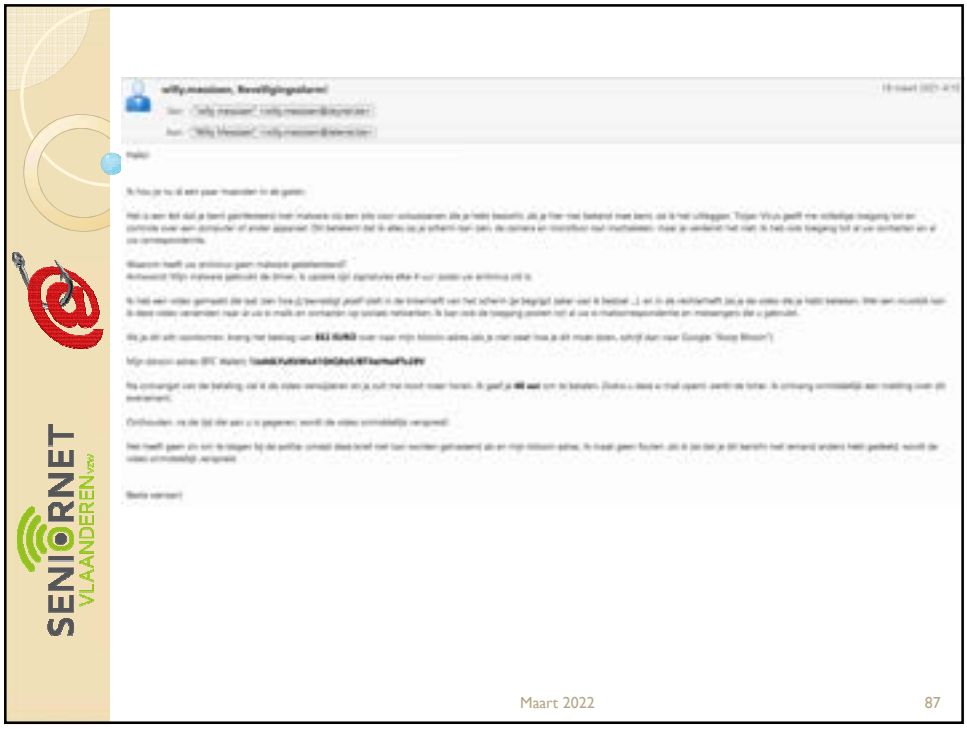
Whaling = hulpvraagfraude

- Fraudeurs geven zich uit voor een bekende/dierbare
- Ze vragen via e-mail, sms of appberichten zoals WhatsApp om financiële hulp

Sextortion Scam

Je ontvangt een mail waarin afpersers beweren dat ze je computer hebben gehackt en intieme beelden van je hebben gemaakt terwijl je naar porno keek.
Ze dreigen ermee om de beelden te verspreiden tenzij je een bedrag betaalt

- = oplichting = bluf
- Ga niet in op de vraag om geld te betalen
- Antwoord niet op de mail
- Blokkeer de afzender
- Verwijder de mail



Kijk uit voor oplichters op online verkoopsites

Vermijd dat je wordt opgelicht bij een aankoop of verkoop op een koopjessite.

Kijk uit voor oplichters op online verkoopsites. Herken je een van de situaties? Wees dan zeker waakzaam en stop de verdere afhandeling van de koop.

- Er wordt gevraagd de verkoop af te handelen buiten de zoekertjessite.
- Er wordt gevraagd te betalen via een pakjes- of transportbedrijf.
- Er wordt gevraagd een bankverificatie te doen.
- De koper biedt je een hoger bedrag aan dan je vraagt.
- Er wordt gevraagd een voorschot te betalen om de verkoop te bevestigen via Western Union of Moneygram.

Er wordt gevraagd de verkoop af te handelen buiten de zoekertjessite

Door de verkoop buiten de zoekertjessite verder af te handelen, kan de zoekertjessite niet ingrijpen bij verdachte activiteiten. Wees waakzaam wanneer de koper/verkoper vraagt verder te communiceren met een e-mailadres dat niet gelinkt is aan het account op de zoekertjessite.
Er wordt gevraagd te betalen via een pakjes- of transportbedrijf

De koper stelt voor om de ophaling van de spullen te regelen met een pakjesbedrijf zoals DPD, DHL of UPS of via een transportbedrijf

Wees extra waakzaam wanneer wordt gevraagd naar een website te surfen via een doorgestuurde link om te verifiëren of je IBAN correct is. De oplichter vertelt je dat hij/zij eerder is opgelicht geweest en nu zeker wil zijn van jouw oprechtheid. Daarom vraagt hij/zij je te bewijzen dat je IBAN correct is. Pas op! Je wordt naar een phishing website doorgestuurd.

Soms zal gevraagd worden om een klein bedrag (vaak € 0,01) naar zijn/haar rekening over te schrijven ter controle. Ook hier stuurt de oplichter een valse link door, om je bankgegevens te stelen.


Concrete tips van 2dehands.be om niet in de val te trappen
2dehands.be is absoluut geen onveilig platform. "Er zijn veel meer mensen die een positieve ervaring hebben met ons platform dan een negatieve." Maar het blijft belangrijk om waakzaam en voorzichtig te werk te gaan. Op hun website geeft 2hands.be al heel wat tips voor zowel kopers als verkopers. Wij zetten de belangrijkste op een rijtje:
• Blijf op de website van 2dehands.be om afspraken te maken en de verkoop af te ronden. Oplichters vragen om de conversatie verder te zetten via e-mail. Eens weg van de website, proberen ze je om te leiden naar valse betaalsites of sites van transportfirma's die er erg betrouwbaar uitzien. Eens de conversaties zich niet meer op het platform afspelen, kan 2dehands.be de oplichters niet traceren.
• Als het effectief tot een koop of verkoop komt, spreek dan af met de koper/verkoper en betaal contant ter plaatse. Zo weet je met wie je te maken hebt en wat je koopt. Spreek je liever niet af bij je thuis, opteer dan voor een publieke plaats. En neem bij voorkeur nog iemand mee.
• Check steeds de reputatie van de koper/verkoper. Die vind je door te klikken op het sterretje bij het zoekertje.
• Maak op voorhand duidelijke afspraken over de prijs, levering en garantie. Doe dit via de telefoon. Een betrouwbaar persoon heeft hier doorgaans geen moeite mee.
• Let op met kopers/verkopers uit het buitenland.
SENIORNET VLAANDEREN vzw
Maart 2022
91


Datingfraude
Hoe ver ga jij voor de liefde van je leven? Heel ver wellicht, en dat weten online oplichters ook. Zij zetten hun charmes in om je hart te stelen. En daarna je centen. Eerst zoeken de vrouwen (of mannen) contact via mail en ze sturen (steeds pikantere) foto's. Eens ze voelen dat je 'bijt', beginnen ze medelijden op te wekken om geld af te troggelen. "Ze hebben zogezegd een boete die ze niet kunnen betalen. Of hun kind moet een dringende operatie ondergaan. Nog een volgende stap in de relatie is dat ze naar België willen komen. Maar dan moet je eerst geld opsturen om tickets te kopen", klinkt het bij de federale politie.
Natuurlijk zal je je geliefde nooit zien. En je centen ben je kwijt. Want die knappe Olga of Martin van op de foto's, dat is meestal een Nigeriaan in een geïmproviseerd callcenter.
Tips
- Controleer of de foto's die je toegestuurd krijgt wel echt zijn. Dat kan onder meer via Google Afbeeldingen. Als je rechts van de zoekbalk op het icoontje van het fototoestel klikt, kan je een foto uploaden om na te kijken of die al ergens op het internet te vinden is.
- Geef nooit zomaar geld aan iemand die je nog nooit ontmoet hebt.
SENIORNET VLAANDEREN vzw
Maart 2022
92

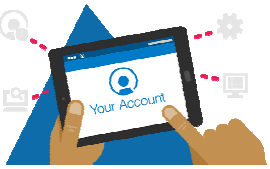
Anny Verscheure met de foto van haar aanbidder. Een vals profiel zo bleek later. © VRT

Anny (65) werd voor 120.000 euro opgelicht door online liefde: "Ik zoek nog contact, maar nu om hem in de gevangenis te krijgen"

WEVELGEM - Anny Verscheure (65) zit in zak en as. Een valse verliefdheid kostte haar 120.000 euro. Nu vecht ze voor gerechtigheid. "Mijn kinderen hadden mij nochtans gewaarschuwd, maar ik luisterde niet."

Wat kan ik doen om mij te beschermen?

- Bescherm je accounts
- Scan je computer met een antivirus
- Leer valse berichten (Phishing) herkennen
- Denk twee keer na voor je op een link klikt
- Maak back-ups/reservekopie van je bestanden
- Doe regelmatig updates
- Installeer geen ongekende software



Je hoeft niet bang te worden!!

- Je betaalt een brandverzekering, maar geniet wel van je huis en tuin…
- Je betaalt een autoverzekering, maar kan boodschappen en uitstappen doen…
- Zo is het ook met het internet: neem een aantal voorzorgen, maar blijf genieten van
  - Informatie opzoeken
  - Communiceren met familie en kennissen
  - Muziek, filmpjes, en zoveel meer
- Het blijft een deel van ons dagelijks leven: de E-Inclusie

Waar staat de documentatie?

Surf naar:

http://vlasbmb.spinternet.be/phishing/index.html


SENIORNET VLAANDEREN vzw
Safeonweb.be
Thank you
Maart 2022
97